On Some Modular Linear Codes

IMS Workshop on Coding and Cryptography, 10–13 September, National University of Singapore, Singapore

Manish K. Gupta

Department of Mathematics
University of Canterbury, Christchurch – 8001, NEW ZEALAND.
e-mail: mankg@computer.org
URL-: web.math.canterbury.ac.nz/~mathmkg

Monday September 10. 2001 Time: 4:30 pm
Outline:

• Brief History, Motivation and Terminology
• Linear Codes over $\mathbb{Z}_p^2$
• The concept of $p$-dimension
• Generalized Hamming Weights and Chain Condition
• Simplex and Hamming Codes
• Properties
• Generalized Gray Images
• Conclusions / Summary
History, Motivation and Introduction

• Codes over finite rings (last decade) Work of Nechaev et al, Hammons et al
  Many important families of binary non-linear codes are linear over $\mathbb{Z}_4$
  K(m) Kerdock Code P(m) Preparata-like code
• These notions has been generalized to codes over $\mathbb{Z}_{p^2}$, $p$ arbitrary prime
  Asch and Tilborg (AAECC-11, 2001)
• $\mathbb{Z}_4$-Simplex and Hamming Codes: Bhandari, Gupta and Lal (1999)
• Construction of these to codes over $\mathbb{Z}_{p^2}$
Basic Terminology:

- **Alphabets** $\mathbb{F}_q := \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$
- $GF(q)$ ($q = p^m$)
  Galois field having $q$ elements
- $\mathbb{Z}_q := \{0, 1, 2, \ldots, q - 1\}$
- $\mathbb{F}_q^n := \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_q\}$
- $\mathcal{C} : (n, M)$ Code : $\mathcal{C} \subseteq \mathbb{F}_q^n$ and $|\mathcal{C}| = M$
- Linear Code : $\mathcal{C} :$ Subspace of $GF(q)^n$
- **Generator Matrix** $G_{k \times n}$ ($k < n$) (of full rank) over $GF(q)$
  s.t. $\mathcal{C} = \text{row space} (G)$
- $|\mathcal{C}| = q^k$ : $k = \text{dim} \mathcal{C}$
- **Parity Check Matrix** $H_{(n-k) \times n}$ (of full rank) over $GF(q)$ s.t. $\mathcal{C} = \text{null space} (H)$
- Dual Code $\mathcal{C}^\perp = \{y \in \mathbb{F}_q^n \mid x \cdot y = 0 \in \mathbb{F}_q, \forall x \in \mathcal{C}\}$
- $\mathcal{C} :$ Self orthogonal (Self dual) if $\mathcal{C} \subseteq \mathcal{C}^\perp (\mathcal{C} = \mathcal{C}^\perp)$
Various distances:

**Hamming distance:** (R. W. Hamming 1948)

\[ d_H(x, y) = | \{ i \mid x_i \neq y_i \} |; x, y \in \mathbb{F}_q^n \]

= Number of nonzero components in \( x - y = w_H(x - y) \)

\[ d_H = \min \{ d_H(x, y) \mid x, y \in \mathcal{C}, x \neq y \} \]

\( \mathcal{C} : [n, k, d_H] \) Code : Can correct up to \( \left\lfloor \frac{(d_H-1)}{2} \right\rfloor \) errors

**Lee distance:** (C. Y. Lee 1958)

Suitable for memoryless, discrete and symmetric channels

\[ w_L(a) = \min \{ a, q - a \}, a \in \mathbb{Z}_q \]

\[ w_L(x) = \sum_{i=1}^{n} w_L(x_i), x \in \mathbb{Z}_q^n \]

\[ d_L(x, y) = w_L(x - y) \]
\[ d_L = \min \{ d_L(x, y) \mid x, y \in C, x \neq y \} \]
Linear Codes over $\mathbb{Z}_{p^2}$

- Linear Code $C$ of length $n$ over $\mathbb{Z}_{p^2}$: Additive subgroup of $\mathbb{Z}_p^n$
- $C : [n, k, d_H, d_{HW}]$: where $k = 2k_0 + k_1$ and $|C| = p^{2k_0}p^{k_1}$
- $C$ has a generator matrix of the form $G = \begin{bmatrix} I_{k_0} & A & B \\ 0 & pI_{k_1} & pC \end{bmatrix}$ $(k_0 + k_1) \times n$
  
  $A$ and $C$ are matrices with entries from $\{0, 1, \ldots, p - 1\}$
  
  $B$ is a matrix with arbitrary entries from $\mathbb{Z}_{p^2}$
  
  $I_{k_i}$ is the identity matrix of order $k_i$.

