Non-Standard Coding Theory

Steven T. Dougherty

July 3, 2013
Rosenbloom-Tsfasman Metric

Codes with the Rosenbloom-Tsfasman Metric
Rosenbloom-Tsfasman Metric

$\text{Mat}_{n,s}(\mathbb{F}_q)$ denotes the linear space of all matrices with $n$ rows and $s$ columns with entries from a finite field $\mathbb{F}_q$ of $q$ elements.
Rosenbloom-Tsfasman Metric

$\text{Mat}_{n,s}(\mathbb{F}_q)$ denotes the linear space of all matrices with $n$ rows and $s$ columns with entries from a finite field $\mathbb{F}_q$ of $q$ elements.

A linear code is a subspace of $\text{Mat}_{n,s}(\mathbb{F}_q)$. 
Rosenbloom-Tsfasman Metric

Define \( \rho \) on \( \text{Mat}_{n,s}(\mathbb{F}_q) \)
Rosenbloom-Tsfasman Metric

Define $\rho$ on $\text{Mat}_{n,s}(\mathbb{F}_q)$

Let $n = 1$ and $\omega = (\xi_1, \xi_2, \ldots, \xi_s) \in \text{Mat}_{1,s}(\mathbb{F}_q)$. Then, we put $\rho(0) = 0$ and

$$\rho(\omega) = \max\{i \mid \xi_i \neq 0\}$$

(1)

for $\omega \neq 0$. 
Define $\rho$ on $\text{Mat}_{n,s}(\mathbb{F}_q)$

Let $n = 1$ and $\omega = (\xi_1, \xi_2, \ldots, \xi_s) \in \text{Mat}_{1,s}(\mathbb{F}_q)$. Then, we put $\rho(0) = 0$ and

$$\rho(\omega) = \max\{i \mid \xi_i \neq 0\}$$ (1)

for $\omega \neq 0$.

Ex: $\rho(1, 0, 0, 1, 0) = 4$. 
Rosenbloom-Tsfasman Metric

Now let $\Omega = (\omega_1, \ldots, \omega_n)^T \in \text{Mat}_{n,s}(\mathbb{F}_q)$, $\omega_j \in \text{Mat}_{1,s}(\mathbb{F}_q)$, $1 \leq j \leq n$, and $(\cdot)^T$ denotes the transpose of a matrix. Then, we put

$$\rho(\Omega) = \sum_{j=1}^{n} \rho(\omega_j)$$

(2)
Rosenbloom-Tsfasman Metric

Now let \( \Omega = (\omega_1, \ldots, \omega_n)^T \in \text{Mat}_{n,s}(\mathbb{F}_q) \), \( \omega_j \in \text{Mat}_{1,s}(\mathbb{F}_q) \), \( 1 \leq j \leq n \), and \((\cdot)^T\) denotes the transpose of a matrix. Then, we put

\[
\rho(\Omega) = \sum_{j=1}^{n} \rho(\omega_j) \quad (2)
\]

Ex:

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

\[
\rho = 5 + 2 + 4 + 1 = 12.
\]
Weight Distribution

For a given linear code $C \subset \text{Mat}_{n,s}(\mathbb{F}_q)$ the following set of nonnegative integers

$$w_r(C) = |\{\Omega \in C \mid \rho(\Omega) = r\}|, \ 0 \leq r \leq ns$$

(3)

is called the $\rho$ weight spectrum of the code $C$. 
Define the $\rho$ weight enumerator by

$$W(C|z) = \sum_{r=0}^{ns} w_r(C) z^r = \sum_{\Omega \in C} z^{\rho(\Omega)}$$

(4)
Define the $\rho$ weight enumerator by

$$W(C|z) = \sum_{r=0}^{ns} w_r(C)z^r = \sum_{\Omega \in C} z^{\rho(\Omega)}$$  \hspace{1cm} (4)$$

