Network Coding and Related Combinatorial Structures

Tuvi Etzion

Lecture 9

Constructions of Subspace Codes
Constructions of Subspace Codes

Outline

- Ferrers diagrams rank-metric codes
- Multilevel construction
- Punctured codes
- Cyclic codes
- Linearized and subspace polynomials
Subspace Codes

\((n, M, d)\) code is a set of \(M\) subspaces of \(P_q(n)\) with minimum subspace (injection) distance \(d\).

\((n, M, 2\delta, k)_q\) code is a set of \(M\) subspaces of \(G_q(n, k)\) with minimum subspace distance \(2\delta\).

\(A_q(n, d)\) is the maximum number of codewords in an \((n, M, d)\) code in \(P_q(n)\).

\(A_q(n, d, k)\) is the maximum number of codewords in an \((n, M, 2\delta, k)_q\) code.
A $[k \times m, \varrho, \delta]_q$ code satisfies
$$\varrho \leq \min\{k(m - \delta + 1), m(k - \delta + 1)\}$$

There exists a $[k \times m, \varrho, \delta]_q$ code which satisfies
$$\varrho = \min\{k(m - \delta + 1), m(k - \delta + 1)\}$$

If $A$ is an $k \times m$ matrix then $[I A]$ is a generator matrix of a $k$-dimensional subspace of $\mathbb{F}^{m+k}_q$.

If $C$ is a $[k \times m, \varrho, \delta]_q$ code then $C = \{[[I X]] : X \in C\}$ is a code in $G_q(m + k, k)$ with $d_S(C) = 2\delta$. 

Theorem

Theorem

Lemma
Lifted Rank-Metric Codes

**Lemma**

If $A$ is an $k \times m$ matrix then $[IA]$ is a generator matrix of a $k$-dimensional subspace of $\mathbb{F}_{q}^{m+k}$.

The subspace $\langle [IA] \rangle$ is called the lifting of $A$.

**Theorem**

If $C$ is a $[k \times m, q, \delta]_q$ code then $\mathcal{C} = \{ \langle [I X] \rangle : X \in C \}$ is a code in $G_q(m+k, k)$ with $d_S(\mathcal{C}) = 2\delta$.

The code $\mathcal{C} = \{ \langle [I X] \rangle : X \in C \}$ is the lifting of $C$. 
A $k \times n$ matrix with rank $k$ is in reduced row echelon form if the following conditions are satisfied.

- 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.

A $k$-dimensional subspace $X$ of $\mathbb{F}_q^n$ can be represented by a $k \times n$ generator matrix whose rows form a basis for $X$. The row echelon form of $X$ will be denoted by $E(X)$. 
A \( k \times n \) matrix with rank \( k \) is in reduced row echelon form if the following conditions are satisfied.

- 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.

\[
E(X) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\]
A Ferrers diagram represents partitions as patterns of dots with the $i$th row having the same number of dots as the $i$th term in the partition. A Ferrers diagram satisfies the following conditions.

- The number of dots in a row is at most the number of dots in the previous row.
- All the dots are shifted to the right of the diagram.

$(21) = 5 + 5 + 4 + 3 + 3 + 1$
Identifying Vectors

Each $k$-dimensional subspace $X$ of $\mathbb{F}^n_q$ has an identifying vector $v(X)$ which is a binary vector of length $n$ and weight $k$, where the ones in $v(X)$ are in the positions (columns) where $E(X)$ has the leading ones (of the rows).

$$E(X) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$v(X) = 1011000$$
Identifying Vectors

Each \( k \)-dimensional subspace \( X \) of \( \mathbb{F}_q^n \) has an identifying vector \( v(X) \) which is a binary vector of length \( n \) and weight \( k \), where the \textit{ones} in \( v(X) \) are in the positions (columns) where \( E(X) \) has the leading \textit{ones} (of the rows).

**Lemma 1** Let \( X \) be a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \), and \( i_1, i_2, \ldots, i_k \) the positions in which \( v(X) \) has \textit{ones}. Then, for each vector \( u \in X \), the leftmost \textit{one} in \( u \) is in position \( i_j \) for some \( 1 \leq j \leq k \).

