# Ordered linear codes

Alexander Barg

Dept of ECE/Inst. for Systems Research
University of Maryland, College Park, MD 20742

April 10, 2013

# Longer Reed-Solomon codes

Recall RS codes: Fix $a_1, a_2, \ldots, a_n \in \mathbb{F}_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), \deg f \leq k-1\}$$

$\#$(zeros)$\leq (k-1)$, so $d(\mathcal{C}) \geq n-(k-1)$

# Longer Reed-Solomon codes

Recall RS codes: Fix $a_1, a_2, \ldots, a_n \in \mathbb{F}_q$

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), \deg f \leq k-1\}$$

$\#$(zeros)$\leq (k-1)$, so $d(\mathcal{C}) \geq n - (k-1)$

Define

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

# Longer Reed-Solomon codes

Recall RS codes:

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), \deg f \le k-1\}$$

$\#$(zeros)$\le (k-1)$, so $d(\mathcal{C}) \ge n-(k-1)$

Or even

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

# Longer Reed-Solomon codes

Recall RS codes:

$$\mathcal{C} = \{(f(a_1), f(a_2), ..., f(a_n)), \deg f \leq k-1\}$$

$\#$(zeros)$\leq (k-1)$, so $d(\mathcal{C}) \geq n-(k-1)$

Or even

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

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 coordinates.

# Ordered Hamming metric

$$x = (x_{1,1}, \ldots, x_{1,r}; x_{2,1}, \ldots, x_{2,r}; \ldots; x_{n,1}, \ldots, x_{n,r})$$

### Definition

$$w(x) = \sum_{i=1}^{n} \max(j : \; x_{i,j+1} = \cdots = x_{i,r} = 0)$$

Rosenbloom-Tsfasman (1997)

# Ordered Hamming metric

$$x = (x_{1,1}, \ldots, x_{1,r}; x_{2,1}, \ldots, x_{2,r}; \ldots; x_{n,1}, \ldots, x_{n,r})$$

### Definition

$$w(x) = \sum_{i=1}^{n} \max(j : \; x_{i,j+1} = \cdots = x_{i,r} = 0)$$

Rosenbloom-Tsfasman (1997)

Niederreiter (1988-92) considered the problem of constructing low-discrepancy point sets in $[0,1]^n$. The discrepancy (proximity to the uniform distribution) is controlled by the dual distance of codes with respect to the ordered Hamming metric.

# Ordered Hamming metric

$$x = (x_{1,1}, \dots, x_{1,r}; x_{2,1}, \dots, x_{2,r}; \dots; x_{n,1}, \dots, x_{n,r})$$

**Definition**

$$w(x) = \sum_{i=1}^{n} \max(j : \; x_{i,j+1} = \dots = x_{i,r} = 0)$$

Rosenbloom-Tsfasman (1997)

Niederreiter (1988-92) considered the problem of constructing low-discrepancy point sets in $[0,1]^n$. The discrepancy (proximity to the uniform distribution) is controlled by the dual distance of codes with respect to the ordered Hamming metric.

NRT metric space

# Poset metrics

Let $\mathcal{P}([\![n]\!], \preceq)$ be a poset on $[\![n]\!] := \{1, \ldots, n\}$

# Poset metrics

Let $\mathcal{P}([\![n]\!], \preceq)$ be a poset on $[\![n]\!] := \{1, \ldots, n\}$

Ideal $I \subset [\![n]\!]$ : ($i \in I$ and $j \prec i$) imply that $j \in I$.

# Poset metrics

Let $\mathcal{P}([\![n]\!], \preceq)$ be a poset on $[\![n]\!] := \{1, \ldots, n\}$

Ideal $I \subset [\![n]\!]$ : ($i \in I$ and $j \prec i$) imply that $j \in I$.

Let $x \in \mathbb{F}_q^n$; $\mathrm{supp}(x) := \{i \in [\![n]\!] : x_i \neq 0\}$;
$\langle x \rangle$ := smallest ideal of $\mathcal{P}$ that contains $\mathrm{supp}(x)$

# Poset metrics

Let $\mathcal{P}(\llbracket n \rrbracket, \preceq)$ be a poset on $\llbracket n \rrbracket := \{1, \ldots, n\}$

Ideal $I \subset \llbracket n \rrbracket$ : ($i \in I$ and $j \prec i$) imply that $j \in I$.

