Codes, metrics, and applications

Alexander Barg

University of Maryland
IITP RAS, Moscow

ISIT 2016

Talk summary

Coding theory in a class of metric spaces:

combinatorial and information-theoretic results and applications.

Talk summary

Coding theory in a class of metric spaces:
combinatorial and information-theoretic results and applications.

Problems:

- Distance distribution of codes
- Duality of linear codes
- Ordered linear codes and matroid invariants

Talk summary

Coding theory in a class of metric spaces:
combinatorial and information-theoretic results and applications.

Problems:

- Distance distribution of codes
- Duality of linear codes
- Ordered linear codes and matroid invariants
- Channel models matched to the ordered metrics; applications to polar codes, wiretap channels
- Association schemes and bounds on the size of codes
- Further extensions

Talk summary

Coding theory in a class of metric spaces:
combinatorial and information-theoretic results and applications.

Problems:

- Distance distribution of codes
- Duality of linear codes
- Ordered linear codes and matroid invariants
- Channel models matched to the ordered metrics; applications to polar codes, wiretap channels
- Association schemes and bounds on the size of codes
- Further extensions

Collaborators: Punarbasu Purkayastha, Woomyoung Park, Marcelo Firer, Maksim Skriganov, Min Ye, Talha Gulcu

Talk summary

Coding theory in a class of metric spaces:
combinatorial and information-theoretic results and applications.

Problems:

- Distance distribution of codes
- Duality of linear codes
- Ordered linear codes and matroid invariants
- Channel models matched to the ordered metrics; applications to polar codes, wiretap channels
- Association schemes and bounds on the size of codes
- Further extensions

Acknowledgment: NSF grants

CCF1217245 “Ordered metrics and their applications”

CCF1422955, CCF0916919, CCF0807411

Outline

- I. Brief recap: Linear codes, Weight distributions and duality, orthogonal arrays
- II. Applications of the ordered distance
  - Wireless
  - Reed-Solomon codes
  - Approximation theory
- III. Results on linear ordered codes
  - Shape distributions and bounds on codes
  - Duality of linear codes for poset metrics
  - Channel models
  - Polar codes

I. Linear codes

A linear code $\mathcal{C} \subset F_q^n$

G, H *generator* and *parity-check* matrices

Weight distribution $B_i, i = 0, 1, \ldots, n$, where

$$B_i = \sharp\{x \in \mathcal{C} : \mathrm{w}(x) = i\}$$

I. Linear codes

A linear code $\mathcal{C} \subset F_q^n$

G, H *generator* and *parity-check* matrices

Weight distribution $B_i, i = 0, 1, \ldots, n$, where

$$B_i = \sharp\{x \in \mathcal{C} : \mathrm{w}(x) = i\}$$

Weight distributions are useful for analyzing structural properties of codes; probability of error under MAP or incomplete decoding

I. Linear codes

A linear code $\mathcal{C} \subset F_q^n$

G, H *generator* and *parity-check* matrices

Weight distribution $B_i, i = 0, 1, \ldots, n$, where

$$B_i = \sharp\{x \in \mathcal{C} : \mathrm{w}(x) = i\}$$

Dual code $\mathcal{C}^{\text{(dual)}} = \{y \in F_q^n : (x, y) = 0 \ \forall x \in \mathcal{C}\}$

Weight distribution of $\mathcal{C}^{\textit{(dual)}}$*:* $B_i^{\text{(dual)}}, i = 0, 1, \ldots, n$

Weight enumerators:

$$B_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} B_i x^{n-i} y^i; \ B_{\mathcal{C}^{\text{(dual)}}}(x, y) = \sum_{i=0}^{n} B_i^{\text{(dual)}} x^{n-i} y^i$$

Linear codes and duality

The MacWilliams Theorem:

$$B_{\mathcal{C}}(x,y) = \frac{1}{\left|\mathcal{C}^{\text{(dual)}}\right|} B_{\mathcal{C}^{\text{(dual)}}}(x+(q-1)y, x-y)$$

Linear codes and duality

The MacWilliams Theorem:

$$B_{\mathcal{C}}(x, y) = \frac{1}{\left|\mathcal{C}^{\text{(dual)}}\right|} B_{\mathcal{C}^{\text{(dual)}}}(x + (q-1)y, x - y)$$

One of the basic facts in coding theory. Used for:

- Classification of codes over various domains
- Estimates of error probability
- Bounds on the size of codes in terms of distance
- Extensions used in sphere packing, optimality of lattices

Linear codes and duality

The MacWilliams Theorem:

$$B_{\mathcal{C}}(x,y) = \frac{1}{\left|\mathcal{C}^{\text{(dual)}}\right|} B_{\mathcal{C}^{\text{(dual)}}}(x+(q-1)y, x-y)$$

Approach via Fourier analysis:

$$B_j^{\text{(dual)}} = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} B_i K_j(i),\ j = 0, 1, \ldots, n$$

where

$$K_j(i) = \sum_{\ell=0}^{i} (-i)^{\ell} \binom{i}{\ell} \binom{n-i}{j-\ell} (q-1)^{j-\ell}$$

is a Krawtchouk polynomial

Linear codes and duality

The MacWilliams Theorem:

- Linear algebraic approach:
  Let $A \subset \{1, 2, \ldots, n\}$, $\rho A = \mathrm{rank}(G(A))$, $k = \dim \mathcal{C}$
  Define $Z_{\mathcal{C}}(x, y) = \sum_{A \subset [n]} x^{k-\rho A} y^{|A|-\rho A}$. Then

$$Z_{\mathcal{C}}(x, y) = Z_{\mathcal{C}^{\text{(dual)}}}(y, x)$$

  $Z_{\mathcal{C}}(x, y)$ is the Whitney rank-nullity function of $\mathcal{C}$

Linear codes and duality

The MacWilliams Theorem:

- Linear algebraic approach:
  Let $A \subset \{1, 2, \ldots, n\}$, $\rho A = \operatorname{rank}(G(A))$, $k = \dim \mathcal{C}$
  Define $Z_{\mathcal{C}}(x, y) = \sum_{A \subset [n]} x^{k-\rho A} y^{|A|-\rho A}$. Then

  $$Z_{\mathcal{C}}(x, y) = Z_{\mathcal{C}^{\text{(dual)}}}(y, x)$$

  $Z_{\mathcal{C}}(x, y)$ is the Whitney rank-nullity function of $\mathcal{C}$

- $$B_{\mathcal{C}}(x, y) = (x - y)^k y^{n-k} Z_{\mathcal{C}}\left(\frac{qy}{x - y}, \frac{x - y}{y}\right) \quad \text{(Greene 1976)}$$

Linear codes and duality

The MacWilliams Theorem:

- Linear algebraic approach:
  Let $A \subset \{1, 2, \dots, n\}$, $\rho A = \operatorname{rank}(G(A))$, $k = \dim \mathcal{C}$
  Define $Z_{\mathcal{C}}(x, y) = \sum_{A \subset [n]} x^{k - \rho A} y^{|A| - \rho A}$. Then

  $$Z_{\mathcal{C}}(x, y) = Z_{\mathcal{C}^{\text{(dual)}}}(y, x)$$

  $Z_{\mathcal{C}}(x, y)$ is the Whitney rank-nullity function of $\mathcal{C}$

- $$B_{\mathcal{C}}(x, y) = (x - y)^k y^{n-k} Z_{\mathcal{C}}\left(\frac{qy}{x - y}, \frac{x - y}{y}\right) \quad \text{(Greene 1976)}$$

- This connection extends to *higher support weights* (B ’97) (Wei ’91, Ozarow-Wyner ’84).