Note that if $s = 1$, it reduces to the Hamming weight enumerator.
Inner-Product

Introduce the following innerproduct on $Mat_{n,s} (\mathbb{F}_q)$. At first, let $n = 1$ and $\omega_1 = (\xi'_1, \ldots, \xi'_s)$, $\omega_2 = (\xi''_1, \ldots, \xi''_s) \in Mat_{1,s} (\mathbb{F}_q)$. Then we put

$$\langle \omega_1, \omega_2 \rangle = \langle \omega_2, \omega_1 \rangle = \sum_{i=1}^{s} \xi'_i \xi''_{s+1-i} \quad (5)$$
Inner-Product

Introduce the following innerproduct on $\text{Mat}_{n,s}(\mathbb{F}_q)$. At first, let $n = 1$ and $\omega_1 = (\xi_1', \ldots, \xi_s')$, $\omega_2 = (\xi_1'', \ldots, \xi_s'') \in \text{Mat}_{1,s}(\mathbb{F}_q)$. Then we put

$$\langle \omega_1, \omega_2 \rangle = \langle \omega_2, \omega_1 \rangle = \sum_{i=1}^{s} \xi_i' \xi_{s+1-i}'' \quad (5)$$

Ex: $q = 5$,

$$\langle (1, 2, 1, 3, 4), (2, 1, 4, 3, 4) \rangle = 1(4) + 2(3) + 1(4) + 3(1) + 4(2) = 3.$$
Introduce the following innerproduct on $\text{Mat}_{n,s}(\mathbb{F}_q)$. At first, let $n = 1$ and $\omega_1 = (\xi'_1, \ldots, \xi'_s)$, $\omega_2 = (\xi''_1, \ldots, \xi''_s) \in \text{Mat}_{1,s}(\mathbb{F}_q)$. Then we put

$$\langle \omega_1, \omega_2 \rangle = \langle \omega_2, \omega_1 \rangle = \sum_{i=1}^{s} \xi'_i \xi''_{s+1-i}$$

(5)

Ex: $q = 5$, 

$$\langle (1, 2, 1, 3, 4), (2, 1, 4, 3, 4) \rangle = 1(4) + 2(3) + 1(4) + 3(1) + 4(2) = 3.$$

Note that this is a non-standard inner-product on rows.
Now, let
\[ \Omega_i = (\omega_i^{(1)}, \ldots, \omega_i^{(n)})^T \in \text{Mat}_{n,s}(\mathbb{F}_q), \ i = 1, 2, \ \omega_i^{(j)} \in \text{Mat}_{1,s}(\mathbb{F}_q), \ 1 \leq j \leq n. \] Then we put
\[ \langle \Omega_1, \Omega_2 \rangle = \langle \Omega_2, \Omega_1 \rangle = \sum_{j=1}^{n} \langle \omega_1^{(j)}, \omega_2^{(j)} \rangle \] (6)
Orthogonal

Let $C \subset \text{Mat}_{n,s}(\mathbb{F}_q)$. $C^\perp \subset \text{Mat}_{n,s}(\mathbb{F}_q)$ is defined by

$$C^\perp = \{ \Omega_2 \in \text{Mat}_{n,s}(\mathbb{F}_q) \mid \langle \Omega_2, \Omega_1 \rangle = 0 \text{ for all } \Omega_1 \in C \}. \quad (7)$$
Orthogonal

Let $C \subset \text{Mat}_{n,s}(\mathbb{F}_q)$. $C^\perp \subset \text{Mat}_{n,s}(\mathbb{F}_q)$ is defined by

$$C^\perp = \{ \Omega_2 \in \text{Mat}_{n,s}(\mathbb{F}_q) | \langle \Omega_2, \Omega_1 \rangle = 0 \text{ for all } \Omega_1 \in C \}. \quad (7)$$

$C^\perp$ is a linear code, and $(C^\perp)^\perp = C$. 

We have

$$d + d^\perp = ns, \quad |C| = q^{ns}, \quad |C^\perp| = q^{ns - d}, \quad (8)$$

where $d$ is the dimension of $C$ and $d^\perp$ is the dimension of $C^\perp$. 

