Codes and Designs in the Grassmann Scheme

Tuvi Etzion

Computer Science Department
Technion -Israel Institute of Technology
etzion@cs.technion.ac.il

ALGEBRAIC COMBINATORICS AND APPLICATIONS
ALCOMA10, Thurnau, Germany, 13 April 2010

Joint work with Alexander Vardy

Outline

- Background
- Bounds on the Sizes of Codes
- Known Constructions for Constant Dimension Codes
- New Construction for Constant Weight Codes
- Definitions for q-Covering Designs
- Bounds on the Size of q-Covering Designs

Background

Definition

The projective space of order n over the finite field $\mathbb{F}_q$, denoted as $\mathcal{P}_q(n)$, is the set of all subspaces of the vector space $\mathbb{F}_q^n$.

Definition

The natural measure of distance in $\mathcal{P}_q(n)$ is given by

$$d(U,V) \stackrel{\text{def}}{=} \dim U + \dim V - 2\dim\big(U \cap V\big)$$

for all $U, V \in \mathcal{P}_q(n)$.

Definition

$\mathbb{C} \subseteq \mathcal{P}_q(n)$ is an (n, M, d) code in projective space if $|\mathbb{C}| = M$ and $d(U,V) \geq d$ for all U, V in $\mathbb{C}$.

Koetter and Kschischang [2007] showed that codes in $\mathbb{P}_q(n)$ are precisely what is needed for error-correction in networks.

Background

Definition

Given an integer $0 \leq k \leq n$, the set of all subspaces of $\mathbb{F}_q^n$ with dimension k is known as a Grassmannian, and denoted by $\mathcal{G}_q(n,k)$.

Definition

$\mathbb{C} \subseteq \mathcal{G}_q(n,k)$ is an (n,M,d,k) code in the Grassmannian if $|\mathbb{C}| = M$ and $d(U,V) \geq d$ for all U,V in $\mathbb{C}$.

Definition

A q-analog $t-(n,k,\lambda)$ design is a set $\mathbb{S}$ of k-dimensional subspaces (called blocks) from $\mathbb{F}_q^n$, such that each t-dimensional subspace of $\mathbb{F}_q^n$ is a subspace of exactly λ blocks from $\mathbb{S}$.

Background

q-analog designs:

Thomas [1987, 1996]
Suzuki [1990, 1992]
Miyakawa, Munemasa, and Yosihiara [1995]
Itoh [1998]
Ahlswede, Aydinian, and Khachatrian [2001]
Schwartz and Etzion [2002]
Braun, Kerber, and Laue [2005]

Bounds on the Sizes of Codes

Definition

A Steiner structure $S_q[r, k, n]$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n, k)$ such that each element from $\mathcal{G}_q(n, r)$ is contained in exactly one element of $\mathbb{S}$.

Definition

Let $\mathcal{A}_q(n, d, k)$ denote the maximum number of codewords in an (n, M, d, k) code in $\mathcal{G}_q(n, k)$.

Theorem

$\mathcal{A}_q(n, 2\delta + 2, k) \leq \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}$ with equality holds if and only if a Steiner structure $S_q[k - \delta, k, n]$ exists.

Bounds on the Sizes of Codes

Definition

For a set $\mathbb{S} \subset \mathcal{G}_q(n,k)$ let $\mathbb{S}^\perp$ be the orthogonal complement of $\mathbb{S}$:

$$\mathbb{S}^\perp = \{A^\perp \ : \ A \in \mathcal{S}\},$$

where $A^\perp \in \mathcal{G}_q(n,n-k)$ is the orthogonal complement of the subspace A.

Theorem (complements)

$\mathcal{A}_q(n,d,k) = \mathcal{A}_q(n,d,n-k)$.

Bounds on the Sizes of Codes

Theorem (Johnson)

- $\mathcal{A}_q(n, 2\delta, k) \leq \frac{q^n-1}{q^k-1}\mathcal{A}_q(n-1, 2\delta, k-1)$.
- $\mathcal{A}_q(n, 2\delta, k) \leq \frac{q^n-1}{q^{n-k}-1}\mathcal{A}_q(n-1, 2\delta, k)$.