**Proof** Clearly, there are at least \( k \) vectors with different position for the leftmost \textit{one}. If there are more than \( k \) vectors with different position for the leftmost \textit{one} then the dimension of the subspace will be greater than \( k \).
Identifying Vectors

**Lemma 1** Let $X$ be a $k$-dimensional subspace of $\mathbb{F}_q^n$, and $i_1, i_2, \ldots, i_k$ the positions in which $v(X)$ has ones. Then, for each vector $u \in X$, the leftmost one in $u$ is in position $i_j$ for some $1 \leq j \leq k$.

**Lemma** If $X, Y \in P_q(n)$ then $d_S(X, Y) \geq d_H(v(X), v(Y))$.

**Proof** Clearly, $v(X)$ has $r$ positions with ones where $v(Y)$ has zeros, and $v(Y)$ has $t$ positions with ones where $v(X)$ has zeros. Hence, $r + t = d_H(v(X), v(Y))$. By Lemma 1, there are $r$ linearly independent vectors in $X$ which are not contained in $Y$, and $t$ linearly independent vectors in $Y$ which are not contained in $X$.

Thus, $d_S(X, Y) \geq r + t = d_H(v(X), v(Y))$. 
The echelon Ferrers form of a vector \( u \) of length \( n \) and weight \( k \), \( EF(u) \), is a \( k \times n \) matrix in reduced row echelon form with leading entries (of rows) in the columns indexed by the nonzero entries of \( u \) and \( \cdot \) in all entries which do not have terminals zeros or ones. A \( \cdot \) is called a dot. The dots in this matrix form the Ferrers diagram of \( EF(u) \).

If we substitute the elements of \( \mathbb{F}_q \) in the dots of \( EF(u) \) we obtain a \( k \)-dimensional subspace \( X \) of \( P_q(n) \). \( EF(u) \) will be also called the echelon Ferrers form of \( X \).
The echelon Ferrers form of a vector $u$ of length $n$ and weight $k$, $EF(u)$, is a $k \times n$ matrix in reduced row echelon form with leading entries (of rows) in the columns indexed by the nonzero entries of $u$ and $\bullet$ in all entries which do not have terminals zeros or ones. A $\bullet$ is called a dot. The dots in this matrix form the Ferrers diagram of $EF(u)$.

$$E(X) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$v(X) = 1011000$$

$$EF(v(X)) = \begin{bmatrix} 1 & \bullet & 0 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 0 & 1 & \bullet & \bullet & \bullet \end{bmatrix}$$
Let $u$ be a vector of length $n$ and weight $k$. Let $F$ be the Ferrers diagram of $EF(u)$. $F$ is an $m \times \eta$ Ferrers diagram, $m \leq k$, $\eta \leq n - k$. A code $C$ is an $[F, \varrho, \delta]_q$ Ferrers diagram rank-metric code if all its codewords are $m \times \eta$ matrices in which all entries not in $F$ are zeros, it forms a rank-metric code with dimension $\varrho$ and minimum rank distance $\delta$.

Let $\text{dim } (F, \delta)_q$ be the largest possible dimension of an $[F, \varrho, \delta]_q$ code.
For a given $i$, $0 \leq i \leq \delta - 1$, if $v_i$ is the number of dots in a Ferrers diagram $\mathcal{F}$, which are not contained in the first $i$ rows and are not contained in the rightmost $\delta - 1 - i$ columns, then $\min_i\{v_i\}$ is an upper bound on $\dim (\mathcal{F}, \delta)_q$.

**Proof**

For a given $i$, $0 \leq i \leq \delta - 1$, let $A_i$ be the set of the $v_i$ positions of $\mathcal{F}$ which are not contained in the first $i$ rows and are not contained in the rightmost $\delta - 1 - i$ columns. Assume the contrary, that there exists an $[\mathcal{F}, v_i + 1, \delta]_q$ code $C$. 
Proof

For a given $i$, $0 \leq i \leq \delta - 1$, let $A_i$ be the set of the $\nu_i$ positions of $F$ which are not contained in the first $i$ rows and are not contained in the rightmost $\delta - 1 - i$ columns. Assume the contrary, that there exists an $[F, \nu_i + 1, \delta]_q$ code $C$.