Let $C \subseteq \text{Mat}_{n,s}(\mathbb{F}_q)$. $C^\perp \subseteq \text{Mat}_{n,s}(\mathbb{F}_q)$ is defined by

$$C^\perp = \{ \Omega_2 \in \text{Mat}_{n,s}(\mathbb{F}_q) \mid \langle \Omega_2, \Omega_1 \rangle = 0 \text{ for all } \Omega_1 \in C \}.$$  \hspace{1cm} (7)

$C^\perp$ is a linear code, and $(C^\perp)^\perp = C$.

We have

$$d + d^\perp = ns, \quad |C||C^\perp| = q^{ns}, \quad |C| = q^d, \quad |C^\perp| = q^{ns-d},$$  \hspace{1cm} (8)

where $d$ is the dimension of $C$ and $d^\perp$ is the dimension of $C^\perp$.  

Examples

\[ q = 2, \ n = s = 2 \]
Examples

\[ q = 2, \ n = s = 2 \]

\[ C_1 = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \}, \quad C_2 = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \} \]

(9)
Examples

\[ q = 2, \ n = s = 2 \]

\[ C_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\}, \quad C_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \]  

Both codes have \( \rho \) weight enumerator

\[ 1 + z^2 \]
\[ C_1^\perp = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\} \]
Duals

\[ C_1^\perp = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \} \]

\[ C_2^\perp = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \} \]
Weight Enumerators

The \( \rho \) weight enumerator for \( C_1^\perp \) and \( C_2^\perp \) turns out to be different:

\[
W(C_1^\perp \mid z) = 1 + 4z^4 + 2z + z^2
\]

Therefore, the \( \rho \) weight enumerators cannot be related by a MacWilliams type relation.
Weight Enumerators

The $\rho$ weight enumerator for $C_1^\perp$ and $C_2^\perp$ turns out to be different:

$$W(C_1^\perp \mid z) = 1 + 4z^4 + 2z + z^2$$

$$W(C_2^\perp \mid z) = 1 + 2z^4 + z^3 + 3z^2 + z$$

Therefore, the $\rho$ weight enumerators cannot be related by a MacWilliams type relation.
The \( \rho \) weight enumerator for \( C_1^\perp \) and \( C_2^\perp \) turns out to be different:

\[
W(C_1^\perp \mid z) = 1 + 4z^4 + 2z + z^2
\]

\[
W(C_2^\perp \mid z) = 1 + 2z^4 + z^3 + 3z^2 + z
\]

Therefore, the \( \rho \) weight enumerators cannot be related by a MacWilliams type relation.
Is it a problem with the inner-product

We shall compare the first innerproduct with the common one:

\[ [\omega_1, \omega_2] = \sum_{i=1}^{s} \xi_i' \xi_i''. \]  (11)
Is it a problem with the inner-product

We shall compare the first innerproduct with the common one:

\[ [\omega_1, \omega_2] = \sum_{i=1}^{s} \xi'_i \xi''_i. \quad (11) \]

Consider two linear codes \( C_1 \) and \( C_2 \subset Mat_{1,4}(\mathbb{F}_2) \),

\[ C_1 = \{0000, 1100, 1001, 0101\}, \quad C_2 = \{0000, 0100, 0001, 0101\}. \]
Is it a problem with the inner-product

We shall compare the first innerproduct with the common one:

\[ [\omega_1, \omega_2] = \sum_{i=1}^{s} \xi_i' \xi_i''. \]  
(11)

Consider two linear codes \( C_1 \) and \( C_2 \subset \text{Mat}_{1,4}(\mathbb{F}_2) \),

\( C_1 = \{0000, 1100, 1001, 0101\}, \quad C_2 = \{0000, 0100, 0001, 0101\}. \)

Notice that these codes have the same \( \rho \) weight enumerators:

\[ W(C_i \mid z) = W(C_i^\perp \mid z) = 1 + z^2 + 2z^4, \quad i = 1, 2. \]  
(12)
Is it a problem with the inner-product

