Bounds and Constructions of Constant Dimension Subspace Codes

Anna-Lena Trautmann

Institute of Mathematics
University of Zurich

5th Workshop on Coding and Systems
Dublin, September 2-4 2009
Introduction

Subspace codes recently received a lot of attention since Koetter and Kschischang showed that they are exactly what is needed for error-correction in random network coding.
**Introduction**

Subspace codes recently received a lot of attention since Koetter and Kschischang showed that they are exactly what is needed for error-correction in random network coding.

**Network Coding**

We can optimize the throughput by doing linear combinations on the intermediate nodes.

![Diagram of network coding](image)
Introduction

Subspace codes recently received a lot of attention since Koetter and Kschischang showed that they are exactly what is needed for error-correction in random network coding.

Network Coding
We can optimize the throughput by doing linear combinations on the intermediate nodes.

Random Network Coding
Subspaces remain the same under any linear operations on the basis vectors.
The *generalized projective space* $\mathcal{P}_q(n)$ of order $n$ over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension $k$ is the *Grassmannian* $\mathcal{G}_q(k, n)$. 

A metric on $\mathcal{P}_q(n)$ is given by $d_S(U, V) := \dim U + \dim V - 2 \dim(U \cap V)$. In $\mathcal{G}_q(k, n)$ it turns to $d_S(U, V) = 2(k - \dim(U \cap V))$. 

A subspace code is simply a subset of $\mathcal{P}_q(n)$, a *constant dimension code* (CDC) is a subset of $\mathcal{G}_q(k, n)$. If the distance between any two elements of a CDC is greater than or equal to $2\delta$ we say that the code has minimum distance $2\delta$. 


The *generalized projective space* $\mathcal{P}_q(n)$ of order $n$ over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}^n_q$. The set of all subspaces of dimension $k$ is the *Grassmannian* $\mathcal{G}_q(k, n)$.

A metric on $\mathcal{P}_q(n)$ is given by

$$d_S(U, V) := \dim U + \dim V - 2 \dim(U \cap V)$$

In $\mathcal{G}_q(k, n)$ it turns to

$$d_S(U, V) = 2(k - \dim(U \cap V))$$
The *generalized projective space* $\mathcal{P}_q(n)$ of order $n$ over $\mathbb{F}_q$ is the set of all subspaces of $\mathbb{F}_q^n$. The set of all subspaces of dimension $k$ is the *Grassmannian* $\mathcal{G}_q(k, n)$.

A metric on $\mathcal{P}_q(n)$ is given by

$$d_S(U, V) := \dim U + \dim V - 2 \dim(U \cap V)$$

In $\mathcal{G}_q(k, n)$ it turns to

$$d_S(U, V) = 2(k - \dim(U \cap V))$$

A *subspace code* is simply a subset of $\mathcal{P}_q(n)$, a *constant dimension code (CDC)* is a subset of $\mathcal{G}_q(k, n)$. If the distance between any two elements of a CDC is greater than or equal to $2\delta$ we say that the code has minimum distance $2\delta$. 
$A_q[n, 2\delta, k]$ is the maximal cardinality of a code in $G_q(k, n)$ with minimum distance $2\delta$. It holds that $A_q[n, 2\delta, k] = A_q[n - k, 2\delta, k]$ (orthogonal complement). Therefor we restrict our studies to the case $2k < n$. 
$A_q[n, 2\delta, k]$ is the maximal cardinality of a code in $\mathcal{G}_q(k, n)$ with minimum distance $2\delta$. It holds that $A_q[n, 2\delta, k] = A_q[n - k, 2\delta, k]$ (orthogonal complement). Therefore we restrict our studies to the case $2k < n$.

The \textit{q-binomial coefficients} (or \textit{Gauss coefficients}) are defined as

$$\left[ \begin{array}{c} n \\ k \end{array} \right]_q := \frac{(q^n - 1)(q^{n-1} - 1) \ldots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \ldots (q - 1)}$$

for $1 \leq k \leq n$. It is a well-known result that

$$|\mathcal{G}_q(k, n)| = \left[ \begin{array}{c} n \\ k \end{array} \right]_q$$
Upper Bounds

- Sphere packing

\[
A_q[n, 2\delta, k] \leq \sum_{i=0}^{\left\lfloor \frac{\delta - 1}{2} \right\rfloor} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n - k \\ i \end{bmatrix}_q
\]