Linear codes and duality

The MacWilliams Theorem:

- Linear algebraic approach:
  Let $A \subset \{1, 2, \ldots, n\}$, $\rho A = \mathrm{rank}(G(A))$, $k = \dim \mathcal{C}$
  Define $Z_{\mathcal{C}}(x, y) = \sum_{A \subset [n]} x^{k-\rho A} y^{|A|-\rho A}$. Then

  $$Z_{\mathcal{C}}(x, y) = Z_{\mathcal{C}^{\text{(dual)}}}(y, x)$$

  $Z_{\mathcal{C}}(x, y)$ is the Whitney rank-nullity function of $\mathcal{C}$

- $$B_{\mathcal{C}}(x, y) = (x-y)^k y^{n-k} Z_{\mathcal{C}}\left(\frac{qy}{x-y}, \frac{x-y}{y}\right) \quad \text{(Greene 1976)}$$

- This connection extends to *higher support weights* (B '97) (Wei '91, Ozarow-Wyner '84).

- Codes and matroids: If the code is considered as an F_q-representation of a matroid $\mathcal{M}$ on the set $\{1, 2, \ldots, n\}$, then $Z_{\mathcal{C}}(x, y)$ is the Whitney function of $\mathcal{M}$

Orthogonal arrays

Consider a code $\mathcal{C}$, and suppose that

$$d(\mathcal{C}^{\text{(dual)}}) = t + 1, \text{ i.e., } B_i^{\text{(dual)}} = 0, i = 1, 2, \ldots, t$$

Then $\mathcal{C}$ is called an orthogonal array of strength t (C. R. Rao, 1946+)

Orthogonal arrays

Consider a code $\mathcal{C}$, and suppose that

$$d(\mathcal{C}^{(\text{dual})}) = t+1, \text{ i.e., } B_i^{(\text{dual})} = 0, i = 1, 2, \ldots, t$$

Then $\mathcal{C}$ is called an orthogonal array of strength t (C. R. Rao, 1946+)

$$OA(8,4,1,3): \quad \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix}$$

Orthogonal arrays

Consider a code $\mathcal{C}$, and suppose that

$$d(\mathcal{C}^{\text{(dual)}}) = t + 1, \text{ i.e., } B_i^{\text{(dual)}} = 0, i = 1, 2, \ldots, t$$

Then $\mathcal{C}$ is called an orthogonal array of strength t (C. R. Rao, 1946+)

$$OA(8,4,1,3): \quad \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array}$$

OAs form an example of designs in association schemes (Delsarte '73)

Distances for codes

Different applications of codes give rise to various distance-like functions:

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance
- Lee distance

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance
- Lee distance
- Levenshtein (edit) distance

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance
- Lee distance
- Levenshtein (edit) distance
- ℓ_1 distance; Kendall tau metric; Chebyshev (ℓ_∞) distance

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance
- Lee distance
- Levenshtein (edit) distance
- ℓ_1 distance; Kendall tau metric; Chebyshev (ℓ_∞) distance
- Subspace distance

Distances for codes

Different applications of codes give rise to various distance-like functions:

- Hamming distance
- Lee distance
- Levenshtein (edit) distance
- ℓ_1 distance; Kendall tau metric; Chebyshev (ℓ_∞) distance
- Subspace distance
- Ordered metrics

  (Niederreiter '92; Brualdi et al., '95; Rosenbloom-Tsfasman, '97)

M.Deza and E. Deza, Encyclopedia of distances, Springer 2013

II. Ordered metrics: Motivation

- Universally optimal codes for slow-fading MIMO channels
- Multiplicity codes
- Approximation theory
- Algebraic list decoding
- Linear complexity of sequences

Ordered metrics

Slow-fading point-to-point MIMO channel (Tavildar-Viswanath, ’06)

Ordered metrics

Slow-fading point-to-point MIMO channel (Tavildar-Viswanath, '06)

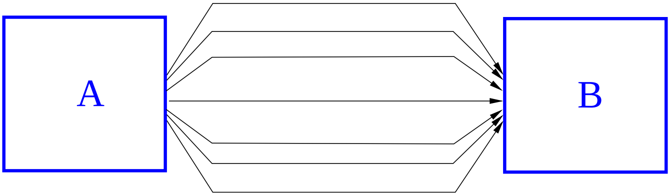
$$y[m] = Hx[m] + w[m]$$

Ordered metrics

Slow-fading point-to-point MIMO channel (Tavildar-Viswanath, ’06)

Parallel fading channel with r diversity branches

$$y_j[m] = h_j x_j[m] + w_j[m], \quad j = 1, \ldots, r$$

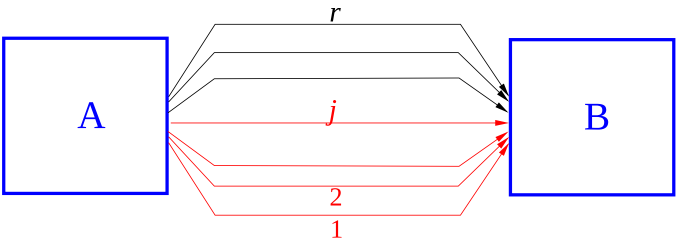


Ordered metrics

Slow-fading point-to-point MIMO channel (Tavildar-Viswanath, '06)

Parallel fading channel with r diversity branches

$$y_j[m] = h_j x_j[m] + w_j[m], \quad j = 1, \ldots, r$$



Universally decodable matrices (see also Ganesan-Vontobel, '07)

RS codes

RS codes: Take n distinct points $a_1, a_2, \ldots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

RS codes

RS codes: Take n distinct points $a_1, a_2, \ldots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

Define

$$\mathcal{C}' = \{(f'(a_1), f(a_1); f'(a_2), f(a_2); \ldots; f'(a_n), f(a_n)), \deg f \leqslant k-1\}$$

RS codes

RS codes: Take n distinct points $a_1, a_2, \ldots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

Or even

$$\mathcal{C}'' = \{(f''(a_1), f'(a_1), f(a_1); f''(a_2), f'(a_2), f(a_2); \ldots; f''(a_n), f'(a_n), f(a_n))\}$$