Let $B_1, B_2, \ldots, B_{\nu_i+1}$ linearly independent codewords in $C$. Since the number of linearly independent codewords is greater than the number of entries in $A_i$, there exists a nontrivial linear combination $Y = \sum_{j=1}^{\nu_i+1} \alpha_j B_j$ for which the $\nu_i$ entries of $A_i$ are equal zeros. $Y$ is not the all-zeros codeword since the $B_i$'s are linearly independent.
Proof. Let $B_1, B_2, \ldots, B_{\nu_i+1}$ linearly independent codewords in $C$. Since the number of linearly independent codewords is greater than the number of entries in $A_i$, there exists a nontrivial linear combination $Y = \sum_{j=1}^{\nu_j+1} \alpha_j B_j$ for which the $\nu_i$ entries of $A_i$ are equal zeros. $Y$ is not the all-zeros codeword since the $B_i$'s are linearly independent.

$\mathcal{F}$ has outside $A_i$ exactly $i$ rows and $\delta - 1 - i$ columns. These $i$ rows ($\delta - 1 - i$ columns) can contribute at most $i$ ($\delta - 1 - i$, respectively) to the rank of $Y$. Thus, $Y$ is a nonzero codeword with rank less than $\delta$, a contradiction, and the theorem is proved.
**Ferrers Diagrams**

**Theorem**
For a given $i$, $0 \leq i \leq \delta - 1$, if $v_i$ is the number of dots in a Ferrers diagram $F$, which are not contained in the first $i$ rows and are not contained in the rightmost $\delta - 1 - i$ columns then $\min_i\{v_i\}$ is an upper bound on $\text{dim} (F, \delta)_q$.

**Corollary**
An upper bound on $\text{dim} (F, \delta)_q$ is the minimum number of dots that can be removed from $F$ such that the diagram remains with at most $\delta - 1$ rows of dots or at most $\delta - 1$ columns of dots.
Theorem

There exists a \([k \times m, q, \delta]_q\) code which satisfies
\[q = \min\{k(m - \delta + 1), m(k - \delta + 1)\}\]

Corollary

An upper bound on \(\dim (F, \delta)_q\) is the minimum number of dots that can be removed from \(F\) such that the diagram remains with at most \(\delta - 1\) rows of dots or at most \(\delta - 1\) columns of dots.
There exists a $[k \times m, \varphi, \delta]_q$ code which satisfies
\[
\varphi = \min\{k(m - \delta + 1), m(k - \delta + 1)\}.
\]

Let $\mathcal{F}$ be an $m \times \eta$, $m \geq \eta$, Ferrers diagram. Assume that each one of the rightmost $\delta - 1$ columns of $\mathcal{F}$ has $m$ dots, and the $i$th column from the left of $\mathcal{F}$ has $\gamma_i$ dots. Then an $[\mathcal{F}, \sum_{i=1}^{\eta-\delta+1} \gamma_i, \delta]_q$ code which attains the bound of the corollary exists.

An upper bound on $\dim (\mathcal{F}, \delta)_q$ is the minimum number of dots that can be removed from $\mathcal{F}$ such that the diagram remains with at most $\delta - 1$ rows of dots or at most $\delta - 1$ columns of dots.
There exists a \([k \times m, q, \delta]_q\) code which satisfies

\[
q = \min\{k(m - \delta + 1), m(k - \delta + 1)\}
\]

Let \(F\) be an \(m \times \eta, m \geq \eta\), Ferrers diagram. Assume that each one of the rightmost \(\delta - 1\) columns of \(F\) has \(m\) dots, and the \(i\)th column from the left of \(F\) has \(\gamma_i\) dots. Then an \([F, \sum_{i=1}^{\eta-\delta+1} \gamma_i, \delta]_q\) code which attains the bound of the corollary exists.

In any \([m \times \eta, m(\eta - \delta + 1), \delta]_q\) rank-metric code \(C\), the codewords which have **zeros** in all the entries which are not contained in \(F\) form an \([F, \sum_{i=1}^{\eta-\delta+1} \gamma_i, \delta]_q\) code.
Network Coding and Related Combinatorial Structures

A SHORT BREAK
Multilevel Construction

First step - choose a binary code $C$ of length $n$.

For each $c \in C$ do

Second step - echelon Ferrers form $EF(c)$.

Third step - construct an $[F, q, \delta]_q$ Ferrers diagram rank-metric code $C_F$ for the Ferrers diagram $F$ of $EF(c)$.

Fourth step - lift $C_F$ to an $(n, q^o, 2\delta, k)_q$ code $C_c$; the echelon Ferrers form of $X \in C_c$ is $EF(c)$.

