Generalized weights of rank metric codes, a combinatorial appraoch

by Trygve Johnsen, based on joint work with Sudhir Ghorpade

August 14, 2019

Linear codes

Let $C \subset (F_q)^n$, for F_q the field with q elements.

Linear codes

Let $C \subset (F_q)^n$, for F_q the field with q elements.
If C is a **subvector space** of $(F_q)^n$, then it called a **linear** code.

Linear codes

Let $C \subset (F_q)^n$, for F_q the field with q elements.
If C is a **subvector space** of $(F_q)^n$, then it called a **linear** code.
The **dimension** k of C is its dimension as vector space over F_q.
Clearly $0 \leq k \leq n$.

Linear codes

Let $C \subset (F_q)^n$, for F_q the field with q elements.
If C is a **subvector space** of $(F_q)^n$, then it called a **linear** code.
The **dimension** k of C is its dimension as vector space over F_q.
Clearly $0 \leq k \leq n$.
Moreover the minimum distance of C is

$$d = d(C) = \min d(\mathbf{x}, \mathbf{y}),$$

for $\mathbf{x}, \mathbf{y} \in C$ and $\mathbf{x} \neq \mathbf{y}$.

Linear codes

Let $C \subset (F_q)^n$, for F_q the field with q elements.
If C is a **subvector space** of $(F_q)^n$, then it called a **linear** code.
The **dimension** k of C is its dimension as vector space over F_q.
Clearly $0 \leq k \leq n$.
Moreover the minimum distance of C is

$$d = d(C) = \min d(\mathbf{x}, \mathbf{y}),$$

for $\mathbf{x}, \mathbf{y} \in C$ and $\mathbf{x} \neq \mathbf{y}$.
From the translation invariance of linear codes,
$d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} - \mathbf{y}, \mathbf{0})$, we observe:

$$d = d(C) = \min w(\mathbf{x}) = \min d(\mathbf{x}, \mathbf{0}),$$

for $\mathbf{x} \in C$ and $\mathbf{x} \neq \mathbf{0}$.

Delsarte rank metric codes

A Delsarte rank metric code C is a subspace of the set of $(m \times n)$-matrices over F_q.

Delsarte rank metric codes

A Delsarte rank metric code C is a subspace of the set of $(m \times n)$-matrices over F_q.
The **dimension** K of C is its dimension as vector space over F_q.
Clearly $0 \leq K \leq m \times n$.

Delsarte rank metric codes

A Delsarte rank metric code C is a subspace of the set of $(m \times n)$-matrices over F_q.
The **dimension** K of C is its dimension as vector space over F_q.
Clearly $0 \leq K \leq m \times n$.
Moreover the minimum distance of C is

$$d = d(C) = \min d(M, N) = \min rk(M - N)$$

for $M, N \in C$ and $M \neq N$.

Delsarte rank metric codes

A Delsarte rank metric code C is a subspace of the set of $(m \times n)$-matrices over F_q.
The **dimension** K of C is its dimension as vector space over F_q.
Clearly $0 \leq K \leq m \times n$.
Moreover the minimum distance of C is

$$d = d(C) = \min d(M, N) = \min rk(M - N)$$

for $M, N \in C$ and $M \neq N$.
From the translation invariance of linear codes, $d(M, N) = d(M - N), \mathbf{0})$, we observe:

$$d = d(C) = \min d(M, \mathbf{0}) = \min rk(M),$$

for $M \in C$ and $M \neq \mathbf{0}$.

Generalized weights of rank metric codes

For X a subspace of $E = F_q^n$ set

$$C(X) = \{M \in C | \ \mathrm{rowspace}(M) \subset X\}$$

.

Generalized weights of rank metric codes

For X a subspace of $E = F_q^n$ set

$$C(X) = \{M \in C | \text{ rowspace}(M) \subset X\}$$

.

For $r = 1, \cdots, k = \dim C$ set:

$$d_r(C) = \min\{\dim X | X \leq E \text{ and } \dim C(X) \geq r\}$$

.

Generalized weights of rank metric codes

For X a subspace of $E = F_q^n$ set

$$C(X) = \{M \in C | \text{ rowspace}(M) \subset X\}$$

.

For $r = 1, \cdots, k = \dim C$ set:

$$d_r(C) = \min\{\dim X | X \leq E \text{ and } \dim C(X) \geq r\}$$

.

In particular

$$d_1(C) = \min\{\dim X | \dim C(X) \geq 1\} =$$

$$\min\{\dim X | \text{ the row space of some M } \in C \text{ is contained in } X\} =$$

$$\min\{rk(M) | M \in C\} = d(C).$$

Duality of rank metric codes

Given a Delsarte rank metric code C. Its dual code $C^{\perp}$ consists of those $(m \times n)$-matrices N, such that

$$[M \times N^t]^T = 0,$$

for all $M \in C$. Here T denotes the trace of a diagonal matrix, and t denotes transposition of matrices.