RS codes

RS codes: Take n distinct points $a_1, a_2, \dots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

Multiplicity codes:

$$\mathcal{C}'' = \{(\overbrace{f''(a_1), f'(a_1), f(a_1)}; \overbrace{f''(a_2), f'(a_2), f(a_2)}; \dots; \overbrace{f''(a_n), f'(a_n), f(a_n)})\}$$

RS codes

RS codes: Take n distinct points $a_1, a_2, \ldots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

Multiplicity codes:

$$\mathcal{C}'' = \{(\overbrace{f''(a_1), f'(a_1), f(a_1)}; \overbrace{f''(a_2), f'(a_2), f(a_2)}; \ldots; \overbrace{f''(a_n), f'(a_n), f(a_n)})\}$$

If $f'(a_1) = f(a_1) = 0$, then a_1 contributes 2 to the count of zeros. Thus what matters is the location of the rightmost nonzero entry in each block of r coordinates (Rosenbloom-Tsfasman, '97)

RS codes

RS codes: Take n distinct points $a_1, a_2, \ldots, a_n \in F_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), f \in F_q[x], \deg f \leqslant k-1\}$$

$\sharp$(zeros)$\leqslant k-1$, so $d(\mathcal{C}) \geqslant n-(k-1)$

Multiplicity codes:

$$\mathcal{C}'' = \{(\overbrace{f''(a_1), f'(a_1), f(a_1)}; \overbrace{f''(a_2), f'(a_2), f(a_2)}; \ldots; \overbrace{f''(a_n), f'(a_n), f(a_n)})\}$$

If $f'(a_1) = f(a_1) = 0$, then a_1 contributes 2 to the count of zeros. Thus what matters is the location of the rightmost nonzero entry in each block of r coordinates (Rosenbloom-Tsfasman, '97)

Extension to RM codes: Kopparty-Saraf-Yekhanin '11; Kopparty '14

NRT metric

$$
\begin{array}{c|cccc|}
 & & & r & \\
\hline
 & 0 & a & 0 & 0 \\
 & a & 0 & b & 0 \\
 & c & c & 0 & 0 \\
n & 0 & 0 & 0 & 0 \\
 & 0 & 0 & 0 & 0 \\
 & d & 0 & 0 & e \\
\hline
\end{array}
$$

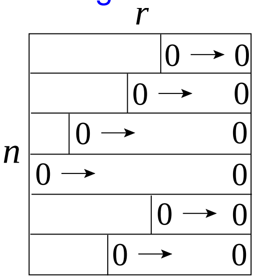
$$w_{NRT}(x) = 2 + 3 + 2 + 4 = 11$$

NRT metric

$$x = \overbrace{\boxed{0011011\color{red}{1}}00000}^{r}$$

Define $w_r(x) = \min\{i : x_{i+1} = \cdots = x_r = 0\}$

Extending to n consecutive blocks of r elements: $x \in F^N, N = nr$



$$w_r(x) \triangleq \sum_{i=1}^{n} \min(j : x_{i,j+1} = \cdots = x_{i,r} = 0)$$

(Niederreiter ’87-’91; Rosenbloom-Tsfasman ’97)

Approximation theory

Monte-Carlo integration: Let $K_n := [0,1]^n$, approximate

$$\int_{K_n} f(x)dx \approx \frac{1}{|P|} \sum_{x_i \in P} f(x_i)$$

for a well-chosen finite set of points P.

Approximation theory

Monte-Carlo integration: Let $K_n := [0,1]^n$, approximate

$$\int_{K_n} f(x)dx \approx \frac{1}{|P|}\sum_{x_i \in P} f(x_i)$$

for a well-chosen finite set of points P.

A set of points $P \in K_n$ is (approximately) uniformly distributed if the *discrepancy*

$$D(P,R) := \max_{R\in\mathscr{R}} \left(\text{vol}\,(R) - \frac{|P\cap R|}{|P|}\right)$$

is small for all R in some class $\mathscr{R}$ of subsets of K_n (Weyl 1916; Van der Corput '42)

Approximation theory

Monte-Carlo integration: Let $K_n := [0,1]^n$, approximate

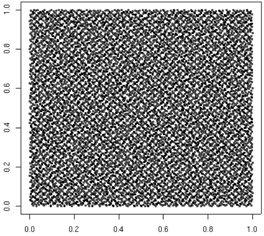
$$\int_{K_n} f(x)dx \approx \frac{1}{|P|} \sum_{x_i \in P} f(x_i)$$

for a well-chosen finite set of points P.

A set of points $P \in K_n$ is (approximately) uniformly distributed if the *discrepancy*

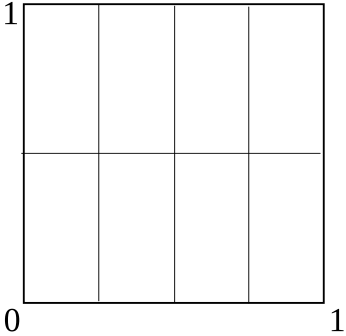
$$D(P,R) := \max_{R \in \mathscr{R}} \left(\text{vol}\,(R) - \frac{|P \cap R|}{|P|} \right)$$

is small for all R in some class $\mathscr{R}$ of subsets of K_n (Weyl 1916; Van der Corput '42)

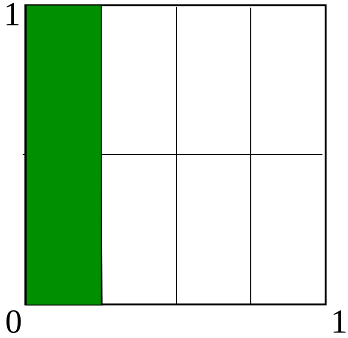


Approximation theory

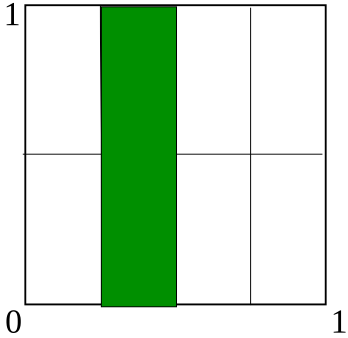
Take $\mathscr{R}$ to be the set of “elementary intervals” (axes-parallel rectanges)