- Wang-Xing-Safavi-Naini

\[
A_q[n, 2\delta, k] \leq \begin{bmatrix} n \\ k - \delta + 1 \end{bmatrix}_q \begin{bmatrix} k \\ k - \delta + 1 \end{bmatrix}_q
\]
• **Singleton-like**

\[ A_q[n, 2\delta, k] \leq \left\lfloor \frac{n - \delta + 1}{n - k} \right\rfloor_q \]

• **Johnson-type I**

\[ A_q[n, 2\delta, k] \leq \left\lfloor \frac{(q^{n-k} - q^{n-k-\delta})(q^n - 1)}{(q^{n-k-1})^2 - (q^n - 1)(q^{n-k-\delta} - 1)} \right\rfloor \]

• **Johnson-type II**

\[ A_q[n, 2\delta, k] \leq \left\lfloor \frac{q^n - 1}{q^k - 1} A_q[n - 1, 2\delta, k - 1] \right\rfloor \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \cdots \left\lfloor \frac{q^{n-k+\delta} - 1}{q^\delta - 1} \right\rfloor \cdots \right\rfloor \]
Bounds and Constructions of Constant Dimension Subspace Codes

Anna-Lena Trautmann

Lower Bounds

- Sphere covering

\[ A_q[n, 2\delta, k] \geq \frac{\binom{n}{k}_q}{\sum_{i=0}^{\delta-1} q^{i^2} \binom{k}{i}_q \binom{n-k}{i}_q} \]

- Constructive bounds
Lifted MRD Codes

Let $A, B \in \text{Mat}_q(m \times n)$ and $d_R := \text{rk}(A - B)$ be the rank distance. A maximum rank distance (MRD) code is a subset of $\text{Mat}_q(m \times n)$ with minimum distance $d$ and size $q^{n(m-d+1)}$ (if $m < n$), which is maximal. MRD codes exist for any set of parameters $m, n \geq d$. (Gabidulin)
Lifted MRD Codes

Let $A, B \in \text{Mat}_q(m \times n)$ and $d_R := rk(A - B)$ be the rank distance. A **maximum rank distance (MRD) code** is a subset of $\text{Mat}_q(m \times n)$ with minimum distance $d$ and size $q^{n(m-d+1)}$ (if $m < n$), which is maximal. MRD codes exist for any set of parameters $m, n \geq d$. (Gabidulin)

**Lifting** an MRD code $G$ (with minimum distance $d$), i.e.

$$\{\text{rowspace } [ I_{m \times m} \ G_i ] | G_i \in G \}$$

leads to a $[m + n, q^{n(m-d+1)}, 2d, m]$-subspace-code. (Koetter and Kschischang)
Lifted MRD Codes

Let $A, B \in \text{Mat}_q(m \times n)$ and $d_R := \text{rk}(A - B)$ be the rank distance. A **maximum rank distance** (MRD) code is a subset of $\text{Mat}_q(m \times n)$ with minimum distance $d$ and size $q^{n(m-d+1)}$ (if $m < n$), which is maximal. MRD codes exist for any set of parameters $m, n \geq d$. (Gabidulin)

**Lifting** an MRD code $G$ (with minimum distance $d$), i.e.

$$\{\text{rowspace } [ I_{m \times m} \ G_i ] | G_i \in G\}$$

leads to a $[m + n, q^{n(m-d+1)}, 2d, m]$-subspace-code. (Koetter and Kschischang)

**Theorem**

$$A_q[n, 2\delta, k] \geq q^{(n-k)(k-\delta+1)}$$
A New Family of RS-like Codes

Appending 0-columns in front of all code elements does not change the minimum distance. Thus

\[
\{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times l} & I_{k \times k} & M_{k \times n-l-k} \end{array} \right] | M \in \text{MRD}^\delta \text{-code} \}
\]

is a \([n, q^{(n-l-k)(k-\delta+1)}, 2\delta, k]\)-code.
A New Family of RS-like Codes

Appending 0-columns in front of all code elements does not change the minimum distance. Thus

\[
\{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times l} & I_{k \times k} & M_{k \times n-l-k} \end{array} \right] | M \in \text{MRD}^\delta\text{-code} \}
\]

is a \([n, q^{(n-l-k)(k-\delta+1)}, 2\delta, k]\)-code.

Let \( l = j \cdot k \) and construct the component codes

\[
C_j = \{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times j \cdot k} & I_{k \times k} & M_{k \times n-(j+1)k} \end{array} \right] \}
\]
A New Family of RS-like Codes

Appending 0-columns in front of all code elements does not change the minimum distance. Thus

$$\{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times l} & I_{k \times k} & M_{k \times n - l - k} \end{array} \right] | M \in \text{MRD}^\delta\text{-code} \}$$

is a $[n, q^{(n-l-k)(k-\delta+1)}, 2\delta, k]$-code.