Let $x \in \mathbb{F}_q^n$; $\mathrm{supp}(x) := \{i \in \llbracket n \rrbracket : x_i \neq 0\}$;
$\langle x \rangle$ := smallest ideal of $\mathcal{P}$ that contains supp($x$)

**Definition (poset norm; Brualdi et al. '95)**

$w_{\mathcal{P}}(x) := |\langle x \rangle|$; $d(x, y) = \mathrm{w}_{\mathcal{P}}(x - y)$

# Poset metrics

Let $\mathcal{P}([\![n]\!], \preceq)$ be a poset on $[\![n]\!] := \{1, \dots, n\}$

Ideal $I \subset [\![n]\!]$ : ($i \in I$ and $j \prec i$) imply that $j \in I$.

Let $x \in \mathbb{F}_q^n$; $\mathrm{supp}(x) := \{i \in [\![n]\!] : x_i \neq 0\}$;
$\langle x \rangle$ := smallest ideal of $\mathcal{P}$ that contains $\mathrm{supp}(x)$

**Definition (poset norm; Brualdi et al. '95)**

$w_{\mathcal{P}}(x) := |\langle x \rangle|$; $d(x, y) = \mathrm{w}_{\mathcal{P}}(x - y)$

Proof: $w_{\mathcal{P}}(x + y) \le |\langle x \rangle \cup \langle y \rangle| \le |\langle x \rangle| + |\langle y \rangle| = w_{\mathcal{P}}(x) + w_{\mathcal{P}}(y)$

# Examples

1. Antichain = Hamming distance

2. Single chain: $1 \prec 2 \prec \cdots \prec n$

$$w_{\mathcal{P}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ \max(i : x_i \neq 0) & \text{otherwise} \end{cases}$$

$$w_{\mathcal{P}}(x+y) \leq \max(w_{\mathcal{P}}(x), w_{\mathcal{P}}(y))$$

3. NRT metric

4. Hierarchical poset

5. Regular tree

# Linear codes; Weight distributions

A = subspace of linear space $(\mathbb{F}_q)^n$, $\mathbb{F}_q = (\alpha_0, \alpha_1, \ldots, \alpha_{q-1})$

Let $b(w) = |\{x \in A, w_H(x) = w\}|$ = number of vectors of Hamming wt $w$

$$B(z_0, z_1) = \sum_{w=0}^{n} b(w) z_0^{n-w} z_1^{w}$$

# Linear codes; Weight distributions

A = subspace of linear space $(\mathbb{F}_q)^n$, $\mathbb{F}_q = (\alpha_0, \alpha_1, \ldots, \alpha_{q-1})$

Let $b(w) = |\{x \in A, w_H(x) = w\}|$ = number of vectors of Hamming wt $w$

$$B(z_0, z_1) = \sum_{w=0}^{n} b(w) z_0^{n-w} z_1^{w}$$

More detailed view:

Let $\omega = (\omega_0, \omega_1, \ldots, \omega_{q-1})$ be a type vector, $\sum_{i=1}^{q-1} \omega_i = n$
Let $b_\omega = |\{x \in A, \sharp(i : x_i = \alpha_j) = \omega_j\}|$

$$B(z_0, z_1, \ldots, z_q) = \sum_{x \in A} z_0^{\omega_0(x)} z_1^{\omega_1(x)} \ldots z_{q-1}^{\omega_{q-1}(x)} = \sum_{\omega} b(\omega) \boldsymbol{z}^{\omega}$$

# Linear codes; Weight distributions

A = subspace of linear space $(\mathbb{F}_q)^n$, $\mathbb{F}_q = (\alpha_0, \alpha_1, \ldots, \alpha_{q-1})$

Let $b(w) = |\{x \in A, w_H(x) = w\}|$ = number of vectors of Hamming wt $w$

$$B(z_0, z_1) = \sum_{w=0}^{n} b(w) z_0^{n-w} z_1^{w}$$

More detailed view:

Let $\omega = (\omega_0, \omega_1, \ldots, \omega_{q-1})$ be a type vector, $\sum_{i=1}^{q-1} \omega_i = n$

Let $b_\omega = |\{x \in A, \sharp(i : x_i = \alpha_j) = \omega_j\}|$

$$B(z_0, z_1, \ldots, z_q) = \sum_{x \in A} z_0^{\omega_0(x)} z_1^{\omega_1(x)} \ldots z_{q-1}^{\omega_{q-1}(x)} = \sum_{\omega} b(\omega) \boldsymbol{z}^{\omega}$$