Corollary

$$\mathcal{A}_q(n, 2\delta, k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n+1-r}-1}{q^{k+1-r}-1} \right\rfloor \cdots \right\rfloor \right\rfloor \leq \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

.

Lemma

$$\mathcal{A}_q(n, 2k, k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor - 1 \qquad \textit{if } n \not\equiv 0 \pmod{k}$$

Constant Dimension Codes (Steiner structure)

Construction

Let $n = sk$, $r = \frac{q^n-1}{q^k-1}$, *and let* α *be a primitive element in* $GF(q^n)$. *For each* i, $0 \leq i \leq r-1$, *we define*

$$H_i = \{\alpha^i, \alpha^{r+i}, \alpha^{2r+i}, \ldots, \alpha^{(q^k-2)r+i}\}.$$

The set $\{H_i \;:\; 0 \leq i \leq r-1\}$ *is a Steiner structure* $S_q[1,k,n]$.

Theorem

Let $n \equiv r \pmod{k}$. *Then, for all* q, *we have*

$$\mathcal{A}_q(n,2k,k) \geq \frac{q^n - q^k(q^r-1)-1}{q^k-1}$$

Constant Dimension Codes (Lifted Codes)

Definition

We can represent $X \in \mathcal{G}_q(n,k)$ by the k linearly independent vectors from X which form a unique $k \times n$ generator matrix in reduced row echelon form, denoted by $RE(X)$, and defined by:

- The leading coefficient of a row is always to the right of the leading coefficient of the previous row.
- All leading coefficients are *ones*.
- Every leading coefficient is the only nonzero entry in its column.

Definition

For each $X \in \mathcal{G}_q(n,k)$ we associate a binary vector of length n and weight k, $v(X)$, called the identifying vector of X, where the *ones* in $v(X)$ are in the positions where $RE(X)$ has the leading *ones*.

Constant Dimension Codes (Lifted Codes)

Example

Let X be the subspace in $\mathcal{G}_2(7,3)$ with the following generator matrix in reduced row echelon form:

$$RE(X) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Its identifying vector is $v(X) = 1011000$, and its echelon Ferrers form, Ferrers diagram, and Ferrers tableaux form are given by

$$\begin{bmatrix} 1 & \bullet & 0 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 0 & 1 & \bullet & \bullet & \bullet \end{bmatrix}, \quad \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \end{array}, \quad \text{and} \quad \begin{array}{cccc} 0 & 1 & 1 & 0 \\ & 1 & 0 & 1 \\ & 0 & 1 & 1 \end{array}.$$

Constant Dimension Codes (Lifted Codes)

Definition

For two $k \times \eta$ matrices A and B over $\mathbb{F}_q$ the rank distance is defined by $d_R(A,B) \overset{\text{def}}{=} \text{rank}(A-B)$.

Definition

A code $\mathcal{C}$ is an $[m \times \eta, \rho, \delta]$ rank-metric code if its codewords are $k \times \eta$ matrices over $\mathbb{F}_q$, they form a linear subspace of dimension ρ of $\mathbb{F}_q^{k \times \eta}$, and for $A, B \in \mathcal{C}$ we have that $d_R(A,B) \geq \delta$.

Theorem

Let $\mathcal{C}$ be an $[k \times \eta, \rho, \delta]$ rank-metric code. The subspaces spanned by the set of matrices in reduced row echelon form

$$\{[I_k \ A] \ : \ A \in \mathcal{C}\}$$

form a $(k+\eta, q^\rho, 2\delta, k)$ code (identifying vector $1 \ldots 10 \ldots 0$).

Constant Dimension Codes (Lifted Codes)

First codes constructed: Koetter and Kschischang [2007].

First lifted codes: Silva, Koetter and Kschischang [2008]

Multilevel Construction: Etzion and Silberstein [2009]

Constant Dimension Codes (Cyclic Codes)

Definition (Cyclic codes)

Let α be a primitive element of $GF(2^n)$. We say that a code $\mathbb{C}$ is cyclic if it has the following property: $\{\mathbf{0}, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_m}\}$ is a codeword of $\mathbb{C}$, so is its cyclic shift $\{\mathbf{0}, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_m+1}\}$. In other words, if we map each vector space $V \in \mathbb{C}$ into the corresponding binary characteristic vector $x_V = (x_0, x_1, \ldots, x_{2^n-2})$ given by

$$x_i = 1 \text{ if } \alpha^i \in V \qquad \text{and} \qquad x_i = 0 \text{ if } \alpha^i \notin V$$

then the set of all such characteristic vectors is closed under cyclic shifts.

