q-Analogues of Designs

Geoff Walsh

Claude Shannon Institute
University College Dublin

May 2010

Motivation

- Codes consisting of n-dimensional subspaces of $\mathbb{F}_q^v$ can be used for error correction in random network coding.

Motivation

- Codes consisting of n-dimensional subspaces of $\mathbb{F}_q^v$ can be used for error correction in random network coding.
- These constant dimension codes are the q-analogues of constant weight codes.

Motivation

- Codes consisting of n-dimensional subspaces of $\mathbb{F}_q^v$ can be used for error correction in random network coding.
- These constant dimension codes are the q-analogues of constant weight codes.
- Certain optimal constant dimension codes are the q-analogues of Steiner systems.

Motivation

- Codes consisting of n-dimensional subspaces of $\mathbb{F}_q^v$ can be used for error correction in random network coding.
- These constant dimension codes are the q-analogues of constant weight codes.
- Certain optimal constant dimension codes are the q-analogues of Steiner systems.
- Does the q-analogue of the Fano plane exist ?

Motivation

- Codes consisting of n-dimensional subspaces of $\mathbb{F}_q^v$ can be used for error correction in random network coding.
- These constant dimension codes are the q-analogues of constant weight codes.
- Certain optimal constant dimension codes are the q-analogues of Steiner systems.
- Does the q-analogue of the Fano plane exist ?
- The q-analogues of Steiner systems first appear in Delsarte's seminal work on association schemes.

Outline

Association Schemes

Definition

A (symmetrical) **n-class association scheme** $X = (X, \mathbf{d})$ consists of a finite set X with a surjective function $\mathbf{d} : X^2 \to \mathbb{N}_n$ such that

1. $\mathbf{d}(x, y) = 0 \Leftrightarrow x = y$
2. $\mathbf{d}(x, y) = \mathbf{d}(y, x)$ for any $y, x \in X$
3. For any $x, y \in X$ and any $i, j \in \mathbb{N}_n$, the number of points $z \in X$ such that $\mathbf{d}(x, z) = i$, $\mathbf{d}(z, y) = j$ depends only on $\mathbf{d}(x, y)$. For $k = \mathbf{d}(x, y)$ this number is denoted by $p_{i,j}^k$.

Association Schemes

- For $k \in \mathbb{N}_n$, let $R_k = \{(x, y) \in X^2 : \mathbf{d}(x, y) = k\}$.

Association Schemes

- For $k \in \mathbb{N}_n$, let $R_k = \{(x, y) \in X^2 : \mathbf{d}(x, y) = k\}$.
- If $\mathbf{d}$ is a metric on X and the graph (X, R_1) is connected, then $(X, \mathbf{d})$ is called a **metric scheme**.

Association Schemes

- For $k \in \mathbb{N}_n$, let $R_k = \{(x, y) \in X^2 : \mathbf{d}(x, y) = k\}$.
- If $\mathbf{d}$ is a metric on X and the graph (X, R_1) is connected, then $(X, \mathbf{d})$ is called a **metric scheme**.
- A 2-class association scheme is alway metric and is equivalent to a **strongly regular graph**.

Association Schemes

- For $k \in \mathbb{N}_n$, let $R_k = \{(x, y) \in X^2 : \mathbf{d}(x, y) = k\}$.
- If $\mathbf{d}$ is a metric on X and the graph (X, R_1) is connected, then $(X, \mathbf{d})$ is called a **metric scheme**.
- A 2-class association scheme is alway metric and is equivalent to a **strongly regular graph**.
- If $(X, \mathbf{d})$ is a metric scheme and $\mathbf{d}$ is the path metric on the graph (X, R_1), then (X, R_1) is a **distance-regular graph**.

Association Schemes

- For $k \in \mathbb{N}_n$, let $R_k = \{(x, y) \in X^2 : \mathbf{d}(x, y) = k\}$.
- If $\mathbf{d}$ is a metric on X and the graph (X, R_1) is connected, then $(X, \mathbf{d})$ is called a **metric scheme**.
- A 2-class association scheme is alway metric and is equivalent to a **strongly regular graph**.
- If $(X, \mathbf{d})$ is a metric scheme and $\mathbf{d}$ is the path metric on the graph (X, R_1), then (X, R_1) is a **distance-regular graph**.
- Suppose X is the vertex set of a distance-regular graph with path metric $\mathbf{d}$ and diameter n. Then $(X, \mathbf{d})$ is an n-class metric scheme.

Examples of Metric Schemes

- **Hamming scheme**. Let $X = \mathbb{F}_q^n$ and let $\mathbf{d}(x, y) = |\{i : x_i \neq y_i\}|$ (usual hamming metric). Then $(X, \mathbf{d})$ is an n-class metric scheme, denoted by $H(n, q)$.