Denote by $C_1^*$ and $C_2^*$ codes dual to $C_1$ and $C_2$ with respect to the common inner product. We have

$$C_1^* = \{0000, 0010, 1111, 1101\}$$
Is it a problem with the inner-product

Denote by $C_1^*$ and $C_2^*$ codes dual to $C_1$ and $C_2$ with respect to the common inner product. We have

$$C_1^* = \{0000, 0010, 1111, 1101\}$$

$$C_2^* = \{0000, 0010, 1000, 1010\}$$
Is it a problem with the inner-product

Denote by $C_1^*$ and $C_2^*$ codes dual to $C_1$ and $C_2$ with respect to the common inner product. We have

$$C_1^* = \{0000, 0010, 1111, 1101\}$$

$$C_2^* = \{0000, 0010, 1000, 1010\}$$

The $\rho$ weight enumerators are different:

$$W(C_1^* \mid Z) = 1 + z^3 + 2z^4, \quad W(C_2^* \mid z) = 1 + z + 2z^3. \quad (13)$$
Is it a problem with the inner-product

Therefore, the $\rho$ weight enumerators $W(C \mid z)$ and $W(C^* \mid z)$ cannot be related by a MacWilliams-type identity with the common inner-product.
Is it a problem with the inner-product

Therefore, the $\rho$ weight enumerators $W(C \mid z)$ and $W(C^* \mid z)$ cannot be related by a MacWilliams-type identity with the common inner-product.

It is not a problem with the inner-product but rather with the weights.
\[ T(C \mid Z_1, \ldots, Z_n) = \sum_{\Omega \in \mathcal{C}} \Upsilon(\Omega \mid Z_1, \ldots, Z_n) \quad (14) \]

where \( \Upsilon(\Omega) = z_{a_1}^{(1)} z_{a_2}^{(2)} \ldots z_{a_n}^{(n)} \) and \( \rho(\omega_i) = a_i, \ 1 \leq i \leq n \).
$T$-Weight Enumerator

\[ T(C \mid Z_1, \ldots, Z_n) = \sum_{\Omega \in C} \gamma(\Omega \mid Z_1, \ldots, Z_n) \quad (14) \]

where $\gamma(\Omega) = z_{a_1}^{(1)} z_{a_2}^{(2)} \ldots z_{a_n}^{(n)}$ and $\rho(\omega_i) = a_i$, $1 \leq i \leq n$.

The $Z_i$ are $n$ complex vectors with $s + 1$ components, $Z_j = (z_0^{(j)}, \ldots, z_s^{(j)})$. 
$T$-Weight Enumerator

Example:

$$\gamma \left( \begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{array} \right) = z_3^1 z_4^2 z_1 z_2^4$$
**H-Weight Enumerator**

\[ H(C \mid Z) = T(C \mid Z, Z, \ldots, Z). \]
In the previous example the monomial becomes $z_3z_4z_1z_2$. 

$H(C \mid Z) = T(C \mid Z, Z, \ldots, Z)$. 
$H$-Weight Enumerator

\[ H(C \mid Z) = T(C \mid Z, Z, \ldots, Z). \]

In the previous example the monomial becomes $z_3 z_4 z_1 z_2$.

Notice that the first enumerator is a polynomial of degree at most one in each of $n(s + 1)$ variables $z_i^{(j)}$, $0 \leq i \leq s$ $1 \leq j \leq n$, while the second enumerator has degree at most $n$ in each of $s + 1$ variables $z_i$, $0 \leq i \leq s$. 
Linear Transformation