Constant Dimension Codes (cyclic Codes)

- $\mathcal{A}_2(8,4,3) \geq 1275$ (compare to $\mathcal{A}_2(8,4,3) \leq 1493$)
- $\mathcal{A}_2(9,4,3) \geq 5694$ (compare to $\mathcal{A}_2(9,4,3) \leq 6205$)
- $\mathcal{A}_2(10,4,3) \geq 21483$ (compare to $\mathcal{A}_2(10,4,3) \leq 24698$)
- $\mathcal{A}_2(11,4,3) \geq 79833$ (compare to $\mathcal{A}_2(11,4,3) \leq 99718$)
- $\mathcal{A}_2(12,4,3) \geq 315315$ (compare to $\mathcal{A}_2(12,4,3) \leq 398385$)
- $\mathcal{A}_2(13,4,3) \geq 1154931$ (compare to $\mathcal{A}_2(13,4,3) \leq 1597245$)
- $\mathcal{A}_2(14,4,3) \geq 4177665$ (compare to $\mathcal{A}_2(14,4,3) \leq 6387029$)

Kohnert and Kurz [2008]

Etzion and Vardy [2008]

New Construction for Constant Weight Codes

Construction (COS - cosets of constant dimension code)

Let $\mathbb{C}$ *be an* (n, M, d, k) *code. From* $X = \{0, \alpha_1, \ldots, \alpha_{2^k-1}\} \in \mathbb{C}$ *we form the following set of words with weight* 2^k*:*

$$\mathcal{C}_X = \{\{\beta, \beta + \alpha_1, \beta + \alpha_2, \ldots, \beta + \alpha_{2^k-1}\} \ : \ \beta \in \mathbb{F}_2^n\} \ .$$

The words of $\mathcal{C}_x$ *represent the cosets of the the* k*-dimensional subspace* X*. Therefore,* $|\mathcal{C}_X| = 2^{n-k}$*. We define our code* $\mathcal{C}$ *as the union of all the sets* $\mathcal{C}_X$ *over all codewords of* $\mathbb{C}$*, i.e.,*

$$\mathcal{C} = \bigcup_{X \in \mathbb{C}} \mathcal{C}_X = \{\{\beta, \beta + \alpha_1, \beta + \alpha_2, \ldots, \beta + \alpha_{2^k-1}\} \ : \ \{0, \alpha_1, \ldots, \alpha_{2^k-1}\} \in \mathbb{C}, \ \beta \in \mathbb{F}_2^n\} \ .$$

New Construction for Constant Weight Codes

Theorem

If $\mathbb{C}$ is an $[n, M, d = 2t, k]$ code then $\mathcal{C}$ of Construction COS is a $(2^n, 2^{n-k}M, 2^{k+1} - 2^{k-t+1}, 2^k)$ code.

Example

Let $\mathbb{C}$ be and an $[n, \frac{(2^n-1)(2^{n-1}-1)}{3}, 2, 2]$ code which consists of all 2-dimensional subspaces of $\mathbb{F}_2^n$. $\mathcal{C}$ is a $(2^n, \frac{(2^n-1)(2^{n-1}-1)2^{n-2}}{3}, 4, 4)$ code forming the codewords of weight four in the extended Hamming code of length 2^n, i.e., a Steiner system $S(3, 4, 2^n)$.

Example

Let $\mathbb{C}$ be an $[n, 2^n - 1, 2, n-1]$ code (all $(n-1)$-dimensional subspaces of $\mathbb{F}_2^n$). $\mathcal{C}$ is a $(2^n, 2^{n+1} - 2, 2^{n-1}, 2^{n-1})$. If we join to $\mathcal{C}$ the allone and the allzero codewords then the formed code is a Hadamard code (a Hadamard matrix and its complement).

New Construction for Constant Weight Codes

Definition

$A(n, d, w)$ is the maximum size of a binary constant weight code of length n, weight w, and minimum Hamming distance d.