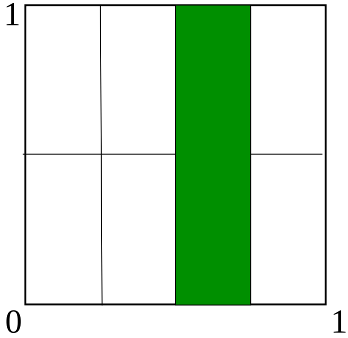
(t, m, n)-nets



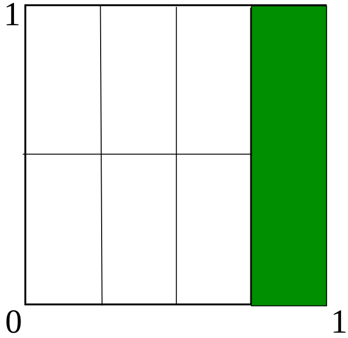
(t, m, n)-nets



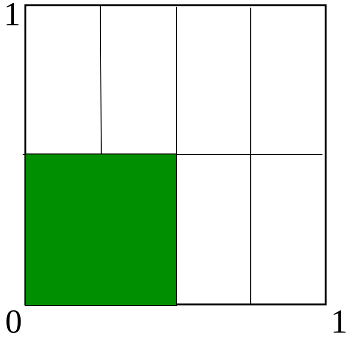
(t, m, n)-nets



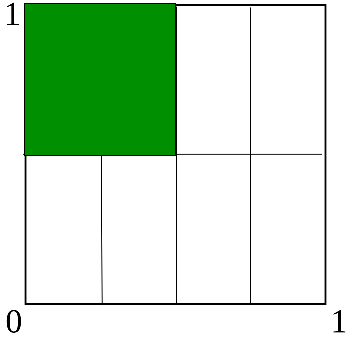
(t, m, n)-nets



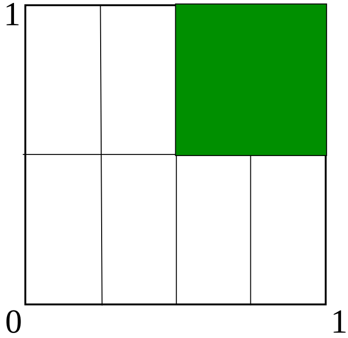
(t, m, n)-nets



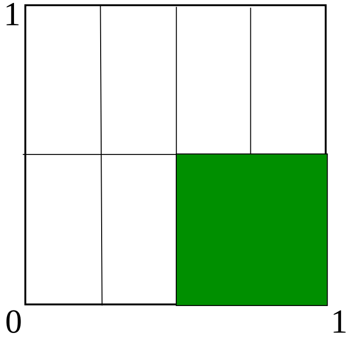
(t, m, n)-nets



(t, m, n)-nets



(t, m, n)-nets



(t, m, n)-nets

Definition

A net is a finite set of points such that every rectangle of some fixed volume contains the same number of points.

For $q \in \mathbb{N}$ consider an elementary interval of the form

$$J = \prod_{i=1}^{n} \left[\frac{a_i}{q^{d_i}}, \frac{a_{i+1}}{q^{d_i}} \right), \quad 0 \leqslant a_i < q^{d_i}$$

(t,m,n)-nets

Definition

A net is a finite set of points such that every rectangle of some fixed volume contains the same number of points.

For $q \in \mathbb{N}$ consider an elementary interval of the form

$$J = \prod_{i=1}^{n} \left[\frac{a_i}{q^{d_i}}, \frac{a_{i+1}}{q^{d_i}} \right), \quad 0 \leqslant a_i < q^{d_i}$$

A set P of size $|P| = q^m$ forms a (t,m,n)-net in K_n if for every J, vol $(J) = q^{t-m}$

$$|P \cap J| = q^t$$

(t, m, n)-nets and ordered metrics

Theorem (Lawrence '96; Mullen-Schmid '96)

There exists a (t, m, n)-net in $[0, 1]^n$ if and only if there exists a q-ary code of length $N = n(m - t)$ with dual NRT distance $m - t + 1$ (i.e., an orthogonal array of strength $m - t$).

(t, m, n)-nets and ordered metrics

Theorem (Lawrence '96; Mullen-Schmid '96)

There exists a (t, m, n)-net in $[0, 1]^n$ if and only if there exists a q-ary code of length $N = n(m - t)$ with dual NRT distance $m - t + 1$ (i.e., an orthogonal array of strength $m - t$).

See also

M. Skriganov, Coding theory and uniform distributions, 1999

Other applications

- List decoding of algebraic codes (Nielsen ’99; Guruswami-Wang ’13)
- Linear complexity of sequences (Massey-Serconek, CRYPTO ’94)

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson '99 B.-Purkayastha '09,'10; B.-Firer '14

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson '99
	B.-Purkayastha '09,'10; B.-Firer '14
Duality of codes	Hyun-Kim 2006-10; B-Firer '13-'14

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson '99
	B.-Purkayastha '09,'10; B.-Firer '14
Duality of codes	Hyun-Kim 2006-10; B-Firer '13-'14
Channel models; polar codes	B.-Park 2010-15
	B.-Park '13; Gulcu-Ye-B. '16

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson '99 B.-Purkayastha '09,'10; B.-Firer '14
Duality of codes	Hyun-Kim 2006-10; B-Firer '13-'14
Channel models; polar codes	B.-Park 2010-15 B.-Park '13; Gulcu-Ye-B. '16
Combinatorics of the ordered space	Martin-Stinson '99; B.-Purkayastha '09

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson ’99
	B.-Purkayastha ’09,’10; B.-Firer ’14
Duality of codes	Hyun-Kim 2006-10; B-Firer ’13-’14
Channel models; polar codes	B.-Park 2010-15
	B.-Park ’13; Gulcu-Ye-B. ’16
Combinatorics of the ordered space	Martin-Stinson ’99; B.-Purkayastha ’09
Linear codes and matroids	B.-Park ’10-’15

A theory of ordered codes

Code $\mathcal{C} \subset F_q^N, N = nr$; for instance, a linear code

Weight (distance) distribution	Martin-Stinson ’99 B.-Purkayastha ’09,’10; B.-Firer ’14
Duality of codes	Hyun-Kim 2006-10; B-Firer ’13-’14
Channel models; polar codes	B.-Park 2010-15 B.-Park ’13; Gulcu-Ye-B. ’16
Combinatorics of the ordered space	Martin-Stinson ’99; B.-Purkayastha ’09
Linear codes and matroids	B.-Park ’10-’15
Infinite orders	B.-Skriganov, ’15

Weight distribution

Consider a pair of dual linear codes $\mathcal{C}, \mathcal{C}^{\text{(dual)}} \in F_q^N, N = nr$

The NRT weight of x equals the sum of the ordered weights of the segments:

$$w(x) = \sum_{i=1}^{n} w(x_i), \text{where } x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,r})$$

The minimum (NRT) distance $d(\mathcal{C}) = \min_{x \in \mathcal{C} \setminus \{0\}} w(x)$

Weight distribution

Consider a pair of dual linear codes $\mathcal{C}, \mathcal{C}^{\text{(dual)}} \in F_q^N, N = nr$

The NRT weight of x equals the sum of the ordered weights of the segments:

$$w(x) = \sum_{i=1}^{n} w(x_i), \text{where } x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,r})$$