- Two $p$-ary linear codes
  
  **Reduction Code**
  
  $C^{(1)} = \{u \mid c \equiv u \pmod{p}, \ c \in C\}$

  **Torsion Code**
  
  $C^{(2)} = \{v \mid pv \in C\}$

- If $k_1 = 0$ then $C^{(1)} = C^{(2)}$
\textbf{p-dimension of Linear Codes over } \mathbb{Z}_p^2:\textbf{ }

- **1990:** Vazirani, Saran and Sundar Rajan
  Trellis Description
- The following two statements are not equivalent for \( S \subseteq \mathbb{Z}_4^n \) over \( \mathbb{Z}_4 \)
  1. A nontrivial linear combination of vectors in \( S \) is zero.
  2. One of the vector in \( S \) is a linear combination of some other vectors in \( S \)
- \( S = \{(1, 2); (1, 0)\} \) satisfies (1) but not (2)
- \( S = \{v_1, v_2, \ldots, v_k\} \) an ordered subset
- \( p\)-span (\( S \)):= \( \left\{ \sum_{i=1}^{k} a_i v_i | a_i \in \mathbb{Z}_p \right\} \)
- \( S : p\)-generating sequence
  \( pv_i = \sum_{j=i+1}^{k} a_j v_j \); \( a_j \in \mathbb{Z}_p \); \( i < k, pv_k = 0 \)
- \( S : p\)-linearly dependent if
  1. \( S \) is \( p\)-gen. seq. and
  2. \( \exists \ a_i \in \mathbb{Z}_p \), not all \( a_i \) zero \( \exists \ \sum_{i=1}^{k} a_i v_i = 0 \)
• $B \subseteq C$ : $p$-basis for $C$ if
  1. $B$ : $p$-linearly independent
  2. $p$-span($B$) = $C$

• Every vector in $C$ is a unique $p$-linear combination of vectors in $B$

• $p - \text{dim} \left( \mathbb{Z}_{p^2}^n \right) = 2n$

• Rows of

\[
B = \begin{bmatrix}
I_{k_0} & A & B \\
pI_{k_0} & pA & pB \\
0 & pI_{k_1} & pC
\end{bmatrix}
\]

form a $p$-basis for the code generated by $G$
Generalized Hamming Weights (G.H.W.)

- $\mathcal{C} : [n, k, d_H]$ Code
- $\mathcal{D}_r(\leq \mathcal{C}) : [n, r]$ $r$-dimensional Subcode
- $w_S(\mathcal{D}_r) = |\{i | x_i \neq 0 \text{ for some } x \in \mathcal{D}_r\}|$ : Support size of $\mathcal{D}_r$
- $d_r(\mathcal{C}) = \min\{w_S(\mathcal{D}_r) | \mathcal{D}_r \leq \mathcal{C}\}; 1 \leq r \leq k$
- For $r=1$, $d_1(\mathcal{C}) = d_H$
- **Weight Hierarchy** of $\mathcal{C}$ : $\{d_r(\mathcal{C}) | 1 \leq r \leq k\}$
- $\mathcal{C}$ satisfies **Chain Condition** if there exists a chain
  \[D_1 \subseteq D_2 \subseteq \cdots \subseteq D_k,\]
  of subcodes of $\mathcal{C}$ satisfying $w_S(D_r) = d_r(\mathcal{C})$, $1 \leq r \leq k$. 

Manish K. Gupta
Homogeneous weight

• For $x \in \mathbb{Z}_{p^2}$ it is defined as:

$$w_{HW}(x) = \begin{cases} 
0 & \text{if } x = 0 \\
p - 1 & \text{if } gcd(x, p^2) = 1 \\
p & \text{if } x \neq 0, gcd(x, p^2) = p.
\end{cases}$$

• For $x \in \mathbb{Z}_{p^2}^n$, $w_{HW}(x) = \sum_{j=1}^{n} w_{HW}(x_i)$.

• For $x, y \in \mathbb{Z}_{p^2}^n$, $d(x, y) = w_{HW}(x - y)$.