Theorem (Johnson)

If $n \geq w > 0$ *then*

$$A(n, d, w) \leq \left\lfloor \frac{n}{w} A(n-1, d, w-1) \right\rfloor$$

.

New Construction for Constant Weight Codes

Theorem (Agrell, Vardy, Zeger)

If $b > 0$ *then*

$$A(n, 2\delta, w) \leq \left\lfloor \frac{\delta}{b} \right\rfloor,$$

where

$$b = \delta - \frac{w(n-w)}{n} + \frac{n}{M^2}\left\{M\frac{w}{n}\right\}\left\{M\frac{n-w}{n}\right\}$$

$$M = A(n, 2\delta, w)$$

$$\{x\} = x - \lfloor x \rfloor$$

.

New Construction for Constant Weight Codes

Theorem

- $A(2^{2m-1}-1, 2^{m+1}-4, 2^m-1) = 2^m+1$.
- $A(2^{2m-1}, 2^{m+1}-4, 2^m) = 2^{2m-1}+2^{m-1}$.

Proof.

The upper bound $A(2^{2m-1}-1, 2^{m+1}-4, 2^m-1) \leq 2^m+1$ is a direct application of AVZ Theorem. Using this bound in Johnson Theorem we obtain $A(2^{2m-1}, 2^{m+1}-4, 2^m) \leq 2^{2m-1}+2^{m-1}$. By applying Construction COS on a $[2m-1, 2^m+1, 2m-2, m]$ code we obtain a $(2^{2m-1}, 2^{2m-1}+2^{m-1}, 2^{m+1}-4, 2^m)$ code. Hence, $A(2^{2m-1}, 2^{m+1}-4, 2^m) \geq 2^{2m-1}+2^{m-1}$ and thus $A(2^{2m-1}, 2^{m+1}-4, 2^m) = 2^{2m-1}+2^{m-1}$. By shortening the $(2^{2m-1}, 2^{2m-1}+2^{m-1}, 2^{m+1}-4, 2^m)$ code we obtain a $(2^{2m-1}-1, 2^m+1, 2^{m+1}-4, 2^m-1)$ code and hence $A(2^{2m-1}-1, 2^{m+1}-4, 2^m-1) = 2^m+1$. □

New Construction for Constant Weight Codes

Theorem

If a Steiner Structure $S_2[2, k, n]$ *exists then a Steiner system* $S(3, 2^k, 2^n)$ *exists.*

Theorem

If a Steiner Structure $S_2[2, 3, 7]$ *exists then a Steiner system* $S(3, 8, 128)$ *exists.*

Definitions for q-Covering Designs

Definition

A q-covering design $C_q[n,k,r]$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,r)$ is contained in at least one element of $\mathbb{S}$.

Definition

A q-Turán design $T_q[n,k,r]$ is a collection $\mathbb{S}$ of elements from $\mathcal{G}_q(n,r)$ such that each element of $\mathcal{G}_q(n,k)$ contains at least one element from $\mathbb{S}$.

Definitions for q-Covering designs

Definition

The q-covering number $\mathcal{C}_q(n,k,r)$ is the minimum size of a q-covering design $C_q[n,k,r]$.

Definition

The q-Turán number $\mathcal{T}_q(n,k,r)$ is the minimum size of a q-Turán design $T_q[n,k,r]$.

Basic Bounds on q-Covering numbers

Theorem

$\mathbb{S}$ is a q-covering design $C_q[n,k,r]$ if and only if $\mathbb{S}^\perp$ is a q-Turán design $T_q[n,n-r,n-k]$.

Corollary

$\mathcal{C}_q(n,k,r) = \mathcal{T}_q(n,n-r,n-k)$.

Basic Bounds on q-Covering numbers

Theorem

$\mathcal{C}_q(n,k,r) \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}_q}{\begin{bmatrix} k \\ r \end{bmatrix}_q}$ *with equality holds if and only if a Steiner structure* $S_q[r,k,n]$ *exists.*

Theorem

$\mathcal{T}_q(n,k,r) \leq \begin{bmatrix} n-k+r \\ r \end{bmatrix}_q$.