The minimum (NRT) distance $d(\mathcal{C}) = \min_{x \in \mathcal{C} \setminus \{0\}} w(x)$

Studies of bounds on codes in terms of $d(\mathcal{C})$

Weight distribution

Consider a pair of dual linear codes $\mathcal{C}, \mathcal{C}^{\text{(dual)}} \in F_q^N, N = nr$

The NRT weight of x equals the sum of the ordered weights of the segments:

$$w(x) = \sum_{i=1}^{n} w(x_i), \text{where } x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,r})$$

The minimum (NRT) distance $d(\mathcal{C}) = \min_{x \in \mathcal{C} \setminus \{0\}} w(x)$

Studies of bounds on codes in terms of $d(\mathcal{C})$

At the same time, the MacWilliams theorem for the weight distributions of $\mathcal{C}, \mathcal{C}^{\text{(dual)}}$ does not hold: The dual weight distribution is not uniquely determined by the weight distribution of the code $\mathcal{C}$

Weight distribution

What is the "correct" definition? Criteria:

- It is a figure of merit for MAP decoding on some relevant channel model
- It supports a MacWilliams-like theorem for a pair of dual codes

MacWilliams theorem

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\mathrm{shape}(x) = (e_0, e_1, \ldots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \ldots, r.$$

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\text{shape}(x) = (e_0, e_1, \dots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \dots, r.$$

$$\begin{array}{cc} & r \\ n & \begin{array}{|c|c|c|c|} \hline 0 & a & 0 & 0 \\ \hline a & 0 & b & 0 \\ \hline c & c & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline d & 0 & 0 & e \\ \hline \end{array} \end{array}$$

$$\text{shape}(x) = (2, 0, 2, 1, 1)$$

MacWilliams theorem

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\text{shape}(x) = (e_0, e_1, \dots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \dots, r.$$

Reasons:

MacWilliams theorem

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\mathrm{shape}(x) = (e_0, e_1, \ldots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \ldots, r.$$

Reasons:

- The group of linear isometries ***acts transitively*** on shape-spheres

$$S_e := \{x \in F_q^n : \mathrm{shape}(x) = e\} \quad e = (e_0, e_1, \ldots, e_r)$$

and shape is the *most coarse invariant* with this property.

MacWilliams theorem

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\text{shape}(x) = (e_0, e_1, \dots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \dots, r.$$

Reasons:

- The group of linear isometries ***acts transitively*** on shape-spheres

$$S_e := \{x \in F_q^n : \text{shape}(x) = e\} \quad e = (e_0, e_1, \dots, e_r)$$

  and shape is the *most coarse invariant* with this property.
- The set of pairs $(x, y) \in (F_q^N)^2$ forms a translation association scheme with classes indexed by the shapes (Martin-Stinson '99; B.-Purkayastha '09)

MacWilliams theorem

Answer in terms of Delsarte's association schemes:

The "correct" invariant of the NRT space is the shape of the vector

$$\mathrm{shape}(x) = (e_0, e_1, \dots, e_r), \text{ where } e_k = \sharp\{i : w(x_i) = k\}, k = 0, 1, \dots, r.$$

Reasons:

- The group of linear isometries ***acts transitively*** on shape-spheres

$$S_e := \{x \in F_q^n : \mathrm{shape}(x) = e\} \quad e = (e_0, e_1, \dots, e_r)$$

  and shape is the *most coarse invariant* with this property.
- The set of pairs $(x, y) \in (F_q^N)^2$ forms a translation association scheme with classes indexed by the shapes (Martin-Stinson '99; B.-Purkayastha '09)
- There are natural channel models for which shapes form sufficient statistics

Linear isometries of the NRT space

Group of linear isometries of the NRT space was found by K. Lee, '03

$$GL(\mathcal{H}_{r,n}) = (T_r)^n \rtimes S_n$$

where $T_r = \begin{bmatrix} * & & & \\ & * & & \\ & & * & \\ & 0 & & \ddots \\ & & & & * \end{bmatrix}$

is the group of upper-triangular matrices with nonzero diagonal

MacWilliams theorem

$$B(z_0, z_1, \dots, z_r) = \sum_{e \in \Delta_{r,n}} \mathcal{B}_e {z_0}^{e_0} {z_1}^{e_1} \dots {z_r}^{e_r},$$

Theorem (Martin-Stinson '99; Skriganov '99)

Let $\mathcal{C}, \mathcal{C}^{(dual)} \subset F_q^N$ be a pair dual linear codes in the ordered Hamming space. Then

$$B^{(dual)}(u_0, u_1, \dots, u_r) = \frac{1}{|\mathcal{C}|} B(z_0, z_1, \dots, z_r)$$

where

$$z_0 = u_0 + (q-1) \sum_{i=1}^{r} q^{i-1} u_i,$$

$$z_{r-j+1} = u_0 + (q-1) \sum_{i=1}^{j-1} q^{i-1} u_k - q^{j-1} u_j, \quad 1 \leqslant j \leqslant r.$$

Implications: Bounds on codes

It is possible to relate the shape distributions of $\mathcal{C}$ and $\mathcal{C}^{\text{(dual)}}$:

Implications: Bounds on codes

It is possible to relate the shape distributions of $\mathcal{C}$ and $\mathcal{C}^{\text{(dual)}}$:

$$B_e = \frac{1}{\left|\mathcal{C}^{\text{(dual)}}\right|} \sum_{f \in \Delta_{n,r}} B_f^{\text{(dual)}} K_e(f), \quad e \in \Delta_{n,r}$$

$(K_e(f))$ - r-variate discrete polynomials orthogonal w.r.t. a multinomial distribution (eigenvalues of the ordered Hamming scheme)

Implications: Bounds on codes

It is possible to relate the shape distributions of $\mathcal{C}$ and $\mathcal{C}^{\text{(dual)}}$:

$$B_e = \frac{1}{|\mathcal{C}^{\text{(dual)}}|} \sum_{f \in \Delta_{n,r}} B_f^{\text{(dual)}} K_e(f), \quad e \in \Delta_{n,r}$$

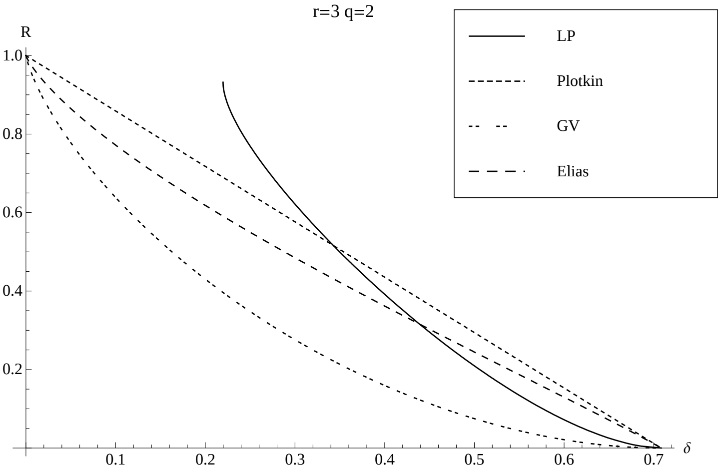
$(K_e(f))$ - r-variate discrete polynomials orthogonal w.r.t. a multinomial distribution (eigenvalues of the ordered Hamming scheme)