Introduce a linear transformation

\[ \Theta_s : \mathbb{C}^{s+1} \rightarrow \mathbb{C}^{s+1} \]

by setting

\[ Z' = \Theta_s Z, \]

where

\[ z'_0 = z_0 + (q - 1)z_1 + q(q - 1) + q^2(q - 1)z_3 + \]
\[ \cdots + q^{s-2}(q - 1)z_{s-1} + q^{s-1}(q - 1)z_s \]
Linear Transformation

\[
\begin{align*}
z'_1 &= z_0 + (q - 1)z_1 + q(q - 1) + q^2(q - 1)z_3 + \\
& \quad \cdots + q^{s-2}(q - 1)z_{s-1} + -q^{s-1}z_s \\
\end{align*}
\]

\[
\cdots
\]

\[
\begin{align*}
z'_{s-2} &= z_0 + (q - 1)z_1 + q(q - 1) - q^2z_3 \\
& \quad z_{s-1}' = z_0 + (q - 1)z_1 - qz_2 \\
& \quad z'_s = z_0 - z_1
\end{align*}
\]
We assume that $Z = (z_0, z_1, z_2, \ldots)$ is an infinite sequence with $z_i = 0$ for $i > s$. Thus the $s + 1$ by $s + 1$ matrix $\Theta_s = ||\theta_{lk}||$, $0 \leq l, k \leq s$, has the following entries.
Linear Transformation

\[ \theta_{lk} = \begin{cases} 
1 & \text{if } l = 0, \\
q^{l-1}(q - 1) & \text{if } 0 < l \leq s - k, \\
-q^{l-1} & \text{if } l + k = s + 1, \\
0 & \text{if } l + k > s + 1. 
\end{cases} \]
Linear Transformation

\[ \theta_{lk} = \begin{cases} 
1 & \text{if } l = 0, \\
q^{l-1}(q - 1) & \text{if } 0 < l \leq s - k, \\
-q^{l-1} & \text{if } l + k = s + 1, \\
0 & \text{if } l + k > s + 1.
\end{cases} \]

\[ \Theta_1 = \begin{pmatrix} 1 & q - 1 \\ 1 & -1 \end{pmatrix} \]
Linear Transformation

\[ \theta_{lk} = \begin{cases} 
1 & \text{if } l = 0, \\
q^{l-1}(q - 1) & \text{if } 0 < l \leq s - k, \\
-q^{l-1} & \text{if } l + k = s + 1, \\
0 & \text{if } l + k > s + 1.
\end{cases} \]

\[ \Theta_1 = \begin{pmatrix} 1 & q - 1 \\ 1 & -1 \end{pmatrix} \]

\[ \Theta_2 = \begin{pmatrix} 1 & q - 1 & q(q - 1) \\ 1 & q - 1 & -q \\ 1 & -1 & 0 \end{pmatrix} \]
Linear Transformation

\[ \theta_{lk} = \begin{cases} 
1 & \text{if } l = 0, \\
q^{l-1}(q-1) & \text{if } 0 < l \leq s - k, \\
-q^{l-1} & \text{if } l + k = s + 1, \\
0 & \text{if } l + k > s + 1.
\end{cases} \]

\[ \Theta_1 = \begin{pmatrix} 1 & q - 1 \\
1 & -1 \end{pmatrix} \]

\[ \Theta_2 = \begin{pmatrix} 1 & q - 1 & q(q - 1) \\
1 & q - 1 & -q \\
1 & -1 & 0 \end{pmatrix} \]

\[ \Theta_3 = \begin{pmatrix} 1 & q - 1 & q(q - 1) & q^2(q - 1) \\
1 & q - 1 & q(q - 1) & -q^2 \\
1 & q - 1 & -q & 0 \\
1 & -1 & 0 & 0 \end{pmatrix} \]
Theorem

The $T$-enumerators of mutually dual linear codes $C$, $C^\perp \subset \text{Mat}_{n,s}(F_q)$ are related by

$$T(C^\perp \mid Z_1, \ldots, Z_n) = \frac{1}{|C|} T(C \mid \Theta_s Z_1, \ldots, \Theta_s Z_n).$$
MacWilliams Relations

**Theorem**

The $H$-enumerator of mutually dual linear codes $C$, $C^\perp \subset Mat_{n,s}(F_q)$ are related by

$$H(C^\perp \mid Z) = \frac{1}{|C|} H(C \mid \Theta_s Z)$$
Hence by expanding the amount of information in the weight enumerator MacWilliams relations can be found!
Singleton Bound