Even more detailed: $qn$ variables $z_{ij}$, corresponding to $x_i = \alpha_j$

# Isometry group of the space

Let $d$ be some metric: $d(x, y) = |(x - y)|$
Isometry $g : X \to X$ such that $d(x, y) = d(gx, gy)$

Isometries of the Hamming space: permutations $\sigma$, replacement of coordinates: $d((0, 1, 1), (2, 1, 2)) = d((2, 0, 0), (1, 0, 1))$

$G =$(Compositions of permutations $S_n$ and replacements $S_q$)$= S_q \wr S_n$
Action of $G$ on $X = \mathbb{F}_q^n$ is transitive: $\forall x, y \;\; \exists g \in G$ such that $gx = y$

# Isometry group of the space

Let $d$ be some metric: $d(x, y) = |(x - y)|$
Isometry $g : X \to X$ such that $d(x, y) = d(gx, gy)$

Isometries of the Hamming space: permutations $\sigma$, replacement of coordinates: $d((0, 1, 1), (2, 1, 2)) = d((2, 0, 0), (1, 0, 1))$

$G =$(Compositions of permutations $S_n$ and replacements $S_q$)$= S_q \wr S_n$
Action of $G$ on $X = \mathbb{F}_q^n$ is transitive: $\forall x, y \;\; \exists g \in G$ such that $gx = y$

Weight $w : x \to \mathbb{N}$ such that $G$ is transitive on spheres around 0:
$S_w(0) = \{x \in X : w(x) \text{ constant}\}$

# Isometry group of the space

Let $d$ be some metric: $d(x, y) = |(x - y)|$
Isometry $g : X \to X$ such that $d(x, y) = d(gx, gy)$

Isometries of the Hamming space: permutations $\sigma$, replacement of coordinates: $d((0,1,1),(2,1,2)) = d((2,0,0),(1,0,1))$

$G =$(Compositions of permutations $S_n$ and replacements $S_q$)$= S_q \wr S_n$
Action of $G$ on $X = \mathbb{F}_q^n$ is transitive: $\forall x, y \ \ \exists g \in G$ such that $gx = y$

Weight $w : x \to \mathbb{N}$ such that $G$ is transitive on spheres around 0:
$S_w(0) = \{x \in X : w(x) \text{ constant}\}$

Examples:
$G$ – Hamming weights
$S_n$ – types
$\{id\}$ – exact weight enumerator

# Weight-like functions (Inner distributions)

**Definition**

Let $(\mathbb{F}_q^n, \mathcal{P})$ be a poset metric space. A mapping $s : \mathbb{F}_q^n \to \mathbb{Z}^m$ is called a shape mapping if it is constant on the orbits of $T \in GL_{\mathcal{P}}(n)$. The value that this maping takes on the orbit of a vector $x \in \mathbb{F}_q^n$ is called the shape of $x$.

# Inner distribution; NRT space

Let $X = \mathbb{F}_q^r$, $1 \prec 2 \prec \cdots \prec r$ (a chain).

$$|x| = \max(i : x_{i+1} = \cdots = x_r = 0); d_{\mathcal{P}}(x, y) = |x - y|$$

$\mathcal{B} < GL(q, r)$ group of upper triangular $r \times r$ matrices with nonzero main diagonal

# Inner distribution; NRT space

Let $X = \mathbb{F}_q^r$, $1 \prec 2 \prec \cdots \prec r$ (a chain).

$$|x| = \max(i : x_{i+1} = \cdots = x_r = 0); d_{\mathcal{P}}(x,y) = |x-y|$$

$\mathcal{B} < GL(q,r)$ group of upper triangular $r \times r$ matrices with nonzero main diagonal

$G$=(permutations of chains ($S_n$) and action of $\mathcal{B}$ on each chain)

Orbits are formed of vectors with $e_1$ chains of weight 1, $e_2$ chains of weight 2,..., $e_r$ chains of weight $r$; all $e = (e_0, e_1, \ldots, e_r)$ that partition $n$

Shape distribution of the code $A$:

$$B_A(z_0, z_1, \ldots, z_r) = \sum_e b(e) z_0^{e_0} z_2^{e_1} \ldots z_r^{e_r}$$