Linear programming bounds on the size of codes

Plotkin bound (Bierbrauer '07)

Elias bound; MRRW bound; asymptotics (B.-Purkayastha '09)

Computing the bounds: Rate vs relative distance



Linear-algebraic perspective

Linear-algebraic perspective

Ordered matroids (Faigle, ’80; Wild, ’08)

Linear-algebraic perspective

Ordered matroids (Faigle, ’80; Wild, ’08)

The NRT case is realtively simple: Define independent sets in accordance with the ordering (ideals of the poset)

Linear-algebraic perspective

Ordered matroids (Faigle, '80; Wild, '08)

The NRT case is realtively simple: Define independent sets in accordance with the ordering (ideals of the poset)

Multivariate rank-nullity function:

Let $x, y = (y_1, \ldots, y_r)$ be a set of variables; define

$$Z(x,y) = \sum_{e \in \Delta_{r,n}} \sum_{\substack{I \in \mathcal{I}(P) \\ \mathrm{shape}(I)=e}} \left\{ (x-1)^{\rho E - \rho I} (y_r - 1)^{|I| - \rho I} \prod_{i=1}^{r-1} (y_i - 1)^{e_i} \right\}.$$

Theorem: $Z_{\mathcal{C}^{\text{(dual)}}}(x, y_1, \ldots, y_r) = Z_{\mathcal{C}}(y_r, y_{r-1}, \ldots, y_1, x)$

Linear-algebraic perspective

Ordered matroids (Faigle, '80; Wild, '08)

The NRT case is realtively simple: Define independent sets in accordance with the ordering (ideals of the poset)

Multivariate rank-nullity function:

Let $x, y = (y_1, \ldots, y_r)$ be a set of variables; define

$$Z(x, y) = \sum_{e \in \Delta_{r,n}} \sum_{\substack{I \in \mathcal{I}(P) \\ \mathrm{shape}(I) = e}} \left\{ (x-1)^{\rho E - \rho I} (y_r - 1)^{|I| - \rho I} \prod_{i=1}^{r-1} (y_i - 1)^{e_i} \right\}.$$

Theorem: $Z_{\mathcal{C}^{\text{(dual)}}}(x, y_1, \ldots, y_r) = Z_{\mathcal{C}}(y_r, y_{r-1}, \ldots, y_1, x)$

This theorem implies a linear-algebraic proof of the MacWilliams theorem

Linear-algebraic perspective

Ordered matroids (Faigle, '80; Wild, '08)

The NRT case is realtively simple: Define independent sets in accordance with the ordering (ideals of the poset)

Multivariate rank-nullity function:

Let $x, y = (y_1, \ldots, y_r)$ be a set of variables; define

$$Z(x,y) = \sum_{e \in \Delta_{r,n}} \sum_{\substack{I \in \mathcal{I}(P) \\ \text{shape}(I)=e}} \left\{ (x-1)^{\rho E - \rho I} (y_r - 1)^{|I| - \rho I} \prod_{i=1}^{r-1} (y_i - 1)^{e_i} \right\}.$$

Theorem: $Z_{\mathcal{C}^{\text{(dual)}}}(x, y_1, \ldots, y_r) = Z_{\mathcal{C}}(y_r, y_{r-1}, \ldots, y_1, x)$

(Work with Woomyoung Park, 2010-15)

A. Sokal, Multivariate Tutte polynomial '05; work with A. Ashikhmin on "Binomial moments" '99

Duality of linear codes

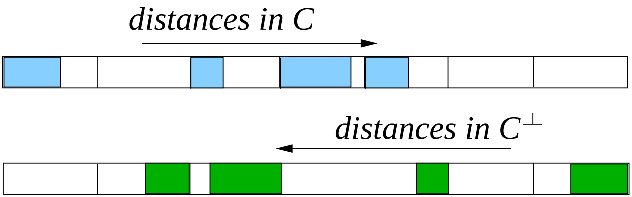
The dual code

$$\mathcal{C}^{\text{(dual)}} = \{y \in F^N : \forall_{x \in \mathcal{C}} (x, y) = 0\}$$

Duality of linear codes

The dual code

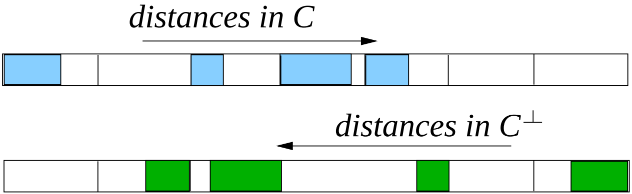
$$\mathcal{C}^{\text{(dual)}} = \{y \in F^N : \forall_{x \in \mathcal{C}} (x, y) = 0\}$$



Duality of linear codes

The dual code

$$\mathcal{C}^{(\text{dual})} = \{y \in F^N : \forall_{x \in \mathcal{C}} (x, y) = 0\}$$

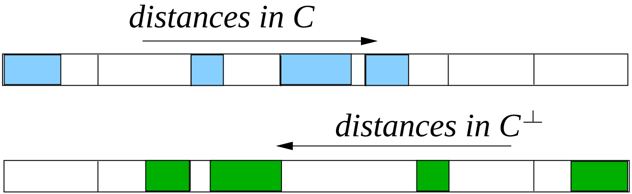


Why are the distances in $\mathcal{C}^{(\text{dual})}$ measured differently than in $\mathcal{C}$?

Duality of linear codes

The dual code

$$\mathcal{C}^{\text{(dual)}} = \{y \in F^N : \forall_{x \in \mathcal{C}} (x, y) = 0\}$$



Why are the distances in $\mathcal{C}^{\text{(dual)}}$ measured differently than in $\mathcal{C}$?

The distances are governed by the combinatorial structure of the space F^N.