Corollary

$\mathcal{C}_q(n,k,r) = \mathcal{T}_q(n,n-r,n-k) \leq \begin{bmatrix} n-k+r \\ r \end{bmatrix}_q$.

Optimal q-Covering Designs

Theorem

$\mathcal{C}_q(n,k,1) = \mathcal{T}_q(n,n-1,n-k) = \left|\mathbb{S}_q[1,k,n]\right| = \frac{q^n-1}{q^k-1}$, *whenever* k *divides* n.

Theorem

If $1 \leq k \leq n$, *then* $\mathcal{C}_q(n,k,1) = \lceil \frac{q^n-1}{q^k-1} \rceil$.

Theorem

If $1 \leq k \leq n-1$, *then* $\mathcal{C}_q(n,n-1,k) = \frac{q^{k+1}-1}{q-1}$.

Upper Bounds on the Size of q-Covering Designs

Theorem (Recursive Construction)

$\mathcal{C}_q(n,k,r) \leq q^{n-k}\mathcal{C}_q(n-1,k-1,r-1) + \mathcal{C}_q(n-1,k,r)$.

Proof.

We represent $\mathbb{F}_q^n$ by $\{(\alpha,\beta) \ : \ \alpha \in \mathbb{F}_q^{n-1}, \ \beta \in \mathbb{F}_q\}$. Let $\mathbb{S}_1$ be a q-covering design $C_q[n-1,k-1,r-1]$ and $\mathbb{S}_2$ be a q-covering design $C_q[n-1,k,r]$. We form a set $\mathbb{S}$ as follows:

- For each subspace $P = \{0, \alpha_1, \cdots, \alpha_{q^{k-1}-1}\} \in \mathbb{S}_1$ let $P_1 = P, P_2, \ldots, P_{q^{n-k}}$ be the disjoint cosets of P in $\mathbb{F}_q^{n-1}$. Let $\beta_0 = 0, \beta_1, \ldots, \beta_{q^{n-k}}$ be any q^{n-k} coset representatives, i.e., $\beta_i \in P_i$, $1 \leq i \leq q^{n-k}$. For each $1 \leq i \leq q^{n-k}$ we form the subspace $\left\langle \{(\alpha_1,0), \cdots, (\alpha_{q^{k-1}-1},0), (\beta_i,1)\} \right\rangle$ in $\mathbb{S}$.
- For each subspace $\{0, \alpha_1, \cdots, \alpha_{q^k-1}\} \in \mathbb{S}_2$ the subspace $\{(0,0), (\alpha_1,0), \cdots, (\alpha_{q^k-1},0)\}$ is formed in $\mathbb{S}$.

$\mathbb{S}$ is a q-covering design $C_q[n,k,r]$ and the theorem follows. $\square$

Lower Bounds on the Size of q-Covering Designs

Theorem

$\mathcal{C}_q(n,k,r) \geq \lceil \frac{q^n-1}{q^k-1} \mathcal{C}_q(n-1,k-1,r-1) \rceil$.

Corollary

$$\mathcal{C}_q(n,k,r) \geq \lceil \frac{q^n-1}{q^k-1} \lceil \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \lceil \frac{q^{n+1-r}-1}{q^{k+1-r}-1} \rceil \cdots \rceil \rceil \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}_q}{\begin{bmatrix} k \\ r \end{bmatrix}_q}.$$

Theorem

$\mathcal{T}_q(n,r+1,r) \geq \frac{(q^{n-r}-1)(q-1)}{(q^r-1)^2} \begin{bmatrix} n \\ r-1 \end{bmatrix}_q$.

Corollary

$\mathcal{C}_q(n,k,k-1) \geq \frac{(q^k-1)(q-1)}{(q^{n-k}-1)^2} \begin{bmatrix} n \\ k+1 \end{bmatrix}_q$.

Some Specific Bounds

Theorem

$\mathcal{C}_2(5,3,2) = 27$. *(compared to* $\mathcal{C}_2(5,3,2) \geq 23$ *by previous theorem).*

Theorem

$381 \leq \mathcal{C}_2(7,3,2) \leq 399$.

Theorem

$304 \leq \mathcal{A}_2(7,4,3) \leq 381$.

THANK YOU