Martin and Stinson, '99; Skriganov '98

# MacWilliams equations for shape distributions

**Theorem** (Martin-Stinson '99, Bierbrauer '07, B.-Purkayastha '09, Park-B. '10)

*Let $A \subset \mathbb{F}_q^n$ and $A^\perp$ be its dual code. Then*

$$B_{A^\perp}(u_0, u_1, \ldots, u_r) = \frac{1}{|A|} B_A(z_0, z_1, \ldots, z_r)$$

*where*

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

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

# MacWilliams equations for shape distributions

**Theorem** (Martin-Stinson '99, Bierbrauer '07, B.-Purkayastha '09, Park-B. '10)

*Let $A \subset \mathbb{F}_q^n$ and $A^\perp$ be its dual code. Then*

$$B_{A^\perp}(u_0, u_1, \dots, u_r) = \frac{1}{|A|} B_A(z_0, z_1, \dots, z_r)$$

*where*

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

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

Remarks. 1. MacWilliams equation for weights does not hold.
2. The shapes in the dual code $A^\perp$ are measured from the opposite side (e.g., from the right).

# Krawtchouk polynomials

Let $C, C^{\perp}$ be a pair of dual linear codes

Classically,

$$b^{\perp}(w) = \frac{1}{|C|}\sum_{k=0}^{n} b(k)K_w(k), \quad w = 0, 1, \ldots, n$$

where $(K_k(\cdot))$ is the family of discrete orthogonal polynomials on $\{0, 1, \ldots, n\}$ with weight $\binom{n}{i}(q-1)^i/q^n$.

# Krawtchouk polynomials

Let $C, C^\perp$ be a pair of dual linear codes

Classically,

$$b^\perp(w) = \frac{1}{|C|}\sum_{k=0}^{n} b(k)K_w(k), \quad w = 0, 1, \dots, n$$

where $(K_k(\cdot))$ is the family of discrete orthogonal polynomials on $\{0, 1, \dots, n\}$ with weight $\binom{n}{i}(q-1)^i/q^n$.

The NRT case: For every shape $e$

$$b^\perp(e) = \frac{1}{|C|}\sum_f b(f)K_e(f)$$

$(K_f(e) = K_{f_1,\dots,f_r}(e_1, \dots, e_r))$ discrete orthogonal polynomials of $r$ variables

(orthogonal on the set of shapes (partitions) with weight $\binom{n}{e_1,\dots,e_r}\prod_{i=0}^{r}(q^{i-r-1}(q-1))^{e_i}$.)

# Krawtchouk polynomials

Let $C, C^\perp$ be a pair of dual linear codes

Classically,

$$b^\perp(w) = \frac{1}{|C|}\sum_{k=0}^{n} b(k)K_w(k), \quad w = 0, 1, \dots, n$$

where $(K_k(\cdot))$ is the family of discrete orthogonal polynomials on $\{0, 1, \dots, n\}$ with weight $\binom{n}{i}(q-1)^i/q^n$.

The NRT case: For every shape $e$

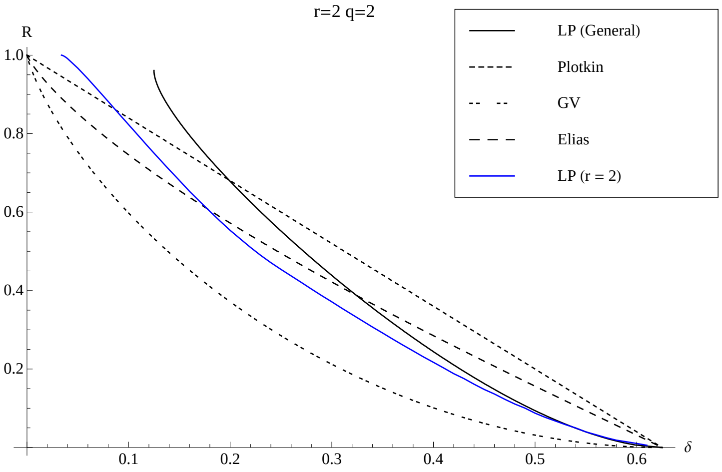
$$b^\perp(e) = \tfrac{1}{|C|}\textstyle\sum_f b(f)K_e(f)$$

$(K_f(e) = K_{f_1,\dots,f_r}(e_1, \dots, e_r))$ discrete orthogonal polynomials of $r$ variables

(orthogonal on the set of shapes (partitions) with weight $\binom{n}{e_1,\dots,e_r}\prod_{i=0}^{r}(q^{i-r-1}(q-1))^{e_i}$.)