Linear-algebraic duality preserves the group but not the association scheme. In other words, $\mathcal{C}$ and $\mathcal{C}^{\text{(dual)}}$ live in different metric spaces (i.e., the metric structure is a priori different)

Metrics generated by partial orders

Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$

Metrics generated by partial orders

Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$

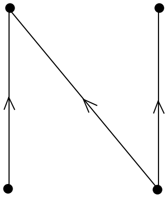
Metrics generated by partial orders

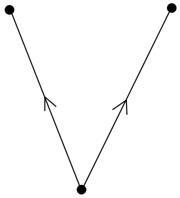
Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$





Metrics generated by partial orders

Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$

$\mathcal{P}$ is called ***self-dual*** if $\mathcal{P} \cong \mathcal{P}^{\text{(dual)}}$

Metrics generated by partial orders

Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

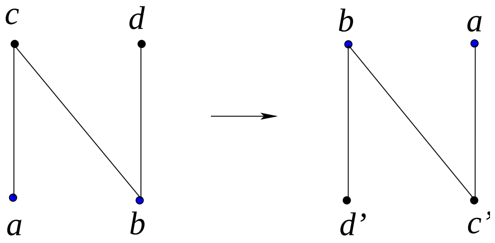
Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$

$\mathcal{P}$ is called ***self-dual*** if $\mathcal{P} \cong \mathcal{P}^{\text{(dual)}}$

Self-dual poset:



Metrics generated by partial orders

Let $\mathcal{P}$ be a partial order on F^N. An ideal in $\mathcal{P}$ is a subset of $[N]$ such that $i \in I$ and $j \prec i$ imply that $j \in I$.

Poset weight of $x \in \mathcal{P}$ (Brualdi et al., '95)

$$w_{\mathcal{P}}(x) = |I|, \text{ where } I \text{ is the smallest ideal s.t. } \operatorname{supp}(x) \subset I$$

Dual order $\mathcal{P}^{\text{(dual)}}$: $i \prec j$ in $\mathcal{P}^{\text{(dual)}}$ iff $j \prec i$ in $\mathcal{P}$

$\mathcal{P}$ is called ***self-dual*** if $\mathcal{P} \cong \mathcal{P}^{\text{(dual)}}$

Theorem (with M. Firer, L. Felix, M. Spreafico '14)

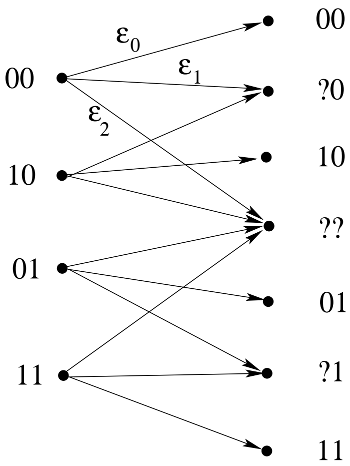
The dual code of $\mathcal{C}$ agrees with $\mathcal{P}^{\text{(dual)}}$ if and only if $\mathcal{P}$ is self-dual.

(proof uses the language of association schemes)

Simple channel models I

Ordered erasure channel

$W : \mathcal{X} \to \mathcal{Y},\ |\mathcal{X}| = 4, |\mathcal{Y}| = 7$



Possible error events:

- Correct transmission
- 1st bit erased
- Both bits erased

Simple channel models II

Definition (Ordered symmetric channel)

Let $\epsilon = (\epsilon_0, \epsilon_1, \ldots, \epsilon_r)$, where $0 \leqslant \epsilon_i \leqslant 1$ for all i and $\sum_i \epsilon_i = 1$. Let $W_r : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = |\mathcal{Y}| = q^r$ be a memoryless vector channel defined by

$$W_r(y|x) = \frac{\epsilon_i}{q^{i-1}(q-1)}, \quad \text{where } d_P(x,y) = i, 1 \leqslant i \leqslant r,$$

and $W_r(y|x) = \epsilon_0$ if $y = x$.

Simple channel models II

Definition (Ordered symmetric channel)

Let $\epsilon = (\epsilon_0, \epsilon_1, \ldots, \epsilon_r)$, where $0 \leqslant \epsilon_i \leqslant 1$ for all i and $\sum_i \epsilon_i = 1$. Let $W_r : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = |\mathcal{Y}| = q^r$ be a memoryless vector channel defined by

$$W_r(y|x) = \frac{\epsilon_i}{q^{i-1}(q-1)}, \quad \text{where } d_P(x,y) = i, 1 \leqslant i \leqslant r,$$

and $W_r(y|x) = \epsilon_0$ if $y = x$.

(*Probability of error events is monotone according to the shapes of the error vectors*)

Simple channel models II

Definition (Ordered symmetric channel)

Let $\epsilon = (\epsilon_0, \epsilon_1, \ldots, \epsilon_r)$, where $0 \leqslant \epsilon_i \leqslant 1$ for all i and $\sum_i \epsilon_i = 1$. Let $W_r : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = |\mathcal{Y}| = q^r$ be a memoryless vector channel defined by

$$W_r(y|x) = \frac{\epsilon_i}{q^{i-1}(q-1)}, \quad \text{where } d_P(x,y) = i, 1 \leqslant i \leqslant r,$$

and $W_r(y|x) = \epsilon_0$ if $y = x$.

(*Probability of error events is monotone according to the shapes of the error vectors*)

Extension: Ordered wiretap channels (connection to higher ordered weights of linear codes)

Simple channel models II

Definition (Ordered symmetric channel)

Let $\epsilon = (\epsilon_0, \epsilon_1, \dots, \epsilon_r)$, where $0 \leqslant \epsilon_i \leqslant 1$ for all i and $\sum_i \epsilon_i = 1$. Let $W_r : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = |\mathcal{Y}| = q^r$ be a memoryless vector channel defined by

$$W_r(y|x) = \frac{\epsilon_i}{q^{i-1}(q-1)}, \quad \text{where } d_P(x,y) = i, 1 \leqslant i \leqslant r,$$

and $W_r(y|x) = \epsilon_0$ if $y = x$.

(*Probability of error events is monotone according to the shapes of the error vectors*)

Extension: Ordered wiretap channels (connection to higher ordered weights of linear codes)

(works with W. Park (2011-'15), P. Purkayastha (2010))

Nonbinary polar codes: Multilevel polarization

Let $W : \mathcal{X} \to \mathcal{Y}$, $|\mathcal{X}| = 2^r$. Consider the polarizing transform given by

$$[x_1, x_2] = [u_1, u_2] \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Nonbinary polar codes: Multilevel polarization

Let $W : \mathcal{X} \to \mathcal{Y}$, $|\mathcal{X}| = 2^r$. Consider the polarizing transform given by

$$[x_1, x_2] = [u_1, u_2] \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Convergence to $r + 1$ levels supported by monotone behavior of the subchannels: If the ith bit in the symbol $x \in \mathcal{X}$ is decoded reliably, then all the bits $x_{i+1}, \dots, x_r$ are also decoded reliably.

Nonbinary polar codes: Multilevel polarization

Let $W : \mathcal{X} \to \mathcal{Y}$, $|\mathcal{X}| = 2^r$. Consider the polarizing transform given by

$$[x_1, x_2] = [u_1, u_2] \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Convergence to $r+1$ levels supported by monotone behavior of the subchannels: If the ith bit in the symbol $x \in \mathcal{X}$ is decoded reliably, then all the bits $x_{i+1}, \ldots, x_r$ are also decoded reliably.