Examples of Metric Schemes

- **Hamming scheme**. Let $X = \mathbb{F}_q^n$ and let $\mathbf{d}(x, y) = |\{i : x_i \neq y_i\}|$ (usual hamming metric). Then $(X, \mathbf{d})$ is an n-class metric scheme, denoted by $H(n, q)$.
- **Johnson scheme** Let X be the set of all n-subsets of $\mathbb{N}_v^1 = \{1, \ldots, v\}$ with metric $\mathbf{d}(x, y) = n - |x \cap y|$. Then $(X, \mathbf{d})$ an n-class metric scheme denoted by $J(v, n, 1)$

Examples of Metric Schemes

- **Hamming scheme**. Let $X = \mathbb{F}_q^n$ and let $\mathbf{d}(x, y) = |\{i : x_i \neq y_i\}|$ (usual hamming metric). Then $(X, \mathbf{d})$ is an n-class metric scheme, denoted by $H(n, q)$.
- **Johnson scheme** Let X be the set of all n-subsets of $\mathbb{N}_v^1 = \{1, \ldots, v\}$ with metric $\mathbf{d}(x, y) = n - |x \cap y|$. Then $(X, \mathbf{d})$ an n-class metric scheme denoted by $J(v, n, 1)$
- **Grassman scheme** Let X be the set of all n-dimensional subspaces of $\mathbb{F}_q^v$ with metric $\mathbf{d}(A, B) = n - \dim(A \cap B)$. Then $(X, \mathbf{d})$ is an n-class metric scheme denoted by $J(v, n, q)$.

The Bose-Mesner Algebra

- The graph (X, R_i) is represented by its **adjacency matrix**

$$D_i \in \mathbb{R}(X^2),\ D_i(x,y) = \begin{cases} 1, & \text{for } \mathbf{d}(x,y) = i \\ 0, & \text{otherwise.} \end{cases}$$

The Bose-Mesner Algebra

- The graph (X, R_i) is represented by its **adjacency matrix** $D_i \in \mathbb{R}(X^2)$, $D_i(x, y) = \begin{cases} 1, & \text{for } \mathbf{d}(x, y) = i \\ 0, & \text{otherwise.} \end{cases}$

Definition

The **Bose-Mesner Algebra** of the n-class metric scheme (X, R), denoted $\mathcal{A}$, is the $(n+1)$-dimensional real commutative algebra

$$\mathcal{A} = \{\sum_{i \in \mathbb{N}_n} \alpha_i D_i : \alpha_i \in \mathbb{R}, \forall i \in \mathbb{N}_n\}.$$

$\mathcal{A}$ is semisimple and therefore has a unique basis of irreducible idempotent matrices $\{E_i\}_{i \in \mathbb{N}_n}$.

The Bose-Mesner Algebra

- As $\{D_i\}_{i\in\mathbb{N}_n}$ and $\{E_i\}_{i\in\mathbb{N}_n}$ are two bases for $\mathcal{A}$, there exist two systems of real numbers $p_j(i)$ and $q_j(i)$, $i,j \in \mathbb{N}_n$ such that

$$D_i = \sum_{j\in\mathbb{N}_n} p_i(j)E_j \ , \ E_i = |X|^{-1} \sum_{j\in\mathbb{N}_n} q_i(j)D_j.$$

The Bose-Mesner Algebra

- As $\{D_i\}_{i\in\mathbb{N}_n}$ and $\{E_i\}_{i\in\mathbb{N}_n}$ are two bases for $\mathcal{A}$, there exist two systems of real numbers $p_j(i)$ and $q_j(i)$, $i,j \in \mathbb{N}_n$ such that

$$D_i = \sum_{j\in\mathbb{N}_n} p_i(j)E_j \ , \ E_i = |X|^{-1} \sum_{j\in\mathbb{N}_n} q_i(j)D_j.$$

- Let P and Q be the matrices with $(i,j)^{th}$ entry equal to $p_j(i)$ and $q_j(i)$ respectively. Clearly $PQ = QP = |X|I$.

The Bose-Mesner Algebra

- As $\{D_i\}_{i\in\mathbb{N}_n}$ and $\{E_i\}_{i\in\mathbb{N}_n}$ are two bases for $\mathcal{A}$, there exist two systems of real numbers $p_j(i)$ and $q_j(i)$, $i,j \in \mathbb{N}_n$ such that

$$D_i = \sum_{j\in\mathbb{N}_n} p_i(j)E_j \ , \ E_i = |X|^{-1} \sum_{j\in\mathbb{N}_n} q_i(j)D_j.$$

- Let P and Q be the matrices with $(i,j)^{th}$ entry equal to $p_j(i)$ and $q_j(i)$ respectively. Clearly $PQ = QP = |X|I$.
- If $(X, \mathbf{d})$ is a metric scheme, then $\forall j,k \in \mathbb{N}_n$, $p_j(k)$ is a real polynomial of degree j in $p_1(k)$.