Use Delsarte's theory to set up a Linear Programming Bound on codes

# Bounds on codes




Work with Punarbasu Purkayastha, [1]

# MacWilliams equations for shape distributions

Linear-algebraic approach (with Woomyoung Park, [3]).

# MacWilliams equations for shape distributions

1. Recall the Hamming case (MacWilliams): Define the *rank function* of an $[n, k]$ linear code $\mathcal{C}$

$$Z_{\mathcal{C}}(x, y) = \sum_{u=0}^{n} \sum_{v=0}^{k} R_u^v x^y y^v$$

where $R_u^v = |\{F \subset [\![n]\!] : |F| = u, \operatorname{rank}(G(F)) = v\}|$. Define the Tutte polynomial by

$$T_{\mathcal{C}}(x, y) = Z_{\mathcal{C}}(x - 1, y - 1)$$

Then

$$T_{\mathcal{C}}(x, y) = T_{\mathcal{C}^\perp}(y, x)$$

Greene's theorem:

$$A(x, y) = y^{n-k}(x - y)^k T_{\mathcal{C}}\Big(\frac{x + (q - 1)y}{x - y}, \frac{x}{y}\Big)$$

# MacWilliams equations for shape distributions

2. The ordered Hamming (NRT) space:

The multivariate Tutte polynomial of $\mathcal{C}$:

$$Z(q, \boldsymbol{z}) = \sum_{e} \sum_{\substack{A \in \mathcal{I}(P) \\ \text{shape}(A)=e}} q^{-\rho A} \prod_{i=1}^{r} z_i^{e_i}, \text{ where } \boldsymbol{z} = (z_1, z_2, \ldots, z_r)$$

Lemma:

$$Z^{\perp}(q, z_1, z_2, \ldots, z_r) = q^{\rho E - nr} z_r^n Z\left(q, \frac{qz_{r-1}}{z_r}, \frac{q^2 z_{r-2}}{z_r}, \ldots, \frac{q^{r-1} z_1}{z_r}, \frac{q^r}{z_r}\right).$$

A different form of this relation: introduce the shape-rank distribution of a code

$$R_e^v \triangleq |\{A \in \mathcal{I}(P) : \text{shape}(A) = e, \text{rank}(G(A)) = v\}|.$$

$$Z(y^{-1}, \boldsymbol{z}) = \sum_{e} \sum_{v=0}^{k} R_e^v {z_1}^{e_1} {z_2}^{e_2} \ldots {z_r}^{e_r} y^v.$$

# MacWilliams equations for shape distributions

Introduce the Tutte polynomial of a linear code:

$$T(x, \boldsymbol{y}) \triangleq \sum_{e} \sum_{\substack{A \in \mathcal{I}(P) \\ \text{shape}(A) = e}} (x-1)^{\rho(E)-\rho(A)} (y_1 - 1)^{e_1} \times \dots$$
$$\times (y_{r-1} - 1)^{e_{r-1}} (y_r - 1)^{|A| - \rho(A)}.$$

Lemma:

$$T^{\perp}(x, y_1, \dots, y_r) = T(y_r, y_{r-1}, \dots, y_1, x).$$

# Extensions

## $t$th Generalized Poset Distance [2,3]

$$d_t(C) = \min\{|\langle D\rangle| : D \text{ is an } [n,t] \text{ subcode of } C\}$$

$$A^j(I) = |\{D : D \subseteq C, \dim(D) = j, \langle D\rangle = I\}|$$

$$D^m(I) = \sum_{u=0}^{m}\left[\prod_{i=0}^{u-1}(q^m - q^i)\right]A^u(I), \quad m \geq 0$$

$$D_e^m = \sum_{I:\text{shape}(I)=e} D^m(I)$$

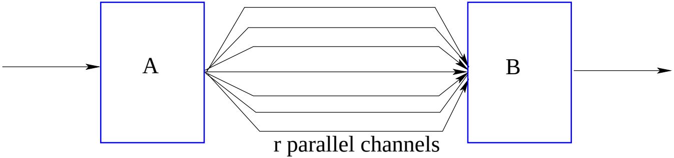
$$D^m(z_0, z_1, \ldots, z_r) = \sum_e D_e^m z_0^{e_0} \ldots z_r^{e_r}, \quad m \geq 0.$$