Duality of rank metric codes

Given a Delsarte rank metric code C. Its dual code $C^\perp$ consists of those $(m \times n)$-matrices N, such that

$$[M \times N^t]^T = 0,$$

for all $M \in C$. Here T denotes the trace of a diagonal matrix, and t denotes transposition of matrices.
We observe that $\dim C^\perp = mn - K$, and that $(C^\perp)^\perp = C$.

Is there some sort of Wei duality between C and $C^{\perp}$?

Is there some sort of Wei duality between C and $C^{\perp}$?
There are K values of r to find $d_r(C)$ for, and $mn - K$ values of r to find $d_r(C^{\perp})$ for, so altogether mn such generalized d_i to consider. All these values are in $\{1, 2, \cdots, n\}$.

Is there some sort of Wei duality between C and $C^{\perp}$?
There are K values of r to find $d_r(C)$ for, and $mn - K$ values of r to find $d_r(C^{\perp})$ for, so altogether mn such generalized d_i to consider. All these values are in $\{1, 2, \cdots, n\}$.
Hence a statement like

$$\{1, 2, \cdots, n\} = \{d_1(C), \cdots, d_K(C)\} \cup$$

$$\{n + 1 - d_1(C^{\perp}), \cdots, n + 1 - d_{mn-K}(C^{\perp})\}$$

is impossible if $m \geq 2$.

Modified Wei duality

Let

$$W_s(C) = \{d_r(C), r = 1, \cdots, K, \text{ and } r = s (\mathrm{mod\ m})\}$$

and

$$\overline{W}_s(C) = \{n + 1 - d_r(C), r = 1, \cdots, K, \text{ and } r = s (\mathrm{mod\ m})\}.$$

Modified Wei duality

Let

$$W_s(C) = \{d_r(C), r = 1, \cdots, K, \text{ and } r = s (\text{mod m})\}$$

and

$$\overline{W}_s(C) = \{n+1-d_r(C), r = 1, \cdots, K, \text{ and } r = s (\text{mod m})\}.$$

Then

$$W_s(C^\perp) = \{1, 2, \cdots, n\} - \overline{W}_{s+^mK}(C),$$

for $0 \leq s < m$. (So $\{1, 2, \cdots, n\}$ is the disjoint union of these two sets.)

Modified Wei duality

Let

$$W_s(C) = \{d_r(C), r = 1, \cdots, K, \text{ and } r = s (\text{mod m})\}$$

and

$$\overline{W}_s(C) = \{n + 1 - d_r(C), r = 1, \cdots, K, \text{ and } r = s (\text{mod m})\}.$$

Then

$$W_s(C^\perp) = \{1, 2, \cdots, n\} - \overline{W}_{s+^m K}(C),$$

for $0 \leq s < m$. (So $\{1, 2, \cdots, n\}$ is the disjoint union of these two sets.)

How does one prove this ?

Modified Wei duality

There are several ways to do it, and various approaches from different authors.

A (q, m)-polymatroid is an ordered pair $P = (E, \rho)$, where $E = (F_q)^n$ as before and ρ is a function from $\Sigma(E)$ $(=\text{the set of subspaces of E})$ to $\mathbb{N}_0 = 0, 1, 2, \cdots\}$ satisfying

Modified Wei duality

There are several ways to do it, and various approaches from different authors.

A (q, m)-polymatroid is an ordered pair $P = (E, \rho)$, where $E = (F_q)^n$ as before and ρ is a function from $\Sigma(E)$ (=the set of subspaces of E) to $\mathbb{N}_0 = 0, 1, 2, \cdots\}$ satisfying

$$\text{(R1) } 0 \leq \rho(X) \leq m \dim X,$$

$$\text{(R2) If } X \leq Y, \text{ then } \rho(X) \leq \rho(Y),$$

$$\text{(R3) } \rho(X + Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y),$$

for all subspaces X, y of E. We set $rk(P) = \rho(E)$.

Polymatroid of a code

For a rank metric code C set $(E = (F_q)^n)$, and

$$\rho(X) = \dim C - \dim C(X^\perp),$$

for the usual dot product on E.

Polymatroid of a code

For a rank metric code C set $(E = (F_q)^n)$, and

$$\rho(X) = \dim C - \dim C(X^{\perp}),$$

for the usual dot product on E.
One can prove (Keisuke Shiromoto) that $P = (E, \rho)$ is a $(q, m)-$polymatroid. Call it $P(C)$.
Let $P^* = (E, \rho^*)$, where

$$\rho^*(X) = \rho(X^{\perp}) + m \dim X - \rho(E),$$

for all subspaces X of E.