The minimum weight of a code $C$ is given by

$$\rho(C) = \min\{\rho(\Omega, \Omega') \mid \Omega, \Omega' \in C, \Omega \neq \Omega'\}.$$
Singleton Bound

The minimum weight of a code $C$ is given by

$$\rho(C) = \min\{\rho(\Omega, \Omega') \mid \Omega, \Omega' \in C, \Omega \neq \Omega'\}.$$  

If the code is linear (i.e. $\mathcal{A}$ is a finite ring and the code is a submodule) then $\rho(C) = \min\{\rho(\Omega) \mid \Omega \in C, \}$ where $\rho(\Omega) = \rho(\Omega, 0)$. 
Singleton Bound

**Theorem**

Let $A$ be any finite alphabet with $q$ elements and let $C \subset \text{Mat}_{n,s}(A)$, be an arbitrary code, then

$$|C| \leq q^{n-d+1}.$$
Singleton Bound

**Theorem**

Let $A$ be any finite alphabet with $q$ elements and let $C \subset \text{Mat}_{n,s}(A)$, be an arbitrary code, then

$$|C| \leq q^{n-d+1}.$$  

**Proof.**

Mark the first $d-1$ positions lexicographically. Two elements of $C$ never coincide in all other positions since otherwise the distance between them would be less than $d$. Hence $|C| \leq q^{n-d+1}$.  

Corollary

Let $C \subset \text{Mat}_{n,s}(A)$, where $|A| = q$, be an arbitrary code consisting of $q^k$, $0 \leq k \leq ns$, points. Then

$$\rho(C) \leq ns - k + 1.$$
Corollary

Let \( C \subset \text{Mat}_{n,s}(A) \), where \(|A| = q\), be an arbitrary code consisting of \( q^k \), \( 0 \leq k \leq ns \), points. Then

\[
\rho(C) \leq ns - k + 1.
\]

Naturally, we define a code meeting this bound as a Maximum Distance Separable Code with respect to the \( \rho \) metric.
Theorem

(Skriganov) If $C$ is a linear MDS code in $\text{Mat}_{n,s}(F_q)$, then $C^\perp$ is also an MDS code.
MDR Bound

Theorem

If $C$ is a linear code in $\text{Mat}_{n,s}(\mathbb{Z}_k)$ of rank $h$, then

$$\rho(C) \leq ns - h + 1.$$
MDR Bound

Theorem
If $C$ is a linear code in $\text{Mat}_{n,s}(\mathbb{Z}_k)$ of rank $h$, then

$$\rho(C) \leq ns - h + 1.$$ 

Codes meeting this bound are called MDR codes.
MDR Codes

Theorem
Let $C_1, C_2, \ldots, C_r$ be linear codes in $\text{Mat}_{n,s}(\mathbb{Z}_{k_1}), \ldots, \text{Mat}_{n,s}(\mathbb{Z}_{k_r})$, respectively, where $k_1, \ldots, k_r$ are positive integers with $\gcd(k_i, k_j) = 1$ for $i \neq j$. If $C_i$ is an MDR code for all $i$, then $C = \text{CRT}(C_1, C_2, \ldots, C_r)$ is an MDR code.
Uniform Distributions

Let $U$ denote the interval $[0, 1)$ and

$$\Delta^M_A = \left[ \frac{m_1}{k^{a_1}}, \frac{m_1 + 1}{k^{a_1}} \right) \ldots \left[ \frac{m_n}{k^{a_n}}, \frac{m_n + 1}{k^{a_n}} \right) \subset U^n$$

an elementary box, where $M = (m_1, \ldots, m_n)$ and $A = (a_1, \ldots, a_n)$. 
Uniform Distributions

Let $U$ denote the interval $[0, 1)$ and

$$\Delta^M_A = \left[ \frac{m_1}{k^{a_1}}, \frac{m_1 + 1}{k^{a_1}} \right) \cdots \left[ \frac{m_n}{k^{a_n}}, \frac{m_n + 1}{k^{a_n}} \right) \subset U^n$$

an elementary box, where $M = (m_1, \ldots, m_n)$ and $A = (a_1, \ldots, a_n)$.