### Theorem

$$D^m(z_0, z_1, \ldots, z_r) = q^{mk} {z_r}^n Z\left(q^m, \frac{z_{r-1} - z_r}{z_r}, \frac{z_{r-2} - z_{r-1}}{z_r}, \ldots, \frac{z_0 - z_1}{z_r}\right)$$

# Transmission over channels

S. Tavildar and P. Viswanath (2006) considered a wireless transmission system with fading



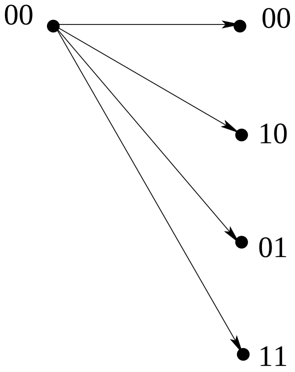

Transmission goes over $r$ parallel channels with increasing SNR; the channels are subordinated so that if transmission over channel $i$ is lost, then so are transmissions over channels $1, \ldots, i-1$.
NRT metric emerges as figure of merit (A. Ganesan and P. Vontobel)

# Ordered symmetric channel

Transmit pairs of bits (r=2)

# Ordered symmetric channel

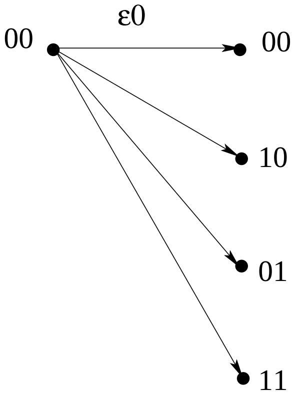
Transmit pairs of bits (r=2)



# Ordered symmetric channel

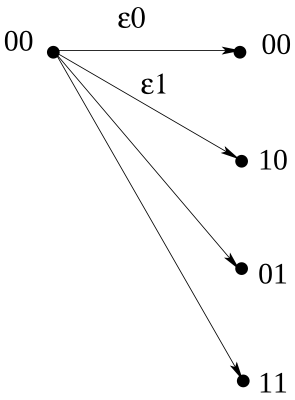
Transmit pairs of bits (r=2)

- Correct transmission



# Ordered symmetric channel

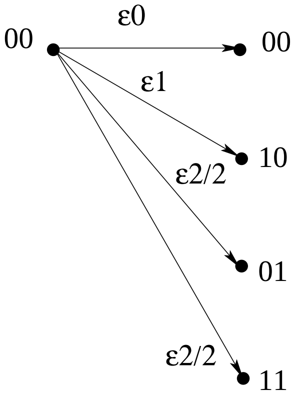
Transmit pairs of bits (r=2)




- Correct transmission
- Error 1 $\epsilon_0 > \epsilon_1$

# Ordered symmetric channel

Transmit pairs of bits (r=2)




- Correct transmission
- Error 1 $\epsilon_0 > \epsilon_1$
- Error 2: no information about 1st bit $\epsilon_1 > \epsilon_2/2$

# Ordered symmetric channel: General definition

## Definition

Let $\epsilon = (\epsilon_0, \epsilon_1, \ldots, \epsilon_r)$, where $0 \le \epsilon_i \le 1$ for all $i$ and $\sum_i \epsilon_i = 1$. Let $W_r : \mathbb{F}_q^r \to \mathbb{F}_q^r$ be a memoryless vector channel defined by

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

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

# Ordered symmetric channel: Properties

Let shape$(y) = e = (e_1, e_2, \ldots, e_r)$, where $e_i$ is the number of blocks of ordered weight $i$

$$W_r(y|\mathbf{0}) = \epsilon_0^{e_0}\left(\frac{\epsilon_1}{q-1}\right)^{e_1}\cdots\left(\frac{\epsilon_r}{q^{r-1}(q-1)}\right)^{e_r}$$
$$= \frac{\epsilon_0^{e_0}}{q^{\mathrm{w}_P(y)}}\prod_{i=1}^{r}\left(\frac{q\epsilon_i}{q-1}\right)^{e_i}.$$

Link to Arikan's polar codes (W. Park & AB, [6])

# Ordered symmetric channel: Properties

Assume that

$$\epsilon_0 > \frac{\epsilon_1}{q-1} > \cdots > \frac{\epsilon_r}{q^{r-1}(q-1)}$$