Polymatroid of a code

For a rank metric code C set $(E = (F_q)^n)$, and

$$\rho(X) = \dim C - \dim C(X^{\perp}),$$

for the usual dot product on E.
One can prove (Keisuke Shiromoto) that $P = (E, \rho)$ is a $(q, m)-$polymatroid. Call it $P(C)$.
Let $P^* = (E, \rho^*)$, where

$$\rho^*(X) = \rho(X^{\perp}) + m \dim X - \rho(E),$$

for all subspaces X of E.
Then $P(C)^* = P(C^{\perp})$.

For a (q, m)-polymatroid P set

$$d_r(P) = \min\{\dim X | \nu^*(X) \geq r\},$$

for $r = 1, \cdots, rk(P)$. Here $\nu^*(X)$ denotes the conullity $m \dim X - \rho^*(X)$.

Theorem

If C is a Delsarte rank metric code, then $d_r(P(C)) = d_r(C)$ (and $d_r(P(C)^*) = d_r(P(C^\perp) = d_r(C^\perp)$ for all r in question.

We prove more:

Wei duality for (q, m)-polymatroids

Wei duality for (q, m)-polymatroids

Theorem

Modified Wei duality is valid for (q, m)-polymatroids in general: Let

$$W_s(P) = \{d_r(C), r = 1, \cdots, K = rk(P), \ \text{and } r = s (\text{mod } m)\}$$

and

$$\overline{W}_s(P) = \{n + 1 - d_r(P), r = 1, \cdots, K, \ \text{and } r = s (\text{mod } m)\}.$$

Wei duality for (q, m)-polymatroids

Theorem

Modified Wei duality is valid for (q, m)-polymatroids in general: Let

$$W_s(P) = \{d_r(C), r = 1, \cdots, K = rk(P), \ and \ r = s(mod \ m)\}$$

and

$$\overline{W}_s(P) = \{n + 1 - d_r(P), r = 1, \cdots, K, \ and \ r = s(mod \ m)\}.$$

Then

$$W_s(P^*) = \{1, 2, \cdots, n\} - \overline{W}_{s+^m K}(P),$$

for $0 \leq s < m$. (So $\{1, 2, \cdots, n\}$ is the disjoint union of these two sets.)

Variations on this theme

There are other definitions of generalized weights for Delsarte rank metric codes using socalled anticodes. (Ravagnani/Gorla). Our description/definition matches theirs for $m > n$. If $m < n$, one could interchange the roles of m and n, and look at the "transposed" (q, n)-polymatroid $P'(C) = ((F_q)^m, \rho')$ defined in an analogous way. Then this matches the definition s of Ravagnani/Gorla, and modified Wei duality can be shown in an analogues, transposed way.

Variations on this theme

There are other definitions of generalized weights for Delsarte rank metric codes using socalled anticodes. (Ravagnani/Gorla). Our description/definition matches theirs for $m > n$. If $m < n$, one could interchange the roles of m and n, and look at the "transposed" (q, n)-polymatroid $P'(C) = ((F_q)^m, \rho')$ defined in an analogous way. Then this matches the definition s of Ravagnani/Gorla, and modified Wei duality can be shown in an analogues, transposed way.

For square $m \times m = n \times n$-matrices, one could look at the function $\rho(X) = \min(\rho_m(X), \rho'(X))$, where ρ_m is the "old" ρ.

Then one can define

$$\rho^*(X) = \rho(X^\perp) + m \dim X - \rho(E),$$

and

$$d_r(P) = \min\{\dim X | \nu^*(X) \geq r\},$$

as before. Then this matches the definition of Ravagnani/Gorla.
Problem: This "new" ρ is not necessarily a (q, m)-polymatroid.
Does modified Wei duality hold ?

Then one can define

$$\rho^*(X) = \rho(X^\perp) + m \dim X - \rho(E),$$

and

$$d_r(P) = \min\{\dim X | \nu^*(X) \geq r\},$$

as before. Then this matches the definition of Ravagnani/Gorla. Problem: This "new" ρ is not necessarily a (q, m)-polymatroid. Does modified Wei duality hold ? Solution: This "new" $P = (E, \rho)$ turns out to be a socalled (q, m)-demipolymatroid, and one can prove that modified Wei duality holds for such combinatorial objects also.