The Bose-Mesner Algebra

- As $\{D_i\}_{i\in\mathbb{N}_n}$ and $\{E_i\}_{i\in\mathbb{N}_n}$ are two bases for $\mathcal{A}$, there exist two systems of real numbers $p_j(i)$ and $q_j(i)$, $i,j \in \mathbb{N}_n$ such that

$$D_i = \sum_{j\in\mathbb{N}_n} p_i(j)E_j \ , \ E_i = |X|^{-1} \sum_{j\in\mathbb{N}_n} q_i(j)D_j.$$

- Let P and Q be the matrices with $(i,j)^{th}$ entry equal to $p_j(i)$ and $q_j(i)$ respectively. Clearly $PQ = QP = |X|I$.
- If $(X, \mathbf{d})$ is a metric scheme, then $\forall j,k \in \mathbb{N}_n$, $p_j(k)$ is a real polynomial of degree j in $p_1(k)$.
- If $(X, \mathbf{d})$ is a metric scheme, then $(X, \mathbf{d})$ is called **polynomial scheme** if $\forall j,k \in \mathbb{N}_n$, $q_j(k)$ is a real polynomial of degree j in $q_1(k)$.

Parameters for Examples

- Let $v, n \in \mathbb{N}$ with $0 \leq n \leq v$, for $q > 1$ define $\begin{bmatrix} v \\ n \end{bmatrix} = \prod_{i=0}^{n-1} \frac{q^{v-i}-1}{q^{n-i}-1}$ and for $q = 1$ $\begin{bmatrix} v \\ n \end{bmatrix} = \begin{pmatrix} v \\ n \end{pmatrix}$.

Parameters for Examples

- Let $v, n \in \mathbb{N}$ with $0 \leq n \leq v$, for $q > 1$ define $\begin{bmatrix} v \\ n \end{bmatrix} = \prod_{i=0}^{n-1} \frac{q^{v-i}-1}{q^{n-i}-1}$ and for $q = 1$ $\begin{bmatrix} v \\ n \end{bmatrix} = \begin{pmatrix} v \\ n \end{pmatrix}$.
- The functions defining $J(v, n, q)$ are as follows, $|X| = \begin{bmatrix} v \\ n \end{bmatrix}$ and

$$q_i(k) = q_i(0) \sum_{j \in \mathbb{N}_i} \frac{(-1)^j}{p_j(0)} \begin{bmatrix} i \\ j \end{bmatrix} \begin{bmatrix} v+1-i \\ j \end{bmatrix} \begin{bmatrix} k \\ j \end{bmatrix} q^{j(-k+(3j-1)/2)},$$

$$p_i(k) = \sum_{j \in \mathbb{N}_i} (-1)^{i-j} \begin{bmatrix} n-j \\ i-j \end{bmatrix} \begin{bmatrix} n-k \\ j \end{bmatrix} \begin{bmatrix} v-n+j-k \\ j \end{bmatrix} q^{kj+\begin{pmatrix} i-j \\ 2 \end{pmatrix}}.$$

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.
- The **distance distribution** of $\mathcal{C}$ is the vector

$$B = \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} B(x).$$

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.
- The **distance distribution** of $\mathcal{C}$ is the vector

$$B = \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} B(x).$$

- The **dual distribution** of $\mathcal{C}$ is the Q-transform of B, i.e. $B^* = BQ$.

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.
- The **distance distribution** of $\mathcal{C}$ is the vector

$$B = \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} B(x).$$

- The **dual distribution** of $\mathcal{C}$ is the Q-transform of B, i.e. $B^* = BQ$.
- The **MacWilliams-Delsarte inequalities** imply $B^* = BQ \geq 0$.

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.
- The **distance distribution** of $\mathcal{C}$ is the vector

$$B = \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} B(x).$$

- The **dual distribution** of $\mathcal{C}$ is the Q-transform of B, i.e. $B^* = BQ$.
- The **MacWilliams-Delsarte inequalities** imply $B^* = BQ \geq 0$.
- A code $\mathcal{C}$ is called **regular** if for all $x \in \mathcal{C}$ $B(x) = B$.

Subsets of Association Schemes

- A code in $(X, \mathbf{d})$ is a nonempty subset $\mathcal{C}$ of X.
- For any $x \in X$, let $B(x) = (B_0(x), \ldots, B_n(x))$ where $B_i(x) = |\{y \in \mathcal{C} : \mathbf{d}(x, y) = i\}|$.
- The **distance distribution** of $\mathcal{C}$ is the vector

$$B = \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} B(x).$$

- The **dual distribution** of $\mathcal{C}$ is the Q-transform of B, i.e. $B^* = BQ$.
- The **MacWilliams-Delsarte inequalities** imply $B^* = BQ \geq 0$.
- A code $\mathcal{C}$ is called **regular** if for all $x \in \mathcal{C}$ $B(x) = B$.
- A code $\mathcal{C}$ is called **completely regular** if for all $x \in X$, $B(x)$ depends only on $\mathbf{d}(x, \mathcal{C})$.