## Proposition

*The capacity of $W_r(\epsilon)$ equals*

$$\mathscr{C}(W_r(\epsilon)) = r(1 - h_{q,r}(\epsilon)),$$

*where*

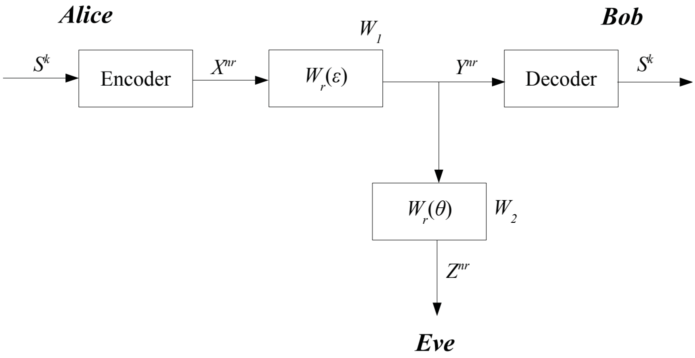
$$h_{q,r}(\epsilon) \triangleq \frac{1}{r}\Big(H_q(\epsilon) + \sum_{i=1}^{r} \epsilon_i \log_q(q^{i-1}(q-1))\Big)$$

*and* $H_q(\epsilon) = -\sum_{i=0}^{r} \epsilon_i \log_q \epsilon_i$.

Recall: If $r = 1$, $\mathcal{C} = 1 + \epsilon \log \frac{\epsilon}{q-1} + (1-\epsilon)\log(1-\epsilon)$

# Extensions

Links to wire-tap channel and polar codes (W.Park - A.B.)




Suppose that transmission between A and B is in fading environment desribed by OSC

Channel to E is also OSC (stochastically degraded)

# Association schemes

$(X, \mathcal{R}), \mathcal{R} = (R_0, R_1, \ldots, R_D)$ is called an association scheme if

- $X \times X = \bigsqcup_{i=0}^{D} R_i$; $R_i$ symmetric; $R_0$ diagonal
- given $x, y \in R_k$, $|\{z \in X : (x,z) \in R_i, (x,y) \in R_j\}|$ is a function of $i, j, k$

Example: $X = \mathbb{F}_q^n, R_i = \{(x,y) \in X^2 : d_H(x,y) = i\}, i = 0, 1, \ldots, n$

# Association schemes

$(X, \mathcal{R}), \mathcal{R} = (R_0, R_1, \dots, R_D)$ is called an association scheme if

- $X \times X = \bigsqcup_{i=0}^{D} R_i$; $R_i$ symmetric; $R_0$ diagonal
- given $x, y \in R_k$, $|\{z \in X : (x, z) \in R_i, (x, y) \in R_j\}|$ is a function of $i, j, k$

Example: $X = \mathbb{F}_q^n, R_i = \{(x, y) \in X^2 : d_H(x, y) = i\}, i = 0, 1, \dots, n$

$\mathcal{A}$ is called a translation association scheme if for all $R \in \mathcal{R}$

$$(x, y) \in R_i \ \Rightarrow \ (x + z, y + z) \in R_i, \quad z \in X.$$

R.C. Bose (1952-59), P. Delsarte (1973), Brouwer, Cohen, Neumaier (1989)

# Duality

Dual code $A^{\perp} = \{y \in X : x \cdot y = 0 \text{ for all } x \in A\}$

# Duality

Dual code $A^{\perp} = \{y \in X : x \cdot y = 0 \text{ for all } x \in A\}$

Dual scheme of a translation scheme $\mathcal{A}$ :

Let $X^* = \{\chi : X \to \mathbb{C}^*\}$ be the group of characters of $X$, $X \cong X^*$

Characters form an association scheme $\mathcal{A}^*$ with relations
$R_i^* = \{(\chi, \psi) : E_i \eta = \eta\}$, where $\eta = \chi^{-1}\psi$.
Generally $\mathcal{A} \ncong \mathcal{A}^*$

Dual code is the subgroup

$$A' = \{\chi \in X^* | \chi(x) = 1 \text{ for all } x \in A\}$$

# Duality

Dual code $A^{\perp} = \{y \in X : x \cdot y = 0 \text{ for all } x \in A\}$

Dual scheme of a translation scheme $\mathcal{A}$ :

Let $X^* = \{\chi : X \to \mathbb{C}^*\}$ be the group of characters of $X$, $X \cong X^*$