**Definition**

Given an integer $0 \leq h \leq n$, a subset $D \subset U^n$ consisting of $k^h$ points is called an optimum $[ns, h]_s$ distribution in base $k$ if each elementary box $\Delta^M_A$ of volume $k^{-h}$ contains exactly one point of $D$. 
Uniform Distributions

For a point $X$ in $Q^n(k^s)$ define the following matrix which is an element of $Mat_{n,s}(Z_k)$:

$$
\Omega\langle X \rangle = (\omega(x_1), \omega(x_2), \ldots, \omega(x_n))^T
$$

where

$$
\omega\langle x \rangle = (\xi_1(x), \xi_2(x), \ldots, \xi_s(x))
$$

and $x = \sum_{i=1}^{s} \xi_i(x) k^{i-s-1}$. 
Theorem
Let $C$ be an optimum distribution in $Q^n(k^s)$ for any $k$ and $C$ its corresponding code then the following are equivalent:

- $D$ is an optimum $[ns, \lambda]_s$ distribution in base $k$
- $C$ is an MDS code in the $\rho$ metric in $\text{Mat}_{n,s}(Z_k)$. 
Codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their Gray Map
Delsarte defines additive codes as subgroups of the underlying abelian group in a translation association scheme.
Delsarte defines additive codes as subgroups of the underlying abelian group in a translation association scheme.

For the binary Hamming scheme, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. 
Delsarte defines additive codes as subgroups of the underlying abelian group in a translation association scheme.

For the binary Hamming scheme, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$.

Thus, the subgroups $C$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme.
Gray Map

\[ \Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n \]

where \( n = \alpha + 2\beta \).
Gray Map

\[ \Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \rightarrow \mathbb{Z}_2^n \]

where \( n = \alpha + 2\beta \).

\[ \Phi(x, y) = (x, \phi(y_1), \ldots, \phi(y_\beta)) \]

for any \( x \in \mathbb{Z}_2^\alpha \) and any \( y = (y_1, \ldots, y_\beta) \in \mathbb{Z}_4^\beta \), where \( \phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2 \) is the usual Gray map.
Gray Map

\[ \Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \rightarrow \mathbb{Z}_2^n \]

where \( n = \alpha + 2\beta \).

\[ \Phi(x, y) = (x, \phi(y_1), \ldots, \phi(y_\beta)) \]

for any \( x \in \mathbb{Z}_2^\alpha \) and any \( y = (y_1, \ldots, y_\beta) \in \mathbb{Z}_4^\beta \), where \( \phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2 \) is the usual Gray map.

The map \( \Phi \) is an isometry which transforms Lee distances in \( \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \) to Hamming distances in \( \mathbb{Z}_2^{\alpha+2\beta} \).
Weights

Denote by $wt_H(v_1)$ the Hamming weight of $v_1 \in \mathbb{Z}_2^\alpha$ and by $wt_L(v_2)$ the Lee weight of $v_2 \in \mathbb{Z}_4^\beta$. 
Weights

Denote by $wt_H(v_1)$ the Hamming weight of $v_1 \in \mathbb{Z}_2^\alpha$ and by $wt_L(v_2)$ the Lee weight of $v_2 \in \mathbb{Z}_4^\beta$.