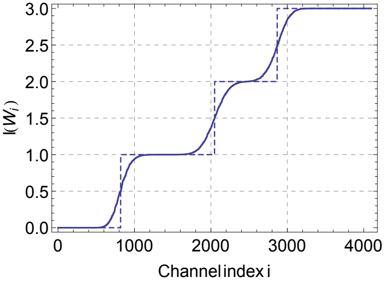
$$Z_v(W) := \frac{1}{2^r} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x)W(y|x')}; \quad Z_i(W) := \frac{1}{2^{i-1}} \sum_{v \in \mathcal{X}_i} Z_v(W)$$

Extremal configurations are of the form:

$$(Z_{1,\infty} = 1, Z_{2,\infty} = 1, \ldots, Z_{j-1,\infty} = 1, Z_{j,\infty} = 0, \ldots, Z_{r,\infty} = 0)$$

Polar codes on ordered channels

Example for the ordered erasure channel (work with W. Park, 2013)



Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \cdots \succ n \succ \dots$

$$x = (x_1, x_2, \dots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \cdots \succ n \succ \dots$

$$x = (x_1, x_2, \dots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

- Group X: $X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_m \supset \dots, \quad \bigcap_{i \geqslant 0} X_i = \{0\}$

Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \cdots \succ n \succ \ldots$

$$x = (x_1, x_2, \ldots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

- Group X: $X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_m \supset \ldots, \quad \bigcap_{i \geqslant 0} X_i = \{0\}$
- Metric $\rho(x) = \max\{j \in \mathbb{N}_0 : x \in X_j\}$, i.e., $x_1 = \cdots = x_{j-1} = 0$

Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \cdots \succ n \succ \dots$

$$x = (x_1, x_2, \dots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

- Group X: $X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_m \supset \dots, \quad \bigcap_{i \geqslant 0} X_i = \{0\}$
- Metric $\rho(x) = \max\{j \in \mathbb{N}_0 : x \in X_j\}$, i.e., $x_1 = \cdots = x_{j-1} = 0$
- Adjacency operators A_i on $L_2(X, \mu) : A_i f(x) = \int_X \chi_i(x - y) f(y) d\mu(y)$

Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \dots \succ n \succ \dots$

$$x = (x_1, x_2, \dots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

- Group X: $X = X_0 \supset X_1 \supset X_2 \supset \dots \supset X_m \supset \dots, \quad \bigcap_{i \geqslant 0} X_i = \{0\}$
- Metric $\rho(x) = \max\{j \in \mathbb{N}_0 : x \in X_j\}$, i.e., $x_1 = \dots = x_{j-1} = 0$
- Adjacency operators A_i on $L_2(X, \mu) : A_i f(x) = \int_X \chi_i(x - y) f(y) d\mu(y)$

Extensions - An infinite order?

Consider a total order given by a single chain: $1 \succ 2 \succ 3 \succ \cdots \succ n \succ \dots$

$$x = (x_1, x_2, \dots) \in \prod_{i \geqslant 1} \mathbb{Z}_p^+$$

- Group X: $X = X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_m \supset \dots, \quad \bigcap_{i \geqslant 0} X_i = \{0\}$
- Metric $\rho(x) = \max\{j \in \mathbb{N}_0 : x \in X_j\}$, i.e., $x_1 = \cdots = x_{j-1} = 0$
- Adjacency operators A_i on $L_2(X, \mu) : A_i f(x) = \int_X \chi_i(x - y) f(y) d\mu(y)$
- Eigenvalues of $\{A_i\} \Leftrightarrow$ functions on X with properties of MRA on $L_2(X, \mu)$

Extending Delsarte's theory of Abelian association schemes to infinite spaces (work with Maksim Skriganov, '15)

References

J. Bierbrauer, A direct approach to linear programmming bounds on codes and (t,m,s)-nets, *Designs, Codes and Cryptography* **42**, no. 2 (2007), pp. 127–143.

A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer, 1989.

P. Delsarte, *An algebraic approach to the association schemes of coding theory*, 1973.

D. S. Kim and H. K. Kim, Duality of translation association schemes coming from certain actions, ArXiv:1108.4947, 2011.

W. J. Martin and D. R. Stinson, Association schemes for ordered orthogonal arrays and (T,M,S)-nets, *Canad. J. Math.* **51**, no.2 (1999), pp. 325–346.

H. Niederreiter, A combinatorial problem for vector spaces over finite fields, *Discrete Math.* **96**, no. 3 (1991), pp. 221–228.

M. Rosenbloom and M. A. Tsfasman, Codes for the m-metric, *Probl. Inform. Trans.*, **33** no. 1 (1997), pp. 45–52.

M. Skriganov, Coding theory and uniform distributions, *St. Petersburg Math. Journal* **13** no. 2 (2002), pp. 191-239.

Talk based on joint works with:

Punarbasu Purkayastha

1. Bounds for ordered codes and orthogonal arrays, *Moscow Mathematical Journal*, **9**, no. 2 (2009), 211–243.
2. Near MDS poset codes and distributions, in *Error-Correcting Codes, Cryptography and Finite Geometries*, Amer. Math. Soc., Providence, RI, 2010, pp. 135–147.

Woomyoung Park

1. Polar codes for q-ary channels, $q = 2^r$, *IEEE Trans. Inform. Theory*, **59**, no. 2, '13.
2. On linear ordered codes, *Moscow Mathematical Journal* **15**, no. 4 (2015), pp. 679–702.

Luciano Felix, Marcelo Firer, and Marcos Spreafico

1. Linear codes on posets with extension property, *Discrete Mathematics* **317** (2014)

Maksim Skriganov

1. Association schemes on general measure spaces and zero-dimensional Abelian groups, *Advances in Mathematics* **281** (2015), pp. 142–247.

Talha Gulcu and Min Ye, Construction of nonbinary polar codes, this ISIT.

Talk based on joint works with:

Punarbasu Purkayastha

1. Bounds for ordered codes and orthogonal arrays, *Moscow Mathematical Journal*, **9**, no. 2 (2009), 211–243.
2. Near MDS poset codes and distributions, in *Error-Correcting Codes, Cryptography and Finite Geometries*, Amer. Math. Soc., Providence, RI, 2010, pp. 135–147.

Woomyoung Park

1. Polar codes for q-ary channels, $q = 2^r$, *IEEE Trans. Inform. Theory*, **59**, no. 2, '13.
2. On linear ordered codes, *Moscow Mathematical Journal* **15**, no. 4 (2015), pp. 679–702.

Luciano Felix, Marcelo Firer, and Marcos Spreafico

1. Linear codes on posets with extension property, *Discrete Mathematics* **317** (2014)

Maksim Skriganov

1. Association schemes on general measure spaces and zero-dimensional Abelian groups, *Advances in Mathematics* **281** (2015), pp. 142–247.

Talha Gulcu and Min Ye, Construction of nonbinary polar codes, this ISIT.

Thank you!