• **Lemma 1:** Let $D : [n, r]$ linear code over $\mathbb{Z}_{p^2}$

$$\sum_{c \in D} w_{HW}(c) = (p - 1)p^r \cdot w_S(D).$$

**Proof:** The $(p^r \times n)$ array of all the codewords in $D$ contains the columns with entries only of the following three types:

1. only zeros
2. $\{0, p, 2p, \ldots, (p - 1)p\}$ equally often
3. Each entry of $\mathbb{Z}_{p^2}$ equally often.
Remark 2: Thus GHW can also be defined by for $1 \leq r \leq k$

$$d_r(C) = \frac{1}{(p-1)p^r} \min \left\{ \sum_{c \in D} w_{HW}(c) \mid D \text{ is an } [n, r] \text{ subcode of } C \right\}.$$ 

- Minimum homogeneous weight $d_{HW} = \min \{ w_{HW}(c) \mid c(\neq 0) \in C \}$

Corollary 3: For $1 \leq r \leq k$ the $r^{th}$ GHW of $C$ satisfies

$$d_r(C) \geq \left\lceil \frac{(p^r - 1)d_{HW}}{(p-1)p^r} \right\rceil.$$

Corollary 4: $d_H \geq \left\lceil \frac{d_{HW}}{p} \right\rceil$.

$C \ : \ type \ \alpha \ (\beta)$ if $d_H = \left\lceil \frac{d_{HW}}{p} \right\rceil \left( d_H > \left\lceil \frac{d_{HW}}{p} \right\rceil \right)$.

Corollary 5: (Plotkin Type Bound) For an $[n, k]$ linear code over $\mathbb{Z}_{p^2}$ we have

$$d_{HW} \leq \frac{n(p-1)p^k}{p^k - 1}.$$
Let $G^\alpha_k$ be a matrix over $\mathbb{Z}_{p^2}$ consisting of all possible distinct columns of length $k$.

$$G^\alpha_k = \begin{bmatrix} (0 1 2 3 \cdots (p^2 - 1)) \otimes 1 \\ 1 \otimes G^\alpha_{k-1} \end{bmatrix}_{k \times p^{2k}}$$

where $1$ (the all 1 vector) in the first row is of length $p^{2(k-1)}$ and that in the second row is of length $p^2$.

- $S^\alpha_k$ is a $[p^{2k}, 2k]$ code.
- Each entry of $\mathbb{Z}_{p^2}$ occurs equally often in every row of $G^\alpha_k$.

**Remark 6:** If $R_i, 1 \leq i \leq k$ are the rows of the matrix $G^\alpha_k$ then $w_H(R_i) = p^{2k-2}(p - 1)$ and $w_{HW}(R_i) = p^{2k}(p - 1)$.
Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ for each $j \in \mathbb{Z}_{p^2}$ let $\omega_j(\mathbf{c}) = |\{i \mid c_i = j\}|$.

**Lemma 7:** Let $\mathbf{c}(\neq 0) \in S_k^\alpha$.

1. If for at least one $i$, $c_i$ is a unit then $\forall j \in \mathbb{Z}_{p^2} \omega_j = p^{2k-2}$ in $\mathbf{c}$.
2. If $\forall i, c_i \in Z = \{0, p, 2p, \ldots, (p-1)p\}$ then $\forall j \in Z \omega_j = p^{2k-1}$ in $\mathbf{c}$.

**$p$-ary type $\alpha$ simplex code**

$$G(P_k^\alpha) = \begin{bmatrix} (0 \ 1 \ 2 \ 3 \ \cdots \ (p-1)) \otimes 1 \\ 1 \otimes G(P_{k-1}^\alpha) \end{bmatrix}_{k \times p^k}$$

$k \geq 2$ and $G(P_1^\alpha) = [0 \ 1 \ 2 \ 3 \ \cdots \ (p-1)]$.

**Lemma 8:** The torsion code of $S_k^\alpha$ is equivalent to the $p^k$ copies of $p$-ary type $\alpha$ simplex code.
**Theorem 9:** The Hamming and Homogeneous weight distribution of $S_k^\alpha$ are:

1. $A_H(0) = 1$, $A_H(p^{2k-1}(p - 1)) = p^k - 1$, $A_H(p^{2k-2}(p^2 - 1)) = p^k(p^k - 1)$, and
2. $A_{HW}(0) = 1$, $A_{HW}(p^{2k}(p - 1)) = p^{2k} - 1$,

where $A_H(i)$ ($A_{HW}(i)$) denotes the number of vectors of Hamming (Homogeneous) weight $i$ in $S_k^\alpha$.

**Proof:** By Lemma 7, each nonzero codeword of $S_k^\alpha$ has Hamming weight either $p^{2k-2}(p^2 - 1)$ or $p^{2k-1}(p - 1)$ and Homogeneous weight $p^