Let $l = j \cdot k$ and construct the component codes

$$C_j = \{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times j \cdot k} & I_{k \times k} & M_{k \times n - (j+1)k} \end{array} \right] \}$$

Two elements of different component codes intersect pairwise only trivially. Hence

$$C = \bigcup_{j=0}^{\left\lfloor \frac{n}{k} \right\rfloor - 1} C_j$$

is a $[n, N, 2\delta, k]$-code with size $N = \sum |C_j|$. 
We can increase the size by choosing $l = j \cdot \delta$:

$$C_j = \{ \text{rs} \left[ \begin{array}{ccc} 0_{k \times j \cdot \delta} & I_{k \times k} & M_{k \times n-k-j \cdot \delta} \end{array} \right] \}$$

$$C = \bigcup_{j=0}^{\left\lfloor \frac{n-k}{\delta} \right\rfloor} C_j$$
We can increase the size by choosing \( l = j \cdot \delta \):

\[
C_j = \{ rs \begin{bmatrix} 0_{k \times j \cdot \delta} & I_{k \times k} & M_{k \times n-k-j \cdot \delta} \end{bmatrix} \}
\]

\[
C = \bigcup_{j=0}^{\left\lfloor \frac{n-k}{\delta} \right\rfloor} C_j
\]

**Theorem**

The above constructed code \( C \) is a \([n, N, 2\delta, k] \)-code of size

\[
N = \sum_{i=0}^{\left\lfloor \frac{n-2k}{\delta} \right\rfloor} q^{(k-\delta+1)(n-k-\delta i)} + \sum_{i=\left\lfloor \frac{n-2k}{\delta} \right\rfloor+1}^{\left\lfloor \frac{n-k}{\delta} \right\rfloor} q^{k(n-k+1-\delta(i+1))}
\]

In the case of \( k = \delta, n \equiv r \mod k \), it holds that

\[
N = \frac{q^n - q^k (q^r - 1) - 1}{q^k - 1} = \frac{q^n - q^{r+k}}{q^k - 1} + 1
\]
Proof.

- Minimum distance: It is clear that the distance between any elements of the same component code $C_i$ is greater or equal to $2\delta$. Now let $U \in C_i$ and $V \in C_{i+1}$. Since the identity blocks are shifted by $\delta$ positions, the maximal intersection is $(k - \delta)$-dimensional. Thus

\[ d_S(U, V) = 2k - 2 \dim(U \cap V) \geq 2k - 2(k - \delta) = 2\delta \]
Proof.

- Minimum distance: It is clear that the distance between any elements of the same component code $C_i$ is greater or equal to $2\delta$. Now let $U \in C_i$ and $V \in C_{i+1}$. Since the identity blocks are shifted by $\delta$ positions, the maximal intersection is $(k - \delta)$-dimensional. Thus

$$d_S(U, V) = 2k - 2 \dim(U \cap V) \geq 2k - 2(k - \delta) = 2\delta$$

- Size of the code: The subspace component code is as large as the corresponding MRD code, thus

$$|C_i| = \begin{cases} 
q^{(n-k-\delta i)(k-\delta+1)} & \text{for } n - \delta i \geq 2k \\
q^{k(n-k+1-\delta(i+1))} & \text{for } n - \delta i < 2k 
\end{cases}$$
Corollary

If $2\delta = 2k$ and \( \begin{cases} n \equiv 0 \mod k \\ n \equiv 1 \mod k \text{ and } q = 2 \end{cases} \) these codes are optimal.
Corollary

If $2\delta = 2k$ and \( \begin{cases} n \equiv 0 \mod k \\ n \equiv 1 \mod k \text{ and } q = 2 \end{cases} \) these codes are optimal.

Proof.

- For $n \equiv 0 \mod k$

\[
\frac{q^n - q^{k+n-k\lfloor \frac{n}{k} \rfloor}}{q^k - 1} + 1 = \frac{q^n - q^k}{q^k - 1} + 1 = \frac{q^n - 1}{q^k - 1}
\]
Corollary

If \( 2\delta = 2k \) and \( \begin{cases} n \equiv 0 \mod k \\ n \equiv 1 \mod k \text{ and } q = 2 \end{cases} \) these codes are optimal.

Proof.

- For \( n \equiv 0 \mod k \)

\[
\frac{q^n - q^{k+n-k\lfloor \frac{n}{k} \rfloor}}{q^k - 1} + 1 = \frac{q^n - q^k}{q^k - 1} + 1 = \frac{q^n - 1}{q^k - 1}
\]

- For \( n \equiv 1 \mod k \) the upper bound can be tightened to \( \lfloor \frac{q^n - 1}{q^k - 1} \rfloor - 1 \). (Etzion and Vardy)

\[
\frac{q^n - q^{k+n-k\lfloor \frac{n}{k} \rfloor}}{q^k - 1} + 1 = \lfloor \frac{q^n - 1}{q^k - 1} \rfloor - 1
\]

\[
\vdots
\]

\[\Leftrightarrow \quad 2q^k - q^{k+1} + q = 2 \]
Echelon-Ferrers Construction

1. Choose a binary linear code of length \( n \), weight \( k \) and minimum distance \( \delta \) as skeleton code. It is not yet known which skeleton code leads to the largest subspace code, but lexicodes seem to be good.
Echelon-Ferrers Construction

1. Choose a binary linear code of length $n$, weight $k$ and minimum distance $\delta$ as skeleton code. It is not yet known which skeleton code leads to the largest subspace code, but lexicodes seem to be good.

2. Build the echelon-Ferrers form of each code element, where the position of the 1’s in the skeleton code word mark the positions of the leading 1’s in each row and the ”free-to-choose”-positions build a Ferrers diagram.
Echelon-Ferrers Construction

1. Choose a binary linear code of length $n$, weight $k$ and minimum distance $\delta$ as skeleton code. It is not yet known which skeleton code leads to the largest subspace code, but lexicodes seem to be good.

2. Build the echelon-Ferrers form of each code element, where the position of the 1’s in the skeleton code word mark the positions of the leading 1’s in each row and the ”free-to-choose”-positions build a Ferrers diagram.

3. Fill the Ferrers diagrams with a compatible rank distance code with minimum distance $\delta$. 
Echelon-Ferrers Construction

1. Choose a binary linear code of length $n$, weight $k$ and minimum distance $\delta$ as skeleton code. It is not yet known which skeleton code leads to the largest subspace code, but lexicodes seem to be good.

2. Build the echelon-Ferrers form of each code element, where the position of the 1’s in the skeleton code word mark the positions of the leading 1’s in each row and the ”free-to-choose”-positions build a Ferrers diagram.

3. Fill the Ferrers diagrams with a compatible rank distance code with minimum distance $\delta$.

4. If we look at the rowspace of the above constructed matrices we get a $[n, N, 2\delta, k]$-subspace code.

(Etzion and Silberstein)
Example

We want to construct a [6, 4, 3]-code, hence we start with a binary linear code of length 6, weight 3 and distance 2:

\[(111000), (100110), (010101)\]

The corresponding echelon-Ferrers forms are:

\[
\begin{pmatrix}
1 & 0 & 0 & \bullet & \bullet & \bullet \\
0 & 1 & 0 & \bullet & \bullet & \bullet \\
0 & 0 & 1 & \bullet & \bullet & \bullet \\
\end{pmatrix}, 
\begin{pmatrix}
1 & \bullet & \bullet & 0 & 0 & \bullet \\
0 & 0 & 0 & 1 & 0 & \bullet \\
0 & 0 & 0 & 0 & 1 & \bullet \\
\end{pmatrix},
\]

\[
\begin{pmatrix}
0 & 1 & \bullet & 0 & \bullet & 0 \\
0 & 0 & 0 & 1 & \bullet & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}
\]

We can fill the Ferrers diagrams with rank distance codes of size \(q^6, q^2\) and \(q\) respectively.
Theorem

Let $\mathcal{F}$ be a Ferrers-diagram code, i.e. a rank-distance code that has 0’s in all positions that are not in the corresponding Ferrers diagram.

$$\Rightarrow |\mathcal{F}| \leq q^{\min_i \{v_i\}}$$

where $v_i$ is the number of dots in $\mathcal{F}$ which are not contained in the first $i$ rows and the rightmost $\delta - 1 - i$ columns ($0 \leq i \leq \delta - 1$). Moreover equality holds for (at least) $\delta = 1, 2$. (Etzion, Silberstein)
Theorem

Let $\mathcal{F}$ be a Ferrers-diagram code, i.e. a rank-distance code that has 0’s in all positions that are not in the corresponding Ferrers diagram.

$$\Rightarrow |\mathcal{F}| \leq q^{\min_i \{v_i\}}$$

where $v_i$ is the number of dots in $\mathcal{F}$ which are not contained in the first $i$ rows and the rightmost $\delta - 1 - i$ columns ($0 \leq i \leq \delta - 1$). Moreover equality holds for (at least) $\delta = 1, 2$. (Etzion, Silberstein)

Example

Let $\delta = 2$. All of the following Ferrers diagrams have $\min v_i = 3$:
A New Skeleton Code

Some skeleton code words lead to a Ferrers diagram where we can remove dots and still achieve the same size of the corresponding Ferrers code. We will call these removable dots \textit{pending dots}.
A New Skeleton Code

Some skeleton code words lead to a Ferrers diagram where we can remove dots and still achieve the same size of the corresponding Ferrers code. We will call these removable dots **pending dots**.

We can improve the size of our subspace codes if we take those pending dots into account. We can use the same row vector several times if we choose the pending dots differently.
A New Skeleton Code

Some skeleton code words lead to a Ferrers diagram where we can remove dots and still achieve the same size of the corresponding Ferrers code. We will call these removable dots **pending dots**.

We can improve the size of our subspace codes if we take those pending dots into account. We can use the same row vector several times if we choose the pending dots differently.

There are two options how to use this: either looking at an existing EF-code and filling in compatible EF-forms or starting with a first skeleton code word, using the above mentioned and then looking for the next suitable skeleton code word in lexicographic order.
Example

We want to construct a $[7, N, 4, 3]$-code. The second lexicographic skeleton code word is $(1001100)$, thus

$$
\begin{pmatrix}
1 & \bullet & \bullet & 0 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 0 & 1 & \bullet & \bullet
\end{pmatrix}
$$

Instead of using the next skeleton code word $(1000011)$ we use

$$
\begin{pmatrix}
1 & 0 & \bullet & 0 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 0 & 1 & \bullet & \bullet
\end{pmatrix}, \quad
\begin{pmatrix}
1 & 1 & \bullet & 0 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\
0 & 0 & 0 & 0 & 0 & 1 & \bullet
\end{pmatrix}
$$

and still maintain the minimum distance.
### Table of Code Sizes

<table>
<thead>
<tr>
<th>n</th>
<th>$2\delta$</th>
<th>k</th>
<th>RSC</th>
<th>family of RSC</th>
<th>lexico-EFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td>2</td>
<td>$q^3$</td>
<td>$q^3 + 1$</td>
<td>$q^3 + 1$</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>3</td>
<td>$q^6$</td>
<td>$q^6 + 1$</td>
<td>$q^6 + q^2 + q + 1$</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>3</td>
<td>$q^8$</td>
<td>$q^8 + 2$</td>
<td>$q^8 + q^4 + q^3 + q^2 + 2q + 1$</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>3</td>
<td>$q^4$</td>
<td>$q^4 + 1$</td>
<td>$q^4 + 1$</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>3</td>
<td>$q^{10}$</td>
<td>$q^{10} + q^6 + 1$</td>
<td>$q^{10} + q^6 + q^5 + 2q^4 + q^3 + q^2$</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>3</td>
<td>$q^{12}$</td>
<td>$q^{12} + q^8 + 2$</td>
<td>$q^{12} + q^8 + q^7 + 2q^6 + q^5 + q^4 + 1$</td>
</tr>
</tbody>
</table>

Improvement on the EFC with the new skeleton code:

- $[7, 4, 3] \quad q^8 + q^4 + q^3 + 2q^2 + q + 1$
- $[8, 4, 3] \quad q^{10} + q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1$
- $[9, 4, 3] \quad q^{12} + q^8 + q^7 + 2q^6 + 2q^5 + 3q^4 + 2q^3 + 2q^2 + q + 1$
Kohnert and Kurz constructed binary constant dimension codes which are larger than the before mentioned constructions for some parameters, e.g.:

\[ |[8, 4, 3]_{KK}| = 1275 \quad |[8, 4, 3]_{NEF}| = 1179 \]
\[ |[9, 4, 3]_{KK}| = 5621 \quad |[9, 4, 3]_{NEF}| = 4747 \]

In other cases the improved echelon-Ferrers codes are the largest codes known so far.
Kohnert and Kurz constructed binary constant dimension codes which are larger than the before mentioned constructions for some parameters, e.g.:

\[
|[8, 4, 3]_{KK}| = 1275 \quad |[8, 4, 3]_{NEF}| = 1179 \\
|[9, 4, 3]_{KK}| = 5621 \quad |[9, 4, 3]_{NEF}| = 4747
\]

In other cases the improved echelon-Ferrers codes are the largest codes known so far.

For many parameters there is still a big gap between the size of the largest code found so far and the lowest upper bound, e.g.

\[
A_2[8, 4, 3] \leq 1542 \\
A_2[9, 4, 3] \leq 6205
\]
Thank you for your attention!