A (q, m)-demipolymatroid is an ordered pair $P = (E, \rho)$, where $E = (F_q)^n$ as before and ρ is a function from $\Sigma(E)$ (=the set of subspaces of E) to $\mathbb{N}_0 = 0, 1, 2, \cdots\}$ satisfying

A (q, m)-demipolymatroid is an ordered pair $P = (E, \rho)$, where $E = (F_q)^n$ as before and ρ is a function from $\Sigma(E)$ (=the set of subspaces of E) to $\mathbb{N}_0 = 0, 1, 2, \cdots \}$ satisfying

$$\text{(R1) } 0 \leq \rho(X) \leq m \dim X,$$

$$\text{(R2) If } X \leq Y, \text{ then } \rho(X) \leq \rho(Y),$$

$$\text{(R4) } \rho^* \text{ satisfies (R1) and (R2).}$$

In particular (q, m)-polymatroids are (q, m)-demipolymatroids.

Gabidulin codes

These are particularly simple since $K = mk$ always is divisible by m. One fixes a k-dimensional subspace of $F_{q^m}^n$ over the field F_{q^m}, in other words a block code of length $n(< m$over this big field. Instead of using the usual Hamming distance, one fixes a basis $\{e_1, \cdots, e_m\}$ of F_{q^m} as a vector space over the field F_q. Hence every n-tuple over F_{q^m} is identified with an $(m \times n)$-matrix with entries in F_q. Then one proceeds as above, and the modified Wei duality simplifies:

$$W_s(C^{\perp}) = \{1, 2, \cdots, n\} - \overline{W}_{s+^mK}(C)$$

becomes

$$W_s(C^{\perp}) = \{1, 2, \cdots, n\} - \overline{W}_s(C),$$

for $s = 0, 1, \cdots, m-1$.

In general, for a Delsarte rank metric code, we call C an MRD code if $m > n$, and $K = mk$ is divisible by m, and $C(X) = \{0\}$ for all subspaces X of $E = (F_q)^n$ with $\dim X \leq n - k$. On the (q, m)-level this gives $\rho_C(X) = K = mk$ if $\dim X \geq k$, and $\rho_C(X) = m \dim X$ if $\dim X \leq k$.

In general, for a Delsarte rank metric code, we call C an MRD code if $m > n$, and $K = mk$ is divisible by m, and $C(X) = \{0\}$ for all subspaces X of $E = (F_q)^n$ with $\dim X \leq n - k$. On the (q, m)-level this gives $\rho_C(X) = K = mk$ if $\dim X \geq k$, and $\rho_C(X) = m \dim X$ if $\dim X \leq k$. This means that $P(C)$ is the "uniform" (q, m)-polymatroid $U(k, m)$. This is analogous to the situation for block codes, that they are MDS if and only their associated (usual) matroids are uniform.

Flags of codes

If $F = C_s \leq \cdots C_2 \leq C_1$ is a flag/chain of Delsarte rank metric codes (and if, say, $m > n$), then look at

$$\rho(X) = \rho_1(X) - \rho_2(X) + \cdots + (-1)^{s+1}\rho_s(X).$$

Then $P = (E, \rho)$ is a (q, m)-demipolymatroid. So modified Wei duality holds on the "matroid"-level. Is there a dual flag/chain $F^{\perp}$ such that $P^* = P(F^{\perp})$.

Flags of codes

If $F = C_s \leq \cdots C_2 \leq C_1$ is a flag/chain of Delsarte rank metric codes (and if, say, $m > n$), then look at

$$\rho(X) = \rho_1(X) - \rho_2(X) + \cdots + (-1)^{s+1}\rho_s(X).$$

Then $P = (E, \rho)$ is a (q, m)-demipolymatroid. So modified Wei duality holds on the "matroid"-level. Is there a dual flag/chain $F^\perp$ such that $P^* = P(F^\perp)$.

It is, if s is odd; just take the chain of orthogonal complements. If s is even, and $C_s \neq 0$, add $C_{s+1} = \{0\}$, and regard it as an "odd" case. If s is even, and $C_s = 0$, delete C_s, and regard it as an "odd" case. The modified Wei duality holds on the code level.

Flags of codes

If $F = C_s \leq \cdots C_2 \leq C_1$ is a flag/chain of Delsarte rank metric codes (and if, say, $m > n$), then look at

$$\rho(X) = \rho_1(X) - \rho_2(X) + \cdots + (-1)^{s+1}\rho_s(X).$$

Then $P = (E, \rho)$ is a (q, m)-demipolymatroid. So modified Wei duality holds on the "matroid"-level. Is there a dual flag/chain $F^\perp$ such that $P^* = P(F^\perp)$.
It is, if s is odd; just take the chain of orthogonal complements. If s is even, and $C_s \neq 0$, add $C_{s+1} = \{0\}$, and regard it as an "odd" case. If s is even, and $C_s = 0$, delete C_s, and regard it as an "odd" case. The modified Wei duality holds on the code level.
Most interesting case: $s = 2$. But the dual/perpendicular objects are triples (or single codes).