Characters form an association scheme $\mathcal{A}^*$ with relations
$R_i^* = \{(\chi, \psi) : E_i \eta = \eta\}$, where $\eta = \chi^{-1}\psi$.
Generally $\mathcal{A} \ncong \mathcal{A}^*$

Dual code is the subgroup

$$A' = \{\chi \in X^* | \chi(x) = 1 \text{ for all } x \in A\}$$

Identifying $X$ and $X^*$ preserves the group, but not the association scheme. In other words, $A$ and $A'$ live in different (metric) spaces (i.e., the metric structures for $A'$ and $A^{\perp}$ are different)

# Association schemes from group action

Let $X = \mathbb{F}_q^n$, $G < GL(q,n)$ a linear group acting on $X$

Example: $G$ is the group of linear isometries for a metric $d$

e.g., for $d_{\text{Hamming}}$, $G = (\mathbb{F}_q^*) \ltimes S_n$

$x, y \in X$ are equivalent, $x \sim y$, if there is $T \in G$ such that $y = Tx$

Let $\mathcal{X} := X/\sim$ be the set of orbits, $|\mathcal{X}| = D + 1$.

Consider the partition $\mathcal{R} = \{R_\alpha | \alpha \in \mathcal{X}\}$ of $X \times X$ given by

$$R_\alpha = \{(x, y) \in X^2 | x - y \in \alpha\}, \quad \alpha \in \mathcal{X}.$$

### Proposition

*The pair $(X, \mathcal{R})$ forms a translation association scheme $\mathcal{A}$ with $D$ classes.*

# Example (W. Martin)

Consider the NRT metric space. Its group of linear isometries:
$G = B_r \wr S_n$ (upper-triangular matrices and permutations)

$\mathcal{A} = (\mathbb{F}_q^{nr}, \mathcal{R} = (R_e))$

$(x, y) \in \mathbb{F}_q^{nr} \times \mathbb{F}_q^{nr}$ is in $R_e$ iff shape$(x - y) = e$.

# Self-dual posets

Under which conditions the orthogonal code is the same as the dual code?

Call $\mathcal{P}^\perp$ a dual poset of $\mathcal{P}$ if $\mathcal{P}^\perp$ is a poset on $[\![n]\!]$ such that if $i \preceq j$ in $\mathcal{P}$ then $i \succeq j$ in $\mathcal{P}^\perp$. Call $\mathcal{P}$ self-dual if $\mathcal{P} \cong \mathcal{P}^\perp$

**Theorem**

*Suppose that $\mathcal{A}$ is a translation association scheme on $X$ whose classes are given by orbits of the group $GL_{\mathcal{P}}(n)$ of linear isometries of a poset metric space $(X, \mathcal{P})$. Then $\mathcal{A}^* \cong \mathcal{A}^\perp$ if and only if $\mathcal{P}$ is self-dual.*

(Work with Marcelo Firer [4])

# Research directions

1. Construct codes for the NRT metric (e.g., what is a good definition of the Hamming code? Simplex code?). See [Rosenbloom and Tsfasman '97], but details are to be filled in.

2. Examples of posets on which shapes are manageable (they are not even on regular trees).

3. If such posets are found, study their association schemes. Do any nice families of polynomials arise?

4. Extend the study of poset association schemes to the case $\{0,1\}^{\mathbb{N}}$.

5. Is there a good concept of ordered matroids (in some special cases) that would connect to poset codes?

# Papers:

[1] A.B. and P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, Moscow Mathematical Journal, vol.9, no. 2, 2009, pp. 211–243.

[2] A. B. and P. Purkayastha, *Near-MDS poset codes and distributions*, in: Error-Correcting Codes, Cryptography and Finite Geometries, AMS CONM, 2010, pp. 135–147.

[3] A. B. and W. Park, *Contributions to the theory of linear poset codes*, manuscript. (preliminary version: Proceedings of 48th Allerton Conference on Communication, Control and Computing, Sept. 29 -Oct. 1, 2010, pp.361–367)

[4] A.B., M. Firer, M.V. Spreafico, and L.V. Felix, *Linear codes on posets with extension property*, arXiv:1304.2263

[5] W. Park, *Applications of ordered weights in information transmission*, Ph. D. thesis, University of Maryland, November 2012, http://drum.lib.umd.edu/handle/1903/13524.

[6] W. Park and AB, *Polar codes for q-ary channels,* $q = 2^r$, IEEE IT Transactions, Feb. 2013.