$C = \bigcup_{c \in C} C_c$
Multilevel Construction

If $C$ should be an $(n, M, 2\delta, k)_q$ code then $C$ is a constant weight code with weight $k$ minimum Hamming distance $2\delta$.

If $C$ should be an $(n, M, d)_q$ code, where $d$ is the subspace distance, then $C$ is a code with minimum Hamming distance $d$.

If $C$ should be an $(n, M, d)_q$ code, where $d$ is the injection distance, then $C$ is a code with minimum asymmetric distance $d$. 
Asymptotic Behavior

**Theorem**

\[
A_q(n, 2\delta, k) \leq \frac{\left[\frac{n}{k-\delta+1}\right]_q}{\left[\frac{k}{k-\delta+1}\right]_q}
\]

\[
Q_\delta(q) = \prod_{j=\delta}^{\infty} (1 - q^{-j})
\]

\[
\begin{align*}
\left[\frac{n}{k-\delta+1}\right]_q &= \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+\delta} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q^\delta - 1)} \\
&= q^{(n-k)(k-\delta+1)} \frac{(1 - q^{-n})(1 - q^{-n+1}) \cdots (1 - q^{-n+k-\delta})}{(1 - q^{-k})(1 - q^{-k+1}) \cdots (1 - q^{-\delta})} \\
&< \frac{q^{(n-k)(k-\delta+1)}}{\prod_{j=\delta}^{\infty} (1 - q^{-j})}
\end{align*}
\]
Asymptotic Behavior

**Theorem**

\[
A_q(n, 2\delta, k) \leq \frac{\left\lfloor \frac{n}{k-\delta+1} \right\rfloor_q}{\left\lfloor \frac{k}{k-\delta+1} \right\rfloor_q} < \frac{q^{(n-k)(k-\delta+1)}}{\prod_{j=\delta}^{\infty} (1-q^{-j})}
\]

\[
Q_\delta(q) = \prod_{j=\delta}^{\infty} (1 - q^{-j})
\]

<table>
<thead>
<tr>
<th>(\delta)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.5776</td>
<td>0.8402</td>
<td>0.9181</td>
<td>0.9504</td>
<td>0.9763</td>
</tr>
<tr>
<td>3</td>
<td>0.7701</td>
<td>0.9452</td>
<td>0.9793</td>
<td>0.9900</td>
<td>0.9966</td>
</tr>
<tr>
<td>4</td>
<td>0.8801</td>
<td>0.9816</td>
<td>0.9948</td>
<td>0.9980</td>
<td>0.9995</td>
</tr>
<tr>
<td>5</td>
<td>0.9388</td>
<td>0.9938</td>
<td>0.9987</td>
<td>0.9996</td>
<td>0.9999</td>
</tr>
</tbody>
</table>
### Multilevel Construction

- \( q = 2, \, n = 8, \, k = 4, \, \delta = 2 \)

- \( A_2(8, 4, 4) \geq 4573 \)

<table>
<thead>
<tr>
<th>( c \in C )</th>
<th>size of ( C_c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11110000</td>
</tr>
<tr>
<td>2</td>
<td>11001100</td>
</tr>
<tr>
<td>3</td>
<td>11000011</td>
</tr>
<tr>
<td>4</td>
<td>10101010</td>
</tr>
<tr>
<td>5</td>
<td>10100101</td>
</tr>
<tr>
<td>6</td>
<td>10011001</td>
</tr>
<tr>
<td>7</td>
<td>10010110</td>
</tr>
<tr>
<td>8</td>
<td>01101001</td>
</tr>
<tr>
<td>9</td>
<td>01100110</td>
</tr>
<tr>
<td>10</td>
<td>01011010</td>
</tr>
<tr>
<td>11</td>
<td>01010101</td>
</tr>
<tr>
<td>12</td>
<td>00111100</td>
</tr>
<tr>
<td>13</td>
<td>00110011</td>
</tr>
<tr>
<td>14</td>
<td>00001111</td>
</tr>
</tbody>
</table>
Multilevel Construction