For a vector $v = (v_1, v_2) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, define the weight of $v$, denoted by $wt(v)$, as $wt_H(v_1) + wt_L(v_2)$, or equivalently, the Hamming weight of $\Phi(v)$.
The generator matrix for a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$:

$$G_S = \begin{pmatrix} I_{\kappa} & T' & 2T_2 & 0 & 0 \\ 0 & 0 & 2T_1 & 2I_{\gamma-\kappa} & 0 \\ 0 & S' & S & R & I_{\delta} \end{pmatrix},$$

where $T'$, $T_1$, $T_2$, $R$, $S'$ are matrices over $\mathbb{Z}_2$ and $S$ is a matrix over $\mathbb{Z}_4$. 
The following inner product is defined for any two vectors \( \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \):

\[
\langle \mathbf{u}, \mathbf{v} \rangle = 2 \left( \sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \in \mathbb{Z}_4.
\]
The following inner product is defined for any two vectors \( u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \):

\[
\langle u, v \rangle = 2\left( \sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \in \mathbb{Z}_4.
\]

The *additive dual code* of \( C \), denoted by \( C^\perp \), is defined in the standard way:

\[
C^\perp = \{ v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \langle u, v \rangle = 0 \text{ for all } u \in C \}.
\]
MacWilliams Relations

Define

\[ WL(x, y) = \sum_{c \in C} x^{n - \text{wt}_L(c)} y^{\text{wt}_L(c)}. \]
MacWilliams Relations

Define

\[ WL(x, y) = \sum_{c \in C} x^{n - wt_L(c)} y^{wt_L(c)}. \]

**Theorem**

Let \( C \) be a \( \mathbb{Z}_2 \mathbb{Z}_4 \) code, then

\[ WL_{C^\perp}(x, y) = \frac{1}{|C|} WL_C(x + y, x - y). \]
Bounds

Theorem

Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then

$$\frac{d(C) - 1}{2} \leq \frac{\alpha}{2} + \frac{\beta}{2} - \frac{\gamma}{2} - \delta;$$ (15)

$$\left\lfloor \frac{d(C) - 1}{2} \right\rfloor \leq \alpha + \beta - \gamma - \delta.$$ (16)
Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. If $C = C_X \times C_Y$, then $C$ is called *separable*. 
Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. If $C = C_X \times C_Y$, then $C$ is called *separable*.

**Theorem**

If $C$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code which is separable, then the minimum distance is given by

$$d(C) = \min \{d(C_X), d(C_Y)\}.$$
We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C$ is maximum distance separable (MDS) if $d(C)$ meets the bound given in The usual Singleton bound for a code $C$ of length $n$ over an alphabet of size $q$ is given by

$$d(C) \leq n - \log_q |C| + 1.$$
We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C$ is maximum distance separable (MDS) if $d(C)$ meets the bound given in The usual Singleton bound for a code $C$ of length $n$ over an alphabet of size $q$ is given by

$$d(C) \leq n - \log_q |C| + 1.$$ 

In the first case, we say that $C$ is MDS with respect to the Singleton bound, briefly MDSS. If it meets the second bound, $C$ is MDS with respect to the rank bound, briefly MDSR.
Theorem

Let $C$ be an MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ such that $1 < |C| < 2^{\alpha+2\beta}$. Then $C$ is either

(i) the repetition code of type $(\alpha, \beta; 1, 0; \kappa)$ and minimum distance $d(C) = \alpha + 2\beta$, where $\kappa = 1$ if $\alpha > 0$ and $\kappa = 0$ otherwise; or

(ii) the even code with minimum distance $d(C) = 2$ and type $(\alpha, \beta; \alpha - 1, \beta; \alpha - 1)$ if $\alpha > 0$, or type $(0, \beta; 1, \beta - 1; 0)$ otherwise.
Theorem

Let $C$ be an MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ such that $1 < |C| < 2^{\alpha+2\beta}$. Then, either

(i) $C$ is the repetition code as in (i) of Theorem 3 with $\alpha \leq 1$; or

(ii) $C$ is of type $(\alpha, \beta; \gamma, \alpha + \beta - \gamma - 1; \alpha)$, where $\alpha \leq 1$ and $d(C) = 4 - \alpha \in \{3, 4\}$; or

(iii) $C$ is of type $(\alpha, \beta; \gamma, \alpha + \beta - \gamma; \alpha)$, where $\alpha \leq 1$ and $d(C) \leq 2 - \alpha \in \{1, 2\}$.