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance d**$(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance d**$(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,
- the **dual distance d**$^*(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i^* \neq 0$,

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance** $\mathbf{d}(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,
- the **dual distance** $\mathbf{d}^*(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i^* \neq 0$,
- the **strength** $\tau(\mathcal{C}) = \mathbf{d}^*(\mathcal{C}) - 1$,

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance** $\mathbf{d}(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,
- the **dual distance** $\mathbf{d}^*(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i^* \neq 0$,
- the **strength** $\tau(\mathcal{C}) = \mathbf{d}^*(\mathcal{C}) - 1$,
- the **degree** $s(\mathcal{C}) = w_H(B) - 1$ and the **dual degree** $s^*(\mathcal{C}) = w_H(B^*) - 1$,

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance** $\mathbf{d}(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,
- the **dual distance** $\mathbf{d}^*(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i^* \neq 0$,
- the **strength** $\tau(\mathcal{C}) = \mathbf{d}^*(\mathcal{C}) - 1$,
- the **degree** $s(\mathcal{C}) = w_H(B) - 1$ and the **dual degree** $s^*(\mathcal{C}) = w_H(B^*) - 1$,
- The **packing radius** $\rho(\mathcal{C}) = \max\{\mathbf{d}(x, \mathcal{C}) : x \in X\}$.

Fundamental Parameters

Definition

Let B be the distance distribution of a code $\mathcal{C} \subset X$, define

- the **minimum distance** $\mathbf{d}(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i \neq 0$,
- the **dual distance** $\mathbf{d}^*(\mathcal{C})$ is the smallest $i \in \mathbb{N}_n^1$ such that $B_i^* \neq 0$,
- the **strength** $\tau(\mathcal{C}) = \mathbf{d}^*(\mathcal{C}) - 1$,
- the **degree** $s(\mathcal{C}) = w_H(B) - 1$ and the **dual degree** $s^*(\mathcal{C}) = w_H(B^*) - 1$,
- The **packing radius** $\rho(\mathcal{C}) = \max\{\mathbf{d}(x, \mathcal{C}) : x \in X\}$.
- For $\mathbf{d} \in \mathbb{N}_n^1$ and $\tau \in \mathbb{N}_n$, a code $\mathcal{C} \subset X$ is said to be a $\mathbf{d}$-code if $\mathbf{d}(\mathcal{C}) \geq \mathbf{d}$ and a τ-design if $\tau(\mathcal{C}) \geq \tau$.

Bounds on Parameters

Theorem

Let $(X, \boldsymbol{d})$ *be an* n*-class polynomial scheme and* $\mathcal{C} \subset X$*, then*

1. $\boldsymbol{d}(\mathcal{C}) + \boldsymbol{d}^*(\mathcal{C}) \leq n + 2$,

Bounds on Parameters

Theorem

Let $(X, \boldsymbol{d})$ *be an* n*-class polynomial scheme and* $\mathcal{C} \subset X$*, then*

1. $\boldsymbol{d}(\mathcal{C}) + \boldsymbol{d}^*(\mathcal{C}) \leq n + 2$,
2. $\boldsymbol{d}(\mathcal{C}) \leq 2s^*(\mathcal{C}) + 1$ *and* $\boldsymbol{d}^*(\mathcal{C}) \leq 2s(\mathcal{C}) + 1$,

Bounds on Parameters

Theorem

Let $(X, \boldsymbol{d})$ *be an* n*-class polynomial scheme and* $\mathcal{C} \subset X$*, then*

1. $\boldsymbol{d}(\mathcal{C}) + \boldsymbol{d}^*(\mathcal{C}) \leq n + 2$,
2. $\boldsymbol{d}(\mathcal{C}) \leq 2s^*(\mathcal{C}) + 1$ *and* $\boldsymbol{d}^*(\mathcal{C}) \leq 2s(\mathcal{C}) + 1$,
3. *if* $\boldsymbol{d}(\mathcal{C}) \geq s^*(\mathcal{C})$ *then* $\mathcal{C}$ *is regular,*

Bounds on Parameters

Theorem

Let $(X, \mathbf{d})$ *be an n-class polynomial scheme and* $\mathcal{C} \subset X$*, then*

1. $\mathbf{d}(\mathcal{C}) + \mathbf{d}^*(\mathcal{C}) \leq n + 2$,
2. $\mathbf{d}(\mathcal{C}) \leq 2s^*(\mathcal{C}) + 1$ *and* $\mathbf{d}^*(\mathcal{C}) \leq 2s(\mathcal{C}) + 1$,
3. *if* $\mathbf{d}(\mathcal{C}) \geq s^*(\mathcal{C})$ *then* $\mathcal{C}$ *is regular,*
4. *if* $\mathbf{d}(\mathcal{C}) \geq 2s^*(\mathcal{C}) - 1$ *then* $\mathcal{C}$ *is completely regular,*