$q = 2$, $n = 7$, $d = 3$

$A_2(7, 3) \geq 394$

<table>
<thead>
<tr>
<th>$c \in C$</th>
<th>size of $\mathbb{C}_c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1110000</td>
</tr>
<tr>
<td>2</td>
<td>1001001</td>
</tr>
<tr>
<td>3</td>
<td>1000110</td>
</tr>
<tr>
<td>4</td>
<td>0101010</td>
</tr>
<tr>
<td>5</td>
<td>0100101</td>
</tr>
<tr>
<td>6</td>
<td>0011100</td>
</tr>
<tr>
<td>7</td>
<td>0010011</td>
</tr>
<tr>
<td>8</td>
<td>0111001</td>
</tr>
<tr>
<td>9</td>
<td>0110110</td>
</tr>
<tr>
<td>10</td>
<td>1010101</td>
</tr>
<tr>
<td>11</td>
<td>1011010</td>
</tr>
<tr>
<td>12</td>
<td>1101100</td>
</tr>
<tr>
<td>13</td>
<td>1100011</td>
</tr>
<tr>
<td>14</td>
<td>0001111</td>
</tr>
<tr>
<td>15</td>
<td>0000000</td>
</tr>
<tr>
<td>16</td>
<td>1111111</td>
</tr>
</tbody>
</table>
Let $C$ be an $(n, M, d)_q$ code in the Hamming space. The punctured code $C'$ is an $(n - 1, M, d - 1)_q$ code obtained from $C$ by deleting one coordinate.

Let $X$ be an $\ell$-dimensional subspace of $\mathbb{F}_q^n$ such that the unity vector with a one in the $i$th coordinate is not an element in $X$. The $i$th coordinate puncturing of $X$, $\Delta_i(X)$, is defined as the $\ell$-dimensional subspace of $\mathbb{F}_q^{n-1}$ obtained from $X$ by deleting the $i$th coordinate from each vector of $X$. 
Punctured Codes

\( \mathbb{C} \subseteq P_q(n) \)

\( Q \in G_q(n, n-1) \)

\( u \in \mathbb{F}_q^n, u \notin Q \)

\( t \) is the unique position of \( \nu(Q) \) with a zero.

The punctured code of \( \mathbb{C} \)

\[ C'_{Q,u} = C_Q \cup C_{Q,u} \]

\[ C_Q = \{ \Delta_t(X) : X \in \mathbb{C}, X \subseteq Q \} \]

\[ C_{Q,u} = \{ \Delta_t(X \cap Q) : X \in \mathbb{C}, u \in X \} \]
The punctured code $\mathbb{C}_Q,u$ of an $(n, M, d)_q$ code $\mathbb{C}$ is an $(n - 1, M', d - 1)_q$ code.

If $\mathbb{C}$ is an $(n, M, d, k)_q$ code then there exist $Q, u$ and an $(n - 1, M', d - 1)_q$ code $\mathbb{C}'_{Q,u}$ such that

$$M' \geq \frac{M(q^{n-k} - q^{k-2})}{q^n - 1}.$$
If \( \mathbb{C} \) is an \((n, M, d, k)\) code then there exist \( Q, u \) and an \((n - 1, M', d - 1)\) code \( \mathbb{C}'_{Q,u} \) such that \( M' \geq \frac{M(q^{n-k} - q^k - 2)}{q^n - 1} \).

Theorem

Proof

\( Q \) can be chosen in \( \frac{q^n - 1}{q - 1} \) different ways. Each \( k \)-dimensional subspace of \( \mathbb{P}_q(n) \) is contained in \( \frac{q^{n-k} - 1}{q - 1} \) \((n - 1)\)-dimensional subspaces of \( \mathbb{P}_q(n) \). Thus, there exists an \((n - 1)\)-dimensional subspace \( Q \) such that \( |\mathbb{C}_Q| \geq M \frac{q^{n-k} - 1}{q^n - 1} \).
Q can be chosen in \( \frac{q^n-1}{q-1} \) ways. A \( k \)-dimensional subspace of \( P_q(n) \). Thus, there exists \( Q \) such that \( |\mathbb{C}_Q| \geq M \frac{q^{n-k}-1}{q^{n-1}} \).

