Codes in classical association schemes

Kai-Uwe Schmidt

Department of Mathematics
Paderborn University
Germany

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m \times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

We will explore:

- Symmetric matrices,

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

We will explore:

- Symmetric matrices,
- Hermitian matrices,

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

We will explore:

- Symmetric matrices,
- Hermitian matrices,
- Alternating matrices,

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

We will explore:

- Symmetric matrices,
- Hermitian matrices,
- Alternating matrices,
- Quadratic forms (or cosets of alternating matrices),

Some motivation

Let Y be a subset of $\mathbb{F}_q^{m\times n}$ such that every nonzero difference has rank at least d.

Singleton bound: $|Y| \leq q^{m(n-d+1)}$ for $m \geq n$.

Proof: Two matrices in Y must differ in any $n-d+1$ columns.

We will explore:

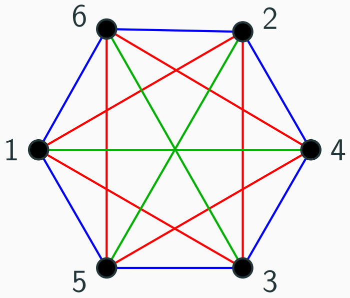
- Symmetric matrices,
- Hermitian matrices,
- Alternating matrices,
- Quadratic forms (or cosets of alternating matrices),
- ...and connections to other objects.

Association schemes

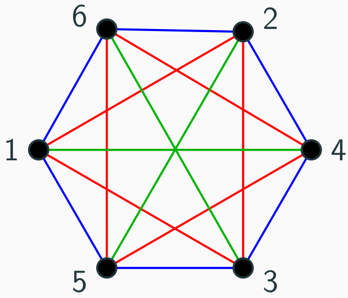
In coding theory and related subjects, an association scheme (such as the Hamming scheme) should mainly be viewed as a "structured space" in which the objects of interest (such as codes, or designs) are living.

— Delsarte & Levenshtein, 1998

A simple example



A simple example

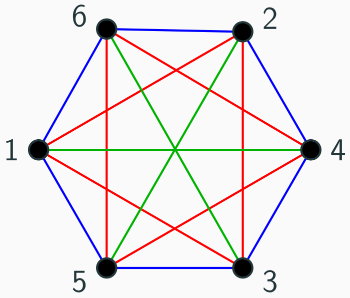


$$D_1 = \begin{pmatrix} 0 & J - I \\ J - I & 0 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} J - I & 0 \\ 0 & J - I \end{pmatrix}$$

$$D_3 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

A simple example



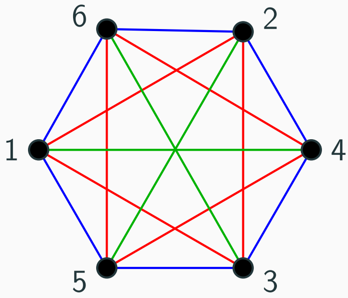
$$D_1 = \begin{pmatrix} 0 & J-I \\ J-I & 0 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} J-I & 0 \\ 0 & J-I \end{pmatrix}$$

$$D_3 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

$$(D_1 D_2)_{x,y} = \#z \text{ with } (D_1)_{x,z} = 1 \text{ and } (D_2)_{z,y} = 1$$

A simple example



$$D_1 = \begin{pmatrix} 0 & J-I \\ J-I & 0 \end{pmatrix}$$

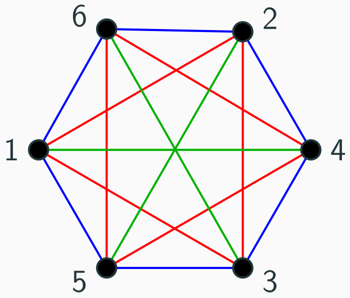
$$D_2 = \begin{pmatrix} J-I & 0 \\ 0 & J-I \end{pmatrix}$$

$$D_3 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

$$(D_1 D_2)_{x,y} = \#z \text{ with } (D_1)_{x,z} = 1 \text{ and } (D_2)_{z,y} = 1$$

$$= \begin{cases} 1 & \text{for } (D_1)_{x,y} = 1 \\ 0 & \text{for } (D_2)_{x,y} = 1 \\ 2 & \text{for } (D_3)_{x,y} = 1 \end{cases}$$

A simple example



$$D_1 = \begin{pmatrix} 0 & J-I \\ J-I & 0 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} J-I & 0 \\ 0 & J-I \end{pmatrix}$$

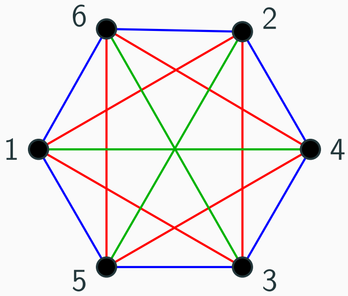
$$D_3 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

$$(D_1 D_2)_{x,y} = \#z \text{ with } (D_1)_{x,z} = 1 \text{ and } (D_2)_{z,y} = 1$$

$$= \begin{cases} 1 & \text{for } (D_1)_{x,y} = 1 \\ 0 & \text{for } (D_2)_{x,y} = 1 \\ 2 & \text{for } (D_3)_{x,y} = 1 \end{cases}$$

$$D_1 D_2 = 1 \cdot D_1 + 0 \cdot D_2 + 2 \cdot D_3$$

A simple example



$$D_1 = \begin{pmatrix} 0 & J - I \\ J - I & 0 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} J - I & 0 \\ 0 & J - I \end{pmatrix}$$

$$D_3 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

The matrices I, D_1, D_2, D_3 generate a commutative algebra:

$$D_1 D_2 = D_2 D_1 = D_1 + 2D_3 \qquad D_1^2 = 2I + D_2$$

$$D_1 D_3 = D_3 D_1 = D_2 \qquad D_2^2 = 2I + D_2$$

$$D_2 D_3 = D_3 D_2 = D_1 \qquad D_3^2 = I$$

(Symmetric) association schemes

Color the complete graph on a vertex set X with n colors and let $D_1, \ldots, D_n$ be the corresponding adjacency matrices.

(Symmetric) association schemes

Color the complete graph on a vertex set X with n colors and let $D_1, \ldots, D_n$ be the corresponding adjacency matrices.

Algebraic definition

The tuple $(D_0 = I, D_1, \ldots, D_n)$ forms an association scheme on X if the vector space generated by $D_0, D_1, \ldots, D_n$ over $\mathbb{R}$ is a (commutative) matrix algebra.

(Symmetric) association schemes

Color the complete graph on a vertex set X with n colors and let $D_1, \ldots, D_n$ be the corresponding adjacency matrices.

Algebraic definition

The tuple $(D_0 = I, D_1, \ldots, D_n)$ forms an association scheme on X if the vector space generated by $D_0, D_1, \ldots, D_n$ over $\mathbb{R}$ is a (commutative) matrix algebra.

This algebra is called the Bose-Mesner algebra.

(Symmetric) association schemes

Color the complete graph on a vertex set X with n colors and let $D_1, \ldots, D_n$ be the corresponding adjacency matrices.

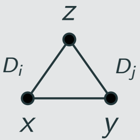
Algebraic definition

The tuple $(D_0 = I, D_1, \ldots, D_n)$ forms an association scheme on X if the vector space generated by $D_0, D_1, \ldots, D_n$ over $\mathbb{R}$ is a (commutative) matrix algebra.

This algebra is called the Bose-Mesner algebra.

Combinatorial definition

The tuple $(D_0 = I, D_1, \ldots, D_n)$ forms an association scheme on X if the number of triangles depends only on the graph containing (x, y).



P- and Q-numbers

Commutativity of the Bose-Mesner algebra implies that all matrices in the algebra can be simultaneoulsy diagonalised.

P- and Q-numbers

Commutativity of the Bose-Mesner algebra implies that all matrices in the algebra can be simultaneoulsy diagonalised.

Hence there exists an idempotent basis $E_0, E_1, \ldots, E_n$:

$$\sum_{k=0}^{n} E_k = I, \qquad E_j E_k = \delta_{jk} E_k.$$

P- and Q-numbers

Commutativity of the Bose-Mesner algebra implies that all matrices in the algebra can be simultaneoulsy diagonalised.

Hence there exists an idempotent basis $E_0, E_1, \ldots, E_n$:

$$\sum_{k=0}^{n} E_k = I, \qquad E_j E_k = \delta_{jk} E_k.$$

Change of basis:

$$D_i = \sum_{k=0}^{n} P_i(k) E_k \qquad |X| \cdot E_k = \sum_{i=0}^{n} Q_k(i) D_i.$$

P- and Q-numbers

Commutativity of the Bose-Mesner algebra implies that all matrices in the algebra can be simultaneoulsy diagonalised.

Hence there exists an idempotent basis $E_0, E_1, \ldots, E_n$:

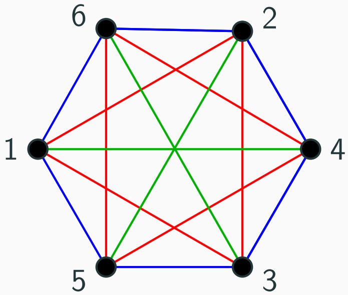
$$\sum_{k=0}^{n} E_k = I, \qquad E_j E_k = \delta_{jk} E_k.$$

Change of basis:

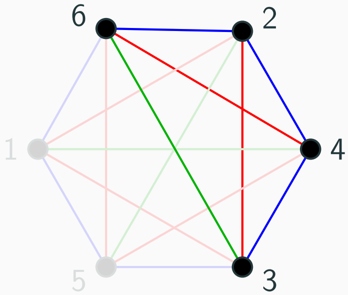
$$D_i = \sum_{k=0}^{n} P_i(k) E_k \qquad |X| \cdot E_k = \sum_{i=0}^{n} Q_k(i) D_i.$$

The number $P_i(k)$ is an eigenvalue of D_i whose eigenspace is the column space of E_k.

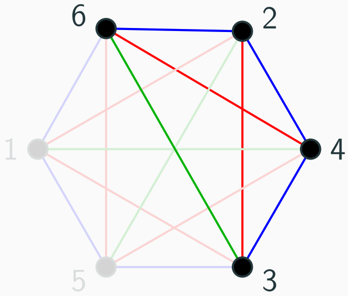
Subsets and inner distribution



Subsets and inner distribution



Subsets and inner distribution



Inner distribution: $\frac{1}{4}(4, 6, 4, 2)^T$.

Subsets and duality

Take a subset Y of the vertex set X with characteristic vector u:

$$u_x = \begin{cases} 1 & \text{for } x \in Y \\ 0 & \text{otherwise.} \end{cases}$$

Subsets and duality

Take a subset Y of the vertex set X with characteristic vector u:

$$u_x = \begin{cases} 1 & \text{for } x \in Y \\ 0 & \text{otherwise.} \end{cases}$$

Inner distribution: $\boldsymbol{a} = (a_i)$, where $a_i = \frac{1}{|Y|} \cdot u^T D_i u$.

Subsets and duality

Take a subset Y of the vertex set X with characteristic vector u:

$$u_x = \begin{cases} 1 & \text{for } x \in Y \\ 0 & \text{otherwise.} \end{cases}$$

Inner distribution: $\boldsymbol{a} = (a_i)$, where $a_i = \frac{1}{|Y|} \cdot u^T D_i u$.

Dual distribution: $\boldsymbol{a}' = Q\boldsymbol{a}$. Then $a'_k = \frac{|X|}{|Y|} \cdot u^T E_k u$.

Subsets and duality

Take a subset Y of the vertex set X with characteristic vector u:

$$u_x = \begin{cases} 1 & \text{for } x \in Y \\ 0 & \text{otherwise.} \end{cases}$$

Inner distribution: $\boldsymbol{a} = (a_i)$, where $a_i = \frac{1}{|Y|} \cdot u^T D_i u$.

Dual distribution: $\boldsymbol{a}' = Q\boldsymbol{a}$. Then $a'_k = \frac{|X|}{|Y|} \cdot u^T E_k u$.

Simple (and important) fact

The entries in the dual distribution are nonnegative.

Subsets and duality

Take a subset Y of the vertex set X with characteristic vector u:

$$u_x = \begin{cases} 1 & \text{for } x \in Y \\ 0 & \text{otherwise.} \end{cases}$$

Inner distribution: $\boldsymbol{a} = (a_i)$, where $a_i = \frac{1}{|Y|} \cdot u^T D_i u$.

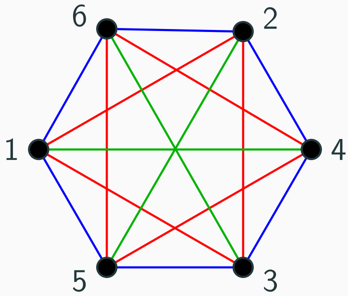
Dual distribution: $\boldsymbol{a}' = Q\boldsymbol{a}$. Then $a'_k = \frac{|X|}{|Y|} \cdot u^T E_k u$.

Simple (and important) fact

The entries in the dual distribution are nonnegative.

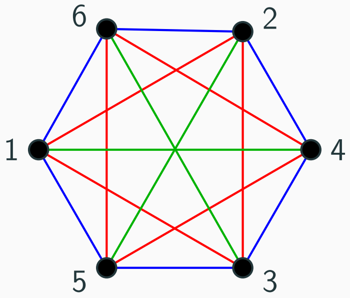
Proof: E_k has eigenvalues 0 or 1, so is positive semidefinite.

A linear program



$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & -1 & -1 & 2 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

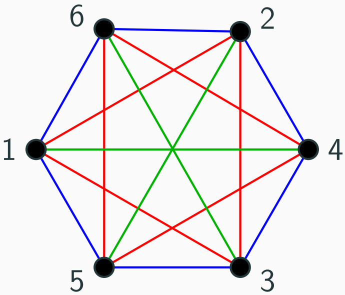
A linear program



$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & -1 & -1 & 2 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

What are the largest independent sets Y in the blue graph?

A linear program



$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & -1 & -1 & 2 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

What are the largest independent sets Y in the blue graph?

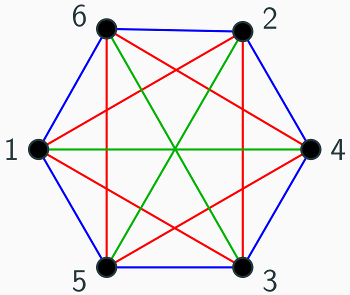
Linear program: Maximize $|Y| = 1 + a_2 + a_3$ subject to

$$2 - a_2 + 2a_3 \geq 0$$

$$2 - a_2 - 2a_3 \geq 0$$

$$1 + a_2 - a_3 \geq 0$$

A linear program



$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & -1 & -1 & 2 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

What are the largest independent sets Y in the blue graph?

Linear program: Maximize $|Y| = 1 + a_2 + a_3$ subject to

$$2 - a_2 + 2a_3 \geq 0$$
$$2 - a_2 - 2a_3 \geq 0$$
$$1 + a_2 - a_3 \geq 0$$

Unique solution: $\boldsymbol{a} = (1, 0, 2, 0)^T$.

Linear programming and duality

Primary LP problem:

Choose $x \in \mathbb{R}^{s\times 1}$ that maximises cx subject to $x \geq 0$, $Ax \geq -b$.

Linear programming and duality

Primary LP problem:

Choose $x \in \mathbb{R}^{s \times 1}$ that maximises cx subject to $x \geq 0$, $Ax \geq -b$.

Dual LP problem:

Choose $y \in \mathbb{R}^{1 \times n}$ that minimises yb subject to $y \geq 0$, $yA \leq -c$.

Linear programming and duality

Primary LP problem:

Choose $x \in \mathbb{R}^{s \times 1}$ that maximises cx subject to $x \geq 0$, $Ax \geq -b$.

Dual LP problem:

Choose $y \in \mathbb{R}^{1 \times n}$ that minimises yb subject to $y \geq 0$, $yA \leq -c$.

Useful facts.

Let x and y be feasible solutions to the primary and dual LP problem, respectively. Then

$$cx \leq -yAx \leq yb.$$

In particular, every feasible solution to the dual problem gives an upper bound for the optimum in the primary problem.

Linear programming and duality

Primary LP problem:

Choose $x \in \mathbb{R}^{s\times 1}$ that maximises cx subject to $x \geq 0$, $Ax \geq -b$.

Dual LP problem:

Choose $y \in \mathbb{R}^{1\times n}$ that minimises yb subject to $y \geq 0$, $yA \leq -c$.

Useful facts.

Let x and y be feasible solutions to the primary and dual LP problem, respectively. Then

$$cx \leq -yAx \leq yb.$$

In particular, every feasible solution to the dual problem gives an upper bound for the optimum in the primary problem.

Moreover, $cx = yb$ if and only if x and y are both optimal solutions.

Translation schemes

Now suppose that the ambient space X has the structure of an abelian group $(X, +)$.

Translation schemes

Now suppose that the ambient space X has the structure of an abelian group $(X, +)$.

An association scheme on X is a translation scheme if there is a partition $X_0, X_1, \ldots, X_n$ of X such that, for every i,

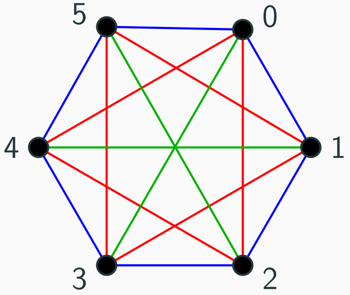
$$(D_i)_{x,y} = 1 \quad \Leftrightarrow \quad x - y \in X_i.$$

Translation schemes

Now suppose that the ambient space X has the structure of an abelian group $(X, +)$.

An association scheme on X is a translation scheme if there is a partition $X_0, X_1, \ldots, X_n$ of X such that, for every i,

$$(D_i)_{x,y} = 1 \quad \Leftrightarrow \quad x - y \in X_i.$$



A translation scheme on $(\mathbb{Z}_6, +)$ with the partition

$X_0 = \{0\}$
$X_1 = \{1, 5\}$
$X_2 = \{2, 4\}$
$X_3 = \{3\}$.

Duality of translation schemes

There is a partition $X'_0, X'_1, \ldots, X'_n$ of the character group X' of X such that

$$\sum_{x \in X_i} x'(x) \quad \text{is constant for all } x' \in X'_k.$$

Duality of translation schemes

There is a partition $X'_0, X'_1, \ldots, X'_n$ of the character group X' of X such that

$$\sum_{x \in X_i} x'(x) \quad \text{is constant for all } x' \in X'_k.$$

This partition defines an association scheme on X', called the dual translation scheme.

Duality of translation schemes

There is a partition $X'_0, X'_1, \ldots, X'_n$ of the character group X' of X such that

$$\sum_{x \in X_i} x'(x) \quad \text{is constant for all } x' \in X'_k.$$

This partition defines an association scheme on X', called the dual translation scheme.

The P- and Q-numbers are given by the character sums

$$P_k(i) = \sum_{x \in X_i} x'(x) \quad \text{for } x' \in X'_k,$$

$$Q_i(k) = \sum_{x' \in X'_k} x'(x) \quad \text{for } x \in X_i.$$

Duality of translation schemes

There is a partition $X'_0, X'_1, \ldots, X'_n$ of the character group X' of X such that

$$\sum_{x \in X_i} x'(x) \quad \text{is constant for all } x' \in X'_k.$$

This partition defines an association scheme on X', called the dual translation scheme.

The P- and Q-numbers are given by the character sums

$$P_k(i) = \sum_{x \in X_i} x'(x) \quad \text{for } x' \in X'_k,$$

$$Q_i(k) = \sum_{x' \in X'_k} x'(x) \quad \text{for } x \in X_i.$$

The role of the P- and the Q-numbers are swapped in the dual translation scheme.

Subsets in translation schemes

A subset Y in a translation scheme on X is additive if $(Y, +)$ is a subgroup of $(X, +)$.

Subsets in translation schemes

A subset Y in a translation scheme on X is additive if $(Y, +)$ is a subgroup of $(X, +)$.

The annihilator of an additive subset Y is

$$Y^\circ = \{x' \in X' : x'(x) = 1 \text{ for all } x \in Y\}.$$

Subsets in translation schemes

A subset Y in a translation scheme on X is additive if $(Y, +)$ is a subgroup of $(X, +)$.

The annihilator of an additive subset Y is

$$Y^\circ = \{x' \in X' : x'(x) = 1 \text{ for all } x \in Y\}.$$

Generalised MacWilliams identities

If Y is an additive subset of X with dual distribution (a'_k), then $(a'_k/|Y|)$ is the inner distribution of Y°.

Subsets in translation schemes

A subset Y in a translation scheme on X is additive if $(Y, +)$ is a subgroup of $(X, +)$.

The annihilator of an additive subset Y is

$$Y^\circ = \{x' \in X' : x'(x) = 1 \text{ for all } x \in Y\}.$$

Generalised MacWilliams identities

If Y is an additive subset of X with dual distribution (a'_k), then $(a'_k/|Y|)$ is the inner distribution of Y°.

For additive subsets Y, we have the divisibility constraints

$$a_i \in \mathbb{Z}, \quad a'_k/|Y| \in \mathbb{Z}.$$

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

Bilinear forms scheme

$\mathrm{Mat}(m, n, q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$.

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

Bilinear forms scheme

$\mathrm{Mat}(m, n, q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$.

Hermitian forms scheme

$\mathrm{Her}(n, q)$ on the set of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$.

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

Bilinear forms scheme

$\mathrm{Mat}(m, n, q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$.

Hermitian forms scheme

$\mathrm{Her}(n, q)$ on the set of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$.

Alternating forms scheme

$\mathrm{Alt}(m, q)$ on the set of $m \times m$ alternating matrices over $\mathbb{F}_q$.

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

Bilinear forms scheme

$\mathrm{Mat}(m, n, q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$.

Hermitian forms scheme

$\mathrm{Her}(n, q)$ on the set of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$.

Alternating forms scheme

$\mathrm{Alt}(m, q)$ on the set of $m \times m$ alternating matrices over $\mathbb{F}_q$.

Two matrices are i-th associates if their difference has rank i (or $2i$ for $\mathrm{Alt}(m, q)$).

q-Hamming schemes

Hamming scheme

$\mathrm{Ham}_t(n)$ on the set of n-tuples over a set of size t.

Two tuples are i-th associates if their Hamming distance is i.

Bilinear forms scheme

$\mathrm{Mat}(m, n, q)$ on the set of $m \times n$ matrices over $\mathbb{F}_q$.

Hermitian forms scheme

$\mathrm{Her}(n, q)$ on the set of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$.

Alternating forms scheme

$\mathrm{Alt}(m, q)$ on the set of $m \times m$ alternating matrices over $\mathbb{F}_q$.

Two matrices are i-th associates if their difference has rank i (or $2i$ for $\mathrm{Alt}(m, q)$).

All are self-dual translation schemes.

P- and Q-numbers

The P- and Q-numbers satisfy a three-term-recurrence, whose solution is determined by generalised Krawtchouk polymials:

$$P_i(k) = Q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} b^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_b \begin{bmatrix} n-i \\ j \end{bmatrix}_b (cb^n)^j,$$

P- and Q-numbers

The P- and Q-numbers satisfy a three-term-recurrence, whose solution is determined by generalised Krawtchouk polymials:

$$P_i(k) = Q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} b^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_b \begin{bmatrix} n-i \\ j \end{bmatrix}_b (cb^n)^j,$$

where

- $b = 1$ and $c = t$ in $\mathrm{Ham}_t(n)$,

P- and Q-numbers

The P- and Q-numbers satisfy a three-term-recurrence, whose solution is determined by generalised Krawtchouk polymials:

$$P_i(k) = Q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} b^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_b \begin{bmatrix} n-i \\ j \end{bmatrix}_b (cb^n)^j,$$

where

- $b = 1$ and $c = t$ in $\mathrm{Ham}_t(n)$,
- $b = q$ and $c = q^{m-n}$ in $\mathrm{Mat}(m, n, q)$, where $m \geq n$ (Delsarte 1978),

P- and Q-numbers

The P- and Q-numbers satisfy a three-term-recurrence, whose solution is determined by generalised Krawtchouk polymials:

$$P_i(k) = Q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} b^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_b \begin{bmatrix} n-i \\ j \end{bmatrix}_b (cb^n)^j,$$

where

- $b = 1$ and $c = t$ in $\mathrm{Ham}_t(n)$,
- $b = q$ and $c = q^{m-n}$ in $\mathrm{Mat}(m, n, q)$, where $m \geq n$ (Delsarte 1978),
- $b = -q$ and $c = -1$ in $\mathrm{Her}(n, q)$ (Carlitz-Hodges 1955, Stanton 1981, S. 2017),

P- and Q-numbers

The P- and Q-numbers satisfy a three-term-recurrence, whose solution is determined by generalised Krawtchouk polymials:

$$P_i(k) = Q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} b^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix}_b \begin{bmatrix} n-i \\ j \end{bmatrix}_b (cb^n)^j,$$

where

- $b = 1$ and $c = t$ in $\mathrm{Ham}_t(n)$,
- $b = q$ and $c = q^{m-n}$ in $\mathrm{Mat}(m, n, q)$, where $m \geq n$ (Delsarte 1978),
- $b = -q$ and $c = -1$ in $\mathrm{Her}(n, q)$ (Carlitz-Hodges 1955, Stanton 1981, S. 2017),
- $b = q^2$ and $c = q$ or $c = 1/q$ and $n = \lfloor m/2 \rfloor$ in $\mathrm{Alt}(m, q)$ (Delsarte-Goethals 1975).

Bounds for d-codes

A subset Y in a q-Hamming scheme is a d-code if all nonzero differences of elements in Y have rank at least d.

Bounds for d-codes

A subset Y in a q-Hamming scheme is a d-code if all nonzero differences of elements in Y have rank at least d.

Theorem (Singleton bound).

If $\begin{bmatrix} k \\ d-1 \end{bmatrix}_b \geq 0$ for all $k \leq n$, then every d-code Y satisfies

$$|Y| \leq (cb^n)^{n-d+1},$$

Bounds for d-codes

A subset Y in a q-Hamming scheme is a d-code if all nonzero differences of elements in Y have rank at least d.

Theorem (Singleton bound).

If $\begin{bmatrix} k \\ d-1 \end{bmatrix}_b \geq 0$ for all $k \leq n$, then every d-code Y satisfies

$$|Y| \leq (cb^n)^{n-d+1},$$

and in case of equality, the inner distribution (a_i) of Y satisfies

$$a_{n-i} = \sum_{j=i}^{n-d} (-1)^{j-i} b^{\binom{j-i}{2}} \begin{bmatrix} j \\ i \end{bmatrix}_b \begin{bmatrix} n \\ j \end{bmatrix}_b ((cb^n)^{n+d-j-1} - 1).$$

Bounds for d-codes

A subset Y in a q-Hamming scheme is a d-code if all nonzero differences of elements in Y have rank at least d.

Theorem (Singleton bound).

If $\begin{bmatrix} k \\ d-1 \end{bmatrix}_b \geq 0$ for all $k \leq n$, then every d-code Y satisfies

$$|Y| \leq (cb^n)^{n-d+1},$$

and in case of equality, the inner distribution (a_i) of Y satisfies

$$a_{n-i} = \sum_{j=i}^{n-d} (-1)^{j-i} b^{\binom{j-i}{2}} \begin{bmatrix} j \\ i \end{bmatrix}_b \begin{bmatrix} n \\ j \end{bmatrix}_b ((cb^n)^{n+d-j-1} - 1).$$

If the condition does not hold, then the bound still holds for additive codes.

Bounds for d-codes in $\mathrm{Her}(n, q)$

Theorem (S. 2017).

For odd d, every d-code Y in $\mathrm{Her}(n, q)$ satisfies

$$|Y| \leq q^{n(n-d+1)}.$$

In case of equality, the inner distribution of Y is determined.

For even d, the bound still holds for additive codes.

Bounds for d-codes in $\mathrm{Her}(n, q)$

Theorem (S. 2017).

For odd d, every d-code Y in $\mathrm{Her}(n, q)$ satisfies

$$|Y| \leq q^{n(n-d+1)}.$$

In case of equality, the inner distribution of Y is determined.

For even d, the bound still holds for additive codes.

The bounds are tight, except possibly when n and d are even.

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x, y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x,y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of additive d-codes of size $q^{n(n-d+1)}$:

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x, y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of additive d-codes of size $q^{n(n-d+1)}$:

- For odd n and odd d, take $a_1 = \cdots = a_d = 0$.

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x, y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of additive d-codes of size $q^{n(n-d+1)}$:

- For odd n and odd d, take $a_1 = \cdots = a_d = 0$.
- For odd n and even d, take $a_{(n-d+3)/2} = \cdots a_{(n+1)/2} = 0$.

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x, y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of additive d-codes of size $q^{n(n-d+1)}$:

- For odd n and odd d, take $a_1 = \cdots = a_d = 0$.
- For odd n and even d, take $a_{(n-d+3)/2} = \cdots a_{(n+1)/2} = 0$.
- For even n and odd d, take $a_{(n-d+3)/2} = \cdots a_{n/2} = 0$.

Constructions of optimal additive codes

Every Hermitian form $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be uniquely written as

$$H(x, y) = \mathrm{Tr}(y^q L(x)),$$

where

$$L(x) = \sum_{i=1}^{n} a_i x^{q^{2i}} \in \mathbb{F}_{q^{2n}}[x], \qquad a_{n-i+1} = a_i^{q^{2n-2i+1}}.$$

Constructions of additive d-codes of size $q^{n(n-d+1)}$:

- For odd n and odd d, take $a_1 = \cdots = a_d = 0$.
- For odd n and even d, take $a_{(n-d+3)/2} = \cdots a_{(n+1)/2} = 0$.
- For even n and odd d, take $a_{(n-d+3)/2} = \cdots a_{n/2} = 0$.
- For even n and even d, I don't know, except when $d \in \{2, n\}$.

Constructions in the non-additive case

Theorem
(Gow-Lavrauw-Sheekey-Vanhove 2014, S. 2017).

Let n be even and let Z be a set of q^n matrices over $\mathbb{F}_{q^2}$ of size $n/2 \times n/2$ with the property that $A - B$ is nonsingular for all distinct $A, B \in Z$. Let

$$Y = \left\{ \begin{pmatrix} I & A^* \\ A & AA^* \end{pmatrix} : A \in Z \right\} \cup \left\{ \begin{pmatrix} O & O \\ O & I \end{pmatrix} \right\},$$

Then Y is an n-code in $\mathrm{Her}(n, q)$ of size $q^n + 1$.

LP bounds

Theorem (S. 2017).

For even d, every d-code Y in $\mathrm{Her}(n, q)$ satisfies

$$|Y| \leq q^{n(n-d+1)} \frac{q^n(q^{n-d+1}+(-1)^n)-(-1)^n(q^{n-d+2}-(-1)^n)}{q^{n-d+1}(q+1)}.$$

LP bounds

Theorem (S. 2017).

For even d, every d-code Y in $\mathrm{Her}(n, q)$ satisfies

$$|Y| \leq q^{n(n-d+1)} \, \frac{q^n(q^{n-d+1}+(-1)^n)-(-1)^n(q^{n-d+2}-(-1)^n)}{q^{n-d+1}(q+1)}.$$

For $d = n$, this is $|Y| \leq q^{2n-1} - q^n + q^{n-1}$ (Thas 1992).

LP bounds

Theorem (S. 2017).

For even d, every d-code Y in $\mathrm{Her}(n,q)$ satisfies

$$|Y| \le q^{n(n-d+1)}\,\frac{q^n(q^{n-d+1}+(-1)^n)-(-1)^n(q^{n-d+2}-(-1)^n)}{q^{n-d+1}(q+1)}.$$

For $d=n$, this is $|Y| \le q^{2n-1} - q^n + q^{n-1}$ (Thas 1992).

Some numbers for 2-codes in $\mathrm{Her}(2,q)$:

q	Largest add. code	Largest code	LP	SDP
2	4	5	6	5
3	9	15	21	17
4	16	24	52	43
5	25	47	105	89

The unique 2-code in $\mathrm{Her}(2,3)$ of size 15

For every of the 15 pairs of matrices over $\mathbb{F}_9$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \theta^3 \\ \theta^2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \theta^2 \\ \theta^3 & 0 \end{bmatrix}, \begin{bmatrix} 1 & \theta^{-2} \\ \theta^{-3} & 0 \end{bmatrix}, \begin{bmatrix} 0 & \theta^{-3} \\ \theta^{-2} & 0 \end{bmatrix}$$

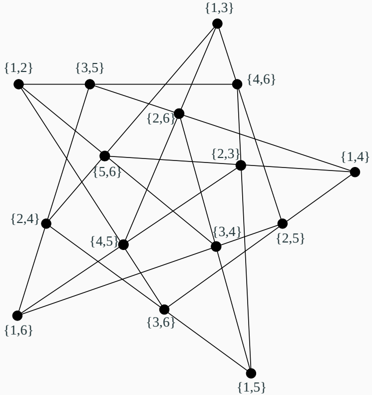
take the third point on the line (M. Schmidt 2016).

The unique 2-code in $\mathrm{Her}(2,3)$ of size 15

For every of the 15 pairs of matrices over $\mathbb{F}_9$

$$\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & \theta^3\\ \theta^2 & 0\end{bmatrix}, \begin{bmatrix}0 & \theta^2\\ \theta^3 & 0\end{bmatrix}, \begin{bmatrix}1 & \theta^{-2}\\ \theta^{-3} & 0\end{bmatrix}, \begin{bmatrix}0 & \theta^{-3}\\ \theta^{-2} & 0\end{bmatrix}$$

take the third point on the line (M. Schmidt 2016).

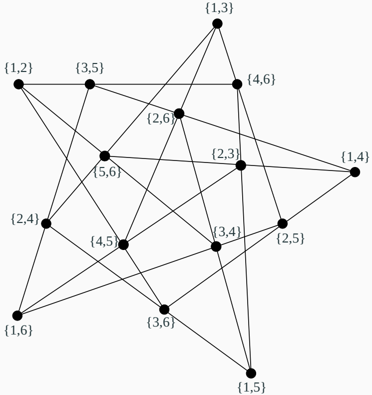


The unique 2-code in Her$(2, 3)$ of size 15

For every of the 15 pairs of matrices over $\mathbb{F}_9$

$$\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & \theta^3\\\theta^2 & 0\end{bmatrix}, \begin{bmatrix}0 & \theta^2\\\theta^3 & 0\end{bmatrix}, \begin{bmatrix}1 & \theta^{-2}\\\theta^{-3} & 0\end{bmatrix}, \begin{bmatrix}0 & \theta^{-3}\\\theta^{-2} & 0\end{bmatrix}$$

take the third point on the line (M. Schmidt 2016).



The Cremona-Richmond configuration.

Partial spreads in the Hermitian polar space

Partial spread in $H(2n-1,q^2)$: Collection of n-dimensional subspaces in $H(2n-1,q^2)$ with pairwise trivial intersection.

Partial spreads in the Hermitian polar space

Partial spread in $H(2n-1,q^2)$: Collection of n-dimensional subspaces in $H(2n-1,q^2)$ with pairwise trivial intersection.

There exists a partial spread in $H(2n-1,q^2)$ of size $N+1$ if and only if there exists an n-code in $\mathrm{Her}(n,q)$ of size N.

The correspondence is: $Y \mapsto \{\langle O \mid I \rangle\} \cup \{\langle I \mid M \rangle \,:\, M \in Y\}$.

Partial spreads in the Hermitian polar space

Partial spread in $H(2n-1,q^2)$: Collection of n-dimensional subspaces in $H(2n-1,q^2)$ with pairwise trivial intersection.

There exists a partial spread in $H(2n-1,q^2)$ of size $N+1$ if and only if there exists an n-code in $\mathrm{Her}(n,q)$ of size N.

The correspondence is: $Y \mapsto \{\langle O \mid I \rangle\} \cup \{\langle I \mid M \rangle \,:\, M \in Y\}$.

Corollary (Vanhove 2009).

For odd n, the size of a partial spread in $H(2n-1,q^2)$ is at most q^n+1.

Partial spreads in the Hermitian polar space

Partial spread in $H(2n-1,q^2)$: Collection of n-dimensional subspaces in $H(2n-1,q^2)$ with pairwise trivial intersection.

There exists a partial spread in $H(2n-1,q^2)$ of size $N+1$ if and only if there exists an n-code in $\mathrm{Her}(n,q)$ of size N.

The correspondence is: $Y \mapsto \{\langle O \mid I \rangle\} \cup \{\langle I \mid M \rangle \,:\, M \in Y\}$.

Corollary (Vanhove 2009).

For odd n, the size of a partial spread in $H(2n-1,q^2)$ is at most q^n+1.

For even n, several bounds have been obtained by (De Beule-Klein-Metsch-Storme 2008, Ihringer 2014, M. Schmidt 2016, Ihringer-Sin-Xiang 2018).

Bounds for d-codes in $\mathrm{Alt}(m, q)$

Theorem (Delsarte-Goethals 1975).

Every d-code Y in $\mathrm{Alt}(m, q)$ satisfies

$$|Y| \leq \begin{cases} q^{m((m-1)/2-d+1)} & \text{for odd } m \\ q^{(m-1)(m/2-d+1)} & \text{for even } m. \end{cases}$$

Bounds for d-codes in $\mathrm{Alt}(m, q)$

Theorem (Delsarte-Goethals 1975).

Every d-code Y in $\mathrm{Alt}(m, q)$ satisfies

$$|Y| \leq \begin{cases} q^{m((m-1)/2-d+1)} & \text{for odd } m \\ q^{(m-1)(m/2-d+1)} & \text{for even } m. \end{cases}$$

This bound is tight when m is odd.

Kerdock sets, spreads and beyond

Two equivalent objects:

Kerdock set: An n-code of size q^{2n-1} in $\mathrm{Alt}(2n, q)$.

Kerdock sets, spreads and beyond

Two equivalent objects:

Kerdock set: An n-code of size q^{2n-1} in $\mathrm{Alt}(2n, q)$.

Orthogonal spread: Collection of $q^{2n-1} + 1$ $(2n)$-dimensional subspaces in $Q^+(4n-1, q)$ with pairwise trivial intersection.

Kerdock sets, spreads and beyond

Two equivalent objects:

Kerdock set: An n-code of size q^{2n-1} in $\mathrm{Alt}(2n, q)$.

Orthogonal spread: Collection of $q^{2n-1} + 1$ $(2n)$-dimensional subspaces in $Q^+(4n-1, q)$ with pairwise trivial intersection.

The correspondence is $Y \mapsto \{\langle O \mid I \rangle\} \cup \{\langle I \mid M \rangle \ : \ M \in Y\}$.

Kerdock sets, spreads and beyond

Two equivalent objects:

Kerdock set: An n-code of size q^{2n-1} in $\mathrm{Alt}(2n, q)$.

Orthogonal spread: Collection of $q^{2n-1} + 1$ $(2n)$-dimensional subspaces in $Q^+(4n-1, q)$ with pairwise trivial intersection.

The correspondence is $Y \mapsto \{\langle O \mid I\rangle\} \cup \{\langle I \mid M\rangle \,:\, M \in Y\}$.

For even q, many constructions are known. For odd q, constructions are known only when $n = 2$ and $q \not\equiv 1 \pmod 3$ (Kantor 1982) or q prime (Conway-Kleidman-Wilson 1988).

Kerdock sets, spreads and beyond

Two equivalent objects:

Kerdock set: An n-code of size q^{2n-1} in $\mathrm{Alt}(2n, q)$.

Orthogonal spread: Collection of $q^{2n-1} + 1$ $(2n)$-dimensional subspaces in $Q^+(4n-1, q)$ with pairwise trivial intersection.

The correspondence is $Y \mapsto \{\langle O \mid I \rangle\} \cup \{\langle I \mid M \rangle \;:\; M \in Y\}$.

For even q, many constructions are known. For odd q, constructions are known only when $n = 2$ and $q \not\equiv 1 \pmod 3$ (Kantor 1982) or q prime (Conway-Kleidman-Wilson 1988).

For odd q and $n > 2$, no nontrivial d-codes in $\mathrm{Alt}(2n, q)$ meeting the LP bound are known to exist.

Additive codes in $\mathrm{Alt}(m, q)$

For odd m, there are always additive d-codes in $\mathrm{Alt}(m, q)$ that meet the Singleton bound, whereas for even m, all known constructions are not additive.

Additive codes in Alt(m, q)

For odd m, there are always additive d-codes in Alt(m, q) that meet the Singleton bound, whereas for even m, all known constructions are not additive.

Conjecture (Cooperstein 1997).

Every additive d-code Y in Alt($2n, q$) satisfies

$$|Y| \leq q^{2n(n-d+1/2)}.$$

Additive codes in Alt(m, q)

For odd m, there are always additive d-codes in Alt(m, q) that meet the Singleton bound, whereas for even m, all known constructions are not additive.

Conjecture (Cooperstein 1997).

Every additive d-code Y in Alt($2n, q$) satisfies

$$|Y| \leq q^{2n(n-d+1/2)}.$$

Proved for $d = 2$ (Heineken 1977), $d = n$ (Nyberg 1991), and $d = n - 1$ (Gow 2017).

Additive codes in Alt(m, q)

For odd m, there are always additive d-codes in Alt(m, q) that meet the Singleton bound, whereas for even m, all known constructions are not additive.

Conjecture (Cooperstein 1997).

Every additive d-code Y in Alt($2n, q$) satisfies

$$|Y| \leq q^{2n(n-d+1/2)}.$$

Proved for $d = 2$ (Heineken 1977), $d = n$ (Nyberg 1991), and $d = n - 1$ (Gow 2017).

There are constructions meeting the bound.

APN functions

An almost perfect nonlinear (APN) function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that

$$f(x + a) - f(x) = b$$

has at most two solutions for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$.

APN functions

An almost perfect nonlinear (APN) function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$.

The Gold function: $f(x) = x^3$.

APN functions

An almost perfect nonlinear (APN) function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$.

The Gold function: $f(x) = x^3$.

Observation (Edel 2009).

Every quadratic APN function corresponds to a minimal additive 1-design in $\mathrm{Alt}(m, q)$ and vice versa.

APN functions

An almost perfect nonlinear (APN) function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$.

The Gold function: $f(x) = x^3$.

Observation (Edel 2009).

Every quadratic APN function corresponds to a minimal additive 1-design in $\mathrm{Alt}(m, q)$ and vice versa.

Among all projections onto $\mathbb{F}_2$ of $f(x+a) - f(x) - f(a)$, we see every value of $\mathbb{F}_2$ equally often

APN functions

An almost perfect nonlinear (APN) function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$.

The Gold function: $f(x) = x^3$.

Observation (Edel 2009).

Every quadratic APN function corresponds to a minimal additive 1-design in $\mathrm{Alt}(m, q)$ and vice versa.

Among all projections onto $\mathbb{F}_2$ of $f(x+a) - f(x) - f(a)$, we see every value of $\mathbb{F}_2$ equally often $\Leftrightarrow a'_1 = 0$.

Nonlinearity of APN functions

The possible inner distributions are directly related to questions about nonlinearities of APN functions.

Nonlinearity of APN functions

The possible inner distributions are directly related to questions about nonlinearities of APN functions.

Most known APN functions have the same nonlinearity spectrum.

The exceptions are: Two infinite nonquadratic families and one sporadic quadratic example for $m = 6$ due to Dillon.

Nonlinearity of APN functions

The possible inner distributions are directly related to questions about nonlinearities of APN functions.

Most known APN functions have the same nonlinearity spectrum.

The exceptions are: Two infinite nonquadratic families and one sporadic quadratic example for $m = 6$ due to Dillon.

- For odd m, the inner distribution is determined.

Nonlinearity of APN functions

The possible inner distributions are directly related to questions about nonlinearities of APN functions.

Most known APN functions have the same nonlinearity spectrum.

The exceptions are: Two infinite nonquadratic families and one sporadic quadratic example for $m = 6$ due to Dillon.

- For odd m, the inner distribution is determined.
- For $m = 6$, there are exactly two different inner distributions:

$$(1, 0, 21, 42), \quad (1, 1, 16, 46).$$

Nonlinearity of APN functions

The possible inner distributions are directly related to questions about nonlinearities of APN functions.

Most known APN functions have the same nonlinearity spectrum.

The exceptions are: Two infinite nonquadratic families and one sporadic quadratic example for $m = 6$ due to Dillon.

- For odd m, the inner distribution is determined.
- For $m = 6$, there are exactly two different inner distributions:

$$(1, 0, 21, 42), \quad (1, 1, 16, 46).$$

- For $m = 8$, there at least three different inner distributions:

$$(1, 0, 0, 85, 170), \quad (1, 0, 1, 80, 174), \quad (1, 0, 2, 75, 178).$$

Two (nonclassical) association schemes

Sym(m, q): $m \times m$ symmetric matrices over $\mathbb{F}_q$

Qua(m, q): cosets of $m \times m$ alternating matrices over $\mathbb{F}_q$

Two (nonclassical) association schemes

Sym(m, q): $m \times m$ symmetric matrices over $\mathbb{F}_q$

Qua(m, q): cosets of $m \times m$ alternating matrices over $\mathbb{F}_q$

The group $\mathbb{F}_q^\times \times \mathrm{GL}_m(\mathbb{F}_q)$ acts on $\mathrm{Sym}(m, q)$ and $\mathrm{Qua}(m, q)$ by

$$((\lambda, L), S) \mapsto \lambda \cdot LSL^T$$
$$((\lambda, L), [A]) \mapsto [\lambda \cdot LAL^T].$$

In each case there is one orbit for each odd rank and two orbits for each nonzero even rank.

These orbits define two translation association association schemes with $m + \lfloor m/2 \rfloor + 1$ classes.

P- and Q-numbers

The character group of Sym(m, q) can be identified with Qua(m, q) and Qua(m, q) and Sym(m, q) are dual to each other. In particular, Sym(m, q) is self-dual for odd q.

P- and Q-numbers

The character group of $\mathrm{Sym}(m, q)$ can be identified with $\mathrm{Qua}(m, q)$ and $\mathrm{Qua}(m, q)$ and $\mathrm{Sym}(m, q)$ are dual to each other. In particular, $\mathrm{Sym}(m, q)$ is self-dual for odd q.

Theorem (S. 2015, 2017).

The P- and Q-numbers of $\mathrm{Sym}(m, q)$ and $\mathrm{Qua}(m, q)$ can be expressed as linear combinations of generalised Krawtchouk polynomials.

Special cases (Bachoc-Serra-Zemor 2017) and recurrence relations (Feng-Wang-Ma-Ma 2008) were known before.

A nice form of the duality

$\mathrm{Sym}(m, q)$	$\mathrm{Qua}(m, q)$
$A_s = a_{2s^+} + a_{2s^-} + a_{2s-1}$	$A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$
$B_s = a_{2s^+} + a_{2s^-} + a_{2s+1}$	$B'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r+1}$
$C_s = q^{-s}(a_{2s^+} - a_{2s^-}) \quad (q \text{ odd})$	$C'_r = q^{-r}(a_{2r^+} - a_{2r^-})$
$C_s = a_{2s^+} \quad (q \text{ even})$	

A nice form of the duality

Sym(m,q) | Qua(m,q)

$$A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \qquad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

$$B_s = a_{2s^+} + a_{2s^-} + a_{2s+1} \qquad B'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r+1}$$

$$C_s = q^{-s}(a_{2s^+} - a_{2s^-}) \quad (q \text{ odd}) \qquad C'_r = q^{-r}(a_{2r^+} - a_{2r^-})$$

$$C_s = a_{2s^+} \quad (q \text{ even})$$

Then

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A}, \qquad \boldsymbol{B}' = q^m\, Q_m\, \boldsymbol{C}, \qquad \boldsymbol{C}' = Q_m \boldsymbol{B},$$

where Q_m is the Q-matrix of Alt(m,q).

Bounds in Sym(m, q)

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A} \quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

Theorem (S. 2017).

For odd d, every d-code Y in Sym(m, q) satisfies

$$|Y| \le \begin{cases} q^{m(m-d+2)/2} & \text{for even } m-d, \\ q^{(m+1)(m-d+1)/2} & \text{for odd } m-d. \end{cases}$$

In case of equality, the inner distribution is determined.

Bounds in Sym(m, q)

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A} \quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

$$\boldsymbol{C}' = Q_m\boldsymbol{B} \quad B_s = a_{2s^+} + a_{2s^-} + a_{2s+1} \quad C'_r = q^{-r}(a_{2r^+} - a_{2r^-}).$$

Theorem (S. 2017).

For odd d, every d-code Y in Sym(m, q) satisfies

$$|Y| \le \begin{cases} q^{m(m-d+2)/2} & \text{for even } m-d, \\ q^{(m+1)(m-d+1)/2} & \text{for odd } m-d. \end{cases}$$

In case of equality, the inner distribution is determined.

For even d, the bound still holds for additive d-codes.

Bounds in Sym(m, q)

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A} \quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

$$\boldsymbol{C}' = Q_m\boldsymbol{B} \quad B_s = a_{2s^+} + a_{2s^-} + a_{2s+1} \quad C'_r = q^{-r}(a_{2r^+} - a_{2r^-}).$$

Theorem (S. 2017).

For odd d, every d-code Y in Sym(m, q) satisfies

$$|Y| \le \begin{cases} q^{m(m-d+2)/2} & \text{for even } m-d, \\ q^{(m+1)(m-d+1)/2} & \text{for odd } m-d. \end{cases}$$

In case of equality, the inner distribution is determined.

For even d, the bound still holds for additive d-codes.

These bounds are tight.

Bounds in Sym(m, q)

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A} \quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

$$\boldsymbol{C}' = Q_m\boldsymbol{B} \quad B_s = a_{2s^+} + a_{2s^-} + a_{2s+1} \quad C'_r = q^{-r}(a_{2r^+} - a_{2r^-}).$$

Theorem (S. 2017).

For odd d, every d-code Y in Sym(m, q) satisfies

$$|Y| \le \begin{cases} q^{m(m-d+2)/2} & \text{for even } m-d, \\ q^{(m+1)(m-d+1)/2} & \text{for odd } m-d. \end{cases}$$

In case of equality, the inner distribution is determined.

For even d, the bound still holds for additive d-codes.

These bounds are tight.

The cases $m - d \in \{1, 2\}$ were first obtained by (Gow 2014).

Some numbers for Sym($m, 2$)

(m, d)	Largest add. code	Largest code	LP bound
$(3, 2)$	16	$= 22$	24
$(4, 2)$	256	≥ 320	384
$(5, 4)$	64	≥ 96	196

The constructions are from (M. Schmidt 2016).

Some numbers for Sym$(m, 2)$

(m, d)	Largest add. code	Largest code	LP bound
$(3, 2)$	16	$= 22$	24
$(4, 2)$	256	≥ 320	384
$(5, 4)$	64	≥ 96	196

The constructions are from (M. Schmidt 2016).

The optimal 2-code in Sym$(3, 2)$: Take the zero matrix together with the 21 nonalternating matrices of rank 2.

Bounds in Qua(m, q) for even q

$$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A} \quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1} \quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$$

$$\boldsymbol{C}' = Q_m\boldsymbol{B} \quad B_s = a_{2s^+} + a_{2s^-} + a_{2s+1} \quad C'_r = a'_{2r^+}.$$

Bounds in Qua(m, q) for even q

$\boldsymbol{A}' = Q_{m+1}\boldsymbol{A}$ $\quad A_s = a_{2s^+} + a_{2s^-} + a_{2s-1}$ $\quad A'_r = a'_{2r^+} + a'_{2r^-} + a'_{2r-1}$

$\boldsymbol{C}' = Q_m\boldsymbol{B}$ $\quad B_s = a_{2s^+} + a_{2s^-} + a_{2s+1}$ $\quad C'_r = a'_{2r^+}$.

Theorem (S. 2017).

Let q be even and let Y be a d-code in Qua(m, q). Then

$$|Y| \le \begin{cases} q^{m(m-d+2)/2} & \text{for odd } m \text{ and odd } d, \\ q^{(m+1)(m-d+1)/2} & \text{for even } m \text{ and odd } d, \\ q^{(m-1)(m-d+2)/2} & \text{for even } m \text{ and even } d, \\ q^{m(m-d+1)/2} & \text{for odd } m \text{ and even } d. \end{cases}$$

These bounds are tight. If d is odd and equality holds, then the inner distribution of Y is determined.

Applications to coding theory

$$\begin{aligned} \mathrm{Qua}(m,q) &\cong \mathrm{GRM}(2,m)/\,\mathrm{GRM}(1,m) \\ \text{inner distribution} &\Leftrightarrow \text{distance distribution} \end{aligned}$$

Applications to coding theory

$$\begin{array}{ccc} \mathrm{Qua}(m,q) & \cong & \mathrm{GRM}(2,m)/\,\mathrm{GRM}(1,m) \\ \text{inner distribution} & \Leftrightarrow & \text{distance distribution} \end{array}$$

type	rank	minimum weight of coset
parabolic	$2s+1$	$q^{m-1}(q-1) - q^{m-s-1}$
elliptic	$2s$	$q^{m-1}(q-1) - q^{m-s-1}$
hyperbolic	$2s$	$(q^{m-1} - q^{m-s-1})(q-1)$

Elliptic and hyperbolic d-codes

Theorem (S. 2017).

Let Y be an elliptic $(2d)$-code in $\mathrm{Qua}(2n, q)$. Then

$$|Y| \leq q^{2n(n-d+1/2)}.$$

This bounds is tight, and if equality holds, then the inner distribution of Y is determined.

The same bound holds for additive hyperbolic d-codes.

Codes and their distance distributions

We obtain many optimal or best known codes and very general theorems for the distance distribution of classes codes, for which many special cases have been previously obtained:

Codes and their distance distributions

We obtain many optimal or best known codes and very general theorems for the distance distribution of classes codes, for which many special cases have been previously obtained:

For $q = 2$: (Berlekamp 1970), (Kasami 1971)

Codes and their distance distributions

We obtain many optimal or best known codes and very general theorems for the distance distribution of classes codes, for which many special cases have been previously obtained:

For $q = 2$: (Berlekamp 1970), (Kasami 1971)

For odd q: (Feng & Luo 2008), (Luo & Feng 2008), (Y. Liu & Yan 2013), (X. Liu & Luo 2014a), (X. Liu & Luo 2014b), (Y. Liu, Yan & Ch. Liu 2014), (Zheng, Wang, Zeng & Hu 2014), ...

Codes in classical association schemes

Kai-Uwe Schmidt

Department of Mathematics
Paderborn University
Germany