Bounds on Parameters

Theorem

Let $(X, \mathbf{d})$ be an n-class polynomial scheme and $\mathcal{C} \subset X$, then

1. $\mathbf{d}(\mathcal{C}) + \mathbf{d}^*(\mathcal{C}) \leq n + 2$,
2. $\mathbf{d}(\mathcal{C}) \leq 2s^*(\mathcal{C}) + 1$ *and* $\mathbf{d}^*(\mathcal{C}) \leq 2s(\mathcal{C}) + 1$,
3. *if* $\mathbf{d}(\mathcal{C}) \geq s^*(\mathcal{C})$ *then* $\mathcal{C}$ *is regular,*
4. *if* $\mathbf{d}(\mathcal{C}) \geq 2s^*(\mathcal{C}) - 1$ *then* $\mathcal{C}$ *is completely regular,*
5. *if* $\mathbf{d}^*(\mathcal{C}) \geq 2s(\mathcal{C}) - 1$ *then* $(\mathcal{C}, \mathbf{d})$ *is a* $s(\mathcal{C})$*-class association scheme,*

Bounds on Parameters

Theorem

Let $(X, \mathbf{d})$ be an n-class polynomial scheme and $\mathcal{C} \subset X$, then

1. $\mathbf{d}(\mathcal{C}) + \mathbf{d}^*(\mathcal{C}) \leq n + 2$,
2. $\mathbf{d}(\mathcal{C}) \leq 2s^*(\mathcal{C}) + 1$ *and* $\mathbf{d}^*(\mathcal{C}) \leq 2s(\mathcal{C}) + 1$,
3. *if* $\mathbf{d}(\mathcal{C}) \geq s^*(\mathcal{C})$ *then* $\mathcal{C}$ *is regular,*
4. *if* $\mathbf{d}(\mathcal{C}) \geq 2s^*(\mathcal{C}) - 1$ *then* $\mathcal{C}$ *is completely regular,*
5. *if* $\mathbf{d}^*(\mathcal{C}) \geq 2s(\mathcal{C}) - 1$ *then* $(\mathcal{C}, \mathbf{d})$ *is a* $s(\mathcal{C})$*-class association scheme,*
6. $\rho(\mathcal{C}) \leq s^*(\mathcal{C})$, *with equality if an only if* $\mathcal{C}$ *is uniformly packed.*

Bounds on Cardinality

- Let $(X, \mathbf{d})$ be a n-class polynomial-scheme for which $p_1(j)$ and $q_1(j)$ are decreasing functions of $j \in \mathbb{N}_n$.

Bounds on Cardinality

- Let $(X, \mathbf{d})$ be a n-class polynomial-scheme for which $p_1(j)$ and $q_1(j)$ are decreasing functions of $j \in \mathbb{N}_n$.

Theorem

Suppose $\mathcal{C} \subset X$ be a d-code and a τ-design, then

$$\frac{|X|}{M_Q(n-\tau+1)} \leq |C| \leq \frac{|X|}{M_Q(d)},$$

where

$$M_Q(\delta) = \sum_{k \in \mathbb{N}_{\delta-1}} \prod_{i \in \mathbb{N}_n^{\delta}} \frac{q_1(k) - q_1(i)}{q_1(0) - q_1(i)} p_k(0).$$

Each of these bounds is attained if and only if $d + \tau = n + 1$, or equivalently $d(\mathcal{C}) + d^*(\mathcal{C}) = n + 2$.

Back to Examples

- The Singleton bound for $C \subset H(n, q)$,

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

Back to Examples

- The Singleton bound for $C \subset H(n, q)$,

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

- The Johnson bound for $C \subset J(v, n, q)$,

$$\frac{\begin{bmatrix} v \\ n \end{bmatrix}}{\begin{bmatrix} v-\tau(C) \\ v-n \end{bmatrix}} \leq |C| \leq \frac{\begin{bmatrix} v \\ n \end{bmatrix}}{\begin{bmatrix} v-n+\mathbf{d}(C)-1 \\ v-n \end{bmatrix}}.$$

q-Analogues of Designs

Definition

Let $t, v, n, \lambda \in \mathbb{N}$ such that $v \geq n \geq t \geq 0$ and $\lambda \geq 1$.

q-Analogues of Designs

Definition

Let $t, v, n, \lambda \in \mathbb{N}$ such that $v \geq n \geq t \geq 0$ and $\lambda \geq 1$.

1. For $q = 1$, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-subsets of $\mathbb{N}_v^1$, called blocks, such that each t-subset of $\mathbb{N}_v^1$ is contained in exactly λ blocks of $\mathcal{S}$.

q-Analogues of Designs

Definition

Let $t, v, n, \lambda \in \mathbb{N}$ such that $v \geq n \geq t \geq 0$ and $\lambda \geq 1$.

1. For $q = 1$, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-subsets of $\mathbb{N}_v^1$, called blocks, such that each t-subset of $\mathbb{N}_v^1$ is contained in exactly λ blocks of $\mathcal{S}$.
2. For q a power of a prime, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-dimensional subspaces of $\mathbb{F}_q^v$, called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks of $\mathcal{S}$.

q-Analogues of Designs

Definition

Let $t, v, n, \lambda \in \mathbb{N}$ such that $v \geq n \geq t \geq 0$ and $\lambda \geq 1$.

1. For $q = 1$, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-subsets of $\mathbb{N}_v^1$, called blocks, such that each t-subset of $\mathbb{N}_v^1$ is contained in exactly λ blocks of $\mathcal{S}$.
2. For q a power of a prime, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-dimensional subspaces of $\mathbb{F}_q^v$, called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks of $\mathcal{S}$.
3. A $t - (v, n, 1; q)$ design is referred to as a Steiner structure $\mathcal{S}_q(t, n, v)$.

q-Analogues of Designs

Definition

Let $t, v, n, \lambda \in \mathbb{N}$ such that $v \geq n \geq t \geq 0$ and $\lambda \geq 1$.

1. For $q = 1$, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-subsets of $\mathbb{N}_v^1$, called blocks, such that each t-subset of $\mathbb{N}_v^1$ is contained in exactly λ blocks of $\mathcal{S}$.
2. For q a power of a prime, a $t - (v, n, \lambda; q)$ design is a set $\mathcal{S}$ of n-dimensional subspaces of $\mathbb{F}_q^v$, called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks of $\mathcal{S}$.
3. A $t - (v, n, 1; q)$ design is referred to as a Steiner structure $\mathcal{S}_q(t, n, v)$.

Theorem

Suppose $\mathcal{C} \subset J(v, n, q)$*, then* $\mathcal{C}$ *is a* τ*-design in* $J(v, n, q)$ *if and only if* $\mathcal{C}$ *is a* $\tau - (v, n, \lambda; q)$ *design for some* $\lambda \in \mathbb{N}$

$q > 1$, Examples

- **S. Thomas**(1987): Construction of $2-(v,3,7;2)$ designs $\forall v \geq 7$ and $(v,6) = 1$.

$q > 1$, Examples

- **S. Thomas**(1987): Construction of $2-(v,3,7;2)$ designs $\forall v \geq 7$ and $(v,6)=1$.
- **H. Suzuki**(1992): Construction of $2-(v,3,q^2+q+1;q)$ designs $\forall v \geq 7$,$(v,6)=1$ and q a prime power.

$q > 1$, Examples

- **S. Thomas**(1987): Construction of $2-(v,3,7;2)$ designs $\forall v \geq 7$ and $(v,6)=1$.
- **H. Suzuki**(1992): Construction of $2-(v,3,q^2+q+1;q)$ designs $\forall v \geq 7$,$(v,6)=1$ and q a prime power.
- **T. Itoh**(1995): Construction of $2-(ml,3,q^3(q^{l-5}-1)/(q-1);q)$ designs for all $m \geq 3$, which admit the action of $SL_m(q^l)$.

$q > 1$, Examples

- **S. Thomas**(1987): Construction of $2-(v,3,7;2)$ designs $\forall v \geq 7$ and $(v,6)=1$.
- **H. Suzuki**(1992): Construction of $2-(v,3,q^2+q+1;q)$ designs $\forall v \geq 7$,$(v,6)=1$ and q a prime power.
- **T. Itoh**(1995): Construction of $2-(ml,3,q^3(q^{l-5}-1)/(q-1);q)$ designs for all $m \geq 3$, which admit the action of $SL_m(q^l)$.
- **M. Braun, A. Kerber and R. Laue**(2005): Constructed a $3-(8,4,11;2)$ design and a $3-(8,4,20;2)$ design.

$q > 1$, Examples

- **S. Thomas**(1987): Construction of $2-(v,3,7;2)$ designs $\forall v \geq 7$ and $(v,6)=1$.
- **H. Suzuki**(1992): Construction of $2-(v,3,q^2+q+1;q)$ designs $\forall v \geq 7$,$(v,6)=1$ and q a prime power.
- **T. Itoh**(1995): Construction of $2-(ml,3,q^3(q^{l-5}-1)/(q-1);q)$ designs for all $m \geq 3$, which admit the action of $SL_m(q^l)$.
- **M. Braun, A. Kerber and R. Laue**(2005): Constructed a $3-(8,4,11;2)$ design and a $3-(8,4,20;2)$ design.
- A $\mathcal{S}_q(1,n,v)$ exists if and only if n divides v.
- No known examples of a $\mathcal{S}_q(\tau,n,v)$ with $\tau \geq 2$.

Steiner Structures $q > 1$

Proposition

Schwartz and Etzion (2002)

- *If a nontrivial $\mathcal{S}_q(t, n, v)$ exists then $v \geq 2n$.*

Steiner Structures $q > 1$

Proposition

Schwartz and Etzion (2002)

- *If a nontrivial* $\mathcal{S}_q(t, n, v)$ *exists then* $v \geq 2n$.
- *If a* $\mathcal{S}_q(t, n, v)$ *exists and* $t \geq 2$, *then* $\forall i \in \mathbb{N}_{t-1}$ *a* $\mathcal{S}_q(t-i, n-i, v-i)$ *exists and* $\begin{bmatrix} v-i \\ t-i \end{bmatrix} / \begin{bmatrix} n-i \\ t-i \end{bmatrix} \in \mathbb{N}$.

Steiner Structures $q > 1$

Proposition

Schwartz and Etzion (2002)

- *If a nontrivial* $\mathcal{S}_q(t, n, v)$ *exists then* $v \geq 2n$.
- *If a* $\mathcal{S}_q(t, n, v)$ *exists and* $t \geq 2$, *then* $\forall i \in \mathbb{N}_{t-1}$ *a* $\mathcal{S}_q(t-i, n-i, v-i)$ *exists and* $\begin{bmatrix} v-i \\ t-i \end{bmatrix} / \begin{bmatrix} n-i \\ t-i \end{bmatrix} \in \mathbb{N}$.

Proposition

Schwartz and Etzion (2002), Etzion and Vardy (2009)

- *If a* $\mathcal{S}_q(2, n, v)$ *exists then a* $\mathcal{S}_1(2, (q^n-1)/(q-1), (q^v-1)/(q-1))$ *exists.*
- *If a* $\mathcal{S}_q(2, n, v)$ *exists then a* $\mathcal{S}_1(2, q^{n-1}, q^{v-1})$ *exists.*
- *If a* $\mathcal{S}_2(3, n, v)$ *exists then a* $\mathcal{S}_1(3, 2^{n-1}, 2^{v-1})$ *exists.*
- *If a* $\mathcal{S}_2(2, n, v)$ *exists then a* $\mathcal{S}_1(3, 2^n, 2^v)$ *exists.*

Steiner Structures $q > 1$

Corollary

Let $\mathcal{C} \subset J(v, n, q)$ be a τ-design, then the following are equivalent

1. *$\mathcal{C}$ achieves the Johnson bound, i.e.* $|\mathcal{C}| = \begin{bmatrix} v \\ n \end{bmatrix} / \begin{bmatrix} v-\tau \\ v-n \end{bmatrix}$,
2. $\tau = \tau(\mathcal{C})$ *and* $\boldsymbol{d}(\mathcal{C}) = n - \tau + 1$,
3. *$\mathcal{C}$ is a $\mathcal{S}_q(\tau, n, v)$.*

Steiner Structures $q > 1$

Corollary

Let $\mathcal{C} \subset J(v, n, q)$ be a τ-design, then the following are equivalent

1. *$\mathcal{C}$ achieves the Johnson bound, i.e. $|\mathcal{C}| = \begin{bmatrix} v \\ n \end{bmatrix} / \begin{bmatrix} v-\tau \\ v-n \end{bmatrix}$,*
2. *$\tau = \tau(\mathcal{C})$ and $\mathbf{d}(\mathcal{C}) = n - \tau + 1$,*
3. *$\mathcal{C}$ is a $\mathcal{S}_q(\tau, n, v)$.*

- Suppose $\mathcal{C} \subset J(v, n, q)$ is a $\mathcal{S}_q(\tau, n, v)$ with $q > 1$ then
  - $\mathbf{d}^*(\mathcal{C}) = \tau + 1$ and $s(\mathcal{C}) = \tau$,
  - $(n - \tau + 1)/2 \leq \rho(\mathcal{C}) \leq s^*(\mathcal{C}) \leq n - \tau$.

Steiner Structures $q > 1$

Corollary

Let $\mathcal{C} \subset J(v, n, q)$ be a τ-design, then the following are equivalent

1. *$\mathcal{C}$ achieves the Johnson bound, i.e.* $|\mathcal{C}| = \begin{bmatrix} v \\ n \end{bmatrix} / \begin{bmatrix} v-\tau \\ v-n \end{bmatrix}$,
2. *$\tau = \tau(\mathcal{C})$ and $\mathbf{d}(\mathcal{C}) = n - \tau + 1$,*
3. *$\mathcal{C}$ is a $\mathcal{S}_q(\tau, n, v)$.*

- Suppose $\mathcal{C} \subset J(v, n, q)$ is a $\mathcal{S}_q(\tau, n, v)$ with $q > 1$ then
  - $\mathbf{d}^*(\mathcal{C}) = \tau + 1$ and $s(\mathcal{C}) = \tau$,
  - $(n - \tau + 1)/2 \leq \rho(\mathcal{C}) \leq s^*(\mathcal{C}) \leq n - \tau$.
- If a $\mathcal{S}_q(\tau, n, v)$ exists then it is a regular design in $J(v, n, q)$.

Steiner Structures $q > 1$

Corollary

Let $\mathcal{C} \subset J(v, n, q)$ be a τ-design, then the following are equivalent

1. *$\mathcal{C}$ achieves the Johnson bound, i.e. $|\mathcal{C}| = \begin{bmatrix} v \\ n \end{bmatrix} / \begin{bmatrix} v-\tau \\ v-n \end{bmatrix}$,*
2. *$\tau = \tau(\mathcal{C})$ and $\mathbf{d}(\mathcal{C}) = n - \tau + 1$,*
3. *$\mathcal{C}$ is a $\mathcal{S}_q(\tau, n, v)$.*

- Suppose $\mathcal{C} \subset J(v, n, q)$ is a $\mathcal{S}_q(\tau, n, v)$ with $q > 1$ then
  - $\mathbf{d}^*(\mathcal{C}) = \tau + 1$ and $s(\mathcal{C}) = \tau$,
  - $(n - \tau + 1)/2 \leq \rho(\mathcal{C}) \leq s^*(\mathcal{C}) \leq n - \tau$.
- If a $\mathcal{S}_q(\tau, n, v)$ exists then it is a regular design in $J(v, n, q)$.
- If a $\mathcal{S}_q(2, n, v)$ exists then it is strongly regular graph.

Steiner Structures $q > 1$

Corollary

Let $\mathcal{C} \subset J(v, n, q)$ be a τ-design, then the following are equivalent

1. *$\mathcal{C}$ achieves the Johnson bound, i.e. $|\mathcal{C}| = \begin{bmatrix} v \\ n \end{bmatrix} / \begin{bmatrix} v-\tau \\ v-n \end{bmatrix}$,*
2. *$\tau = \tau(\mathcal{C})$ and $\mathbf{d}(\mathcal{C}) = n - \tau + 1$,*
3. *$\mathcal{C}$ is a $\mathcal{S}_q(\tau, n, v)$.*

- Suppose $\mathcal{C} \subset J(v, n, q)$ is a $\mathcal{S}_q(\tau, n, v)$ with $q > 1$ then
  - $\mathbf{d}^*(\mathcal{C}) = \tau + 1$ and $s(\mathcal{C}) = \tau$,
  - $(n - \tau + 1)/2 \leq \rho(\mathcal{C}) \leq s^*(\mathcal{C}) \leq n - \tau$.
- If a $\mathcal{S}_q(\tau, n, v)$ exists then it is a regular design in $J(v, n, q)$.
- If a $\mathcal{S}_q(2, n, v)$ exists then it is strongly regular graph.
- If a $\mathcal{S}_q(\tau, \tau + r, v)$ exists for $r \in \{1, 2\}$ then it is a completely regular design in $J(v, n, q)$ with $\rho = s^* = r$.

Some open problems

- For $q = 1$, does there exist a $\mathcal{S}_1(t, n, v)$ with $t > 5$?
- For $q > 1$, does there exist a $\mathcal{S}_q(t, n, v)$ with $t > 1$?
- In particular, $\mathcal{S}_1(2, 3, 7)$ exists (Fano plane), does $\mathcal{S}_2(2, 3, 7)$?
- For $q > 1$, does there exist a $\tau - (v, n, \lambda; q)$ with $t > 3$?
- There are no perfect codes in $J(v, n, q)$ for $q > 1$, are there any perfect codes in $J(v, n, 1)$?

References

- P. Delsarte *An algebraic approach to association schemes of coding theory.* *Phillips Res. Repts. Suppl.*,vol. 10, 1973.
- P. Delsarte *Association schemes and t-designs in regular semilattices.* *J. Combin. Theory Ser. A*,vol. 20, 1976.
- P. Delsarte *Hahn polynomials, discrete harmonics, and t-designs.* *J. Appl. Math.*,vol. 34, 1978.
- P. Delsarte *Bilinear forms over a finite field with applications coding theory.* *J. Combin. Theory Ser. A*,vol. 25, 1978.
- P. Delsarte and V.I. Levenshtein *Association schemes and coding theory.* *IEEE Trans. Inform. Theory*, vol.44, no.6, pp.2477-2504, Oct. 1998.
- T. Etzion and A. Vardy *q-Analogs of Steiner systems and covering designs.* arXiv:0912.1503, Dec., 2009.
- V.I. Levenshtein *Equivalence of Delsarte's bounds for codes and designs in symmetric association schemes and some applications.* *Disc. Math.*,vol. 197-198, 1999.
- M. Schwartz and T. Etzion *Codes and anticodes in the grassman graph.* *J. Combin. Theory Ser. A*,vol. 97, 2002.

This work was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.