There are \( M - |\mathbb{C}_Q| \) codewords in \( \mathbb{C} \) which are not contained in \( Q \). If \( X \in \mathbb{C} \) is such codeword then \( \dim (X \cap Q) = k - 1 \). Therefore, \( X \) contains \( q^k - q^{k-1} \) vectors which do not belong to \( Q \). In \( \mathbb{F}_q^n \) there are \( q^n - q^{n-1} \) vectors which do not belong to \( Q \). There exists an \( (n - 1) \)-dimensional subspace \( Q \in P_q(n) \) and \( u \notin Q \) such that \( |\mathbb{C}_{Q,u}| \geq \frac{(M - |\mathbb{C}_Q|)(q^k - q^{k-1})}{q^n - q^{n-1}} = \frac{M - |\mathbb{C}_Q|}{q^{n-k}} \).
Punctured Codes

**Proof**

We have
\[ |\mathbb{C}_Q| \geq M \frac{q^{n-k}-1}{q^n-1}. \]

We have
\[ |\mathbb{C}_{Q,u}| \geq \frac{(M-|\mathbb{C}_Q|)(q^k-q^{k-1})}{q^n-q^{n-1}} = \frac{M-|\mathbb{C}_Q|}{q^{n-k}}. \]

Therefore, there exists an \((n-1, M', d-1)_q\) code \(\mathbb{C}_{Q,u}'\) such that
\[
M' = |\mathbb{C}_Q| + |\mathbb{C}_{Q,u}| \geq \frac{|\mathbb{C}_Q| q^{n-k} + M - |\mathbb{C}_Q|}{q^{n-k}} \\
= \frac{(q^{n-k}-1)|\mathbb{C}_Q| + M}{q^{n-k}} \geq \frac{(q^{n-k}-1)M(q^{n-k}-1)+M(q^n-1)}{(q^n-1)q^{n-k}} \\
= \frac{M(q^{n-k}+q^k-2)}{q^n-1}. \]
Let $\mathbb{C}$ be the $(8, 4573, 4, 4)_2$ code obtained by the multilevel construction. Let $Q$ be the 7-dimensional subspace whose $7 \times 8$ generator matrix is

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}.
$$

By puncturing $\mathbb{C}$ with $Q$ and $u = 10000001$ we obtain a code $\mathbb{C}'_{Q,u}$ whose size is 573 to which the null space and $\mathbb{F}_2^7$ can be added, and hence $A_2(7, 3) \geq 575$ (compared to 394 by the multilevel construction).
Cyclic Codes

α primitive in $\mathbb{F}_{q^n}$

$\mathbb{C} \subseteq P_q(n)$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q^k-1}}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_{q^k-1}+1}\}$

$\mathbb{C}$ is a cyclic code if $V \in \mathbb{C}$ implies that $\alpha V \in \mathbb{C}$. 
q-Steiner Systems (cyclic)

$S(2, 3, 13)_2$

$\alpha$ primitive in $GF(2^{13})$

$V = \{0, \alpha^{i1}, \alpha^{i2}, \alpha^{i3}, \alpha^{i4}, \alpha^{i5}, \alpha^{i6}, \alpha^{i7}\}$

$\alpha V = \{0, \alpha^{i1+1}, \alpha^{i2+1}, \alpha^{i3+1}, \alpha^{i4+1}, \alpha^{i5+1}, \alpha^{i6+1}, \alpha^{i7+1}\}$

$F(V) = \{0, \alpha^{2\cdot i1}, \alpha^{2\cdot i2}, \alpha^{2\cdot i3}, \alpha^{2\cdot i4}, \alpha^{2\cdot i5}, \alpha^{2\cdot i6}, \alpha^{2\cdot i7}\}$

cyclic shift

Frobenius map

15 representatives

normalizer of Singer subgroup automorphism

1 597 245 3-dimensional subspaces
Linearized polynomials are a special family of polynomials whose roots form a subspace. These polynomials were used to form a subspace code whose parameters are exactly as the ones of lifted MRD codes.

$$L(x) = \sum_{i=0}^{d} a_i x^{q^i}, \quad a_i \in \mathbb{F}_{q^m}$$

The roots of $L(X)$ are in a field $\mathbb{F}_{q^n}$, where $m$ divides $n$. 
Linearized polynomials are a special family of polynomials whose roots form a subspace. These polynomials were used to form a subspace code whose parameters are exactly as the ones of lifted MRD codes.

Subspace polynomials are a subclass of the linearized polynomials. The roots of a subspace polynomial have multiplicity one. The subspaces that they form can be used to form cyclic codes.
Network Coding and Related Combinatorial Structures

END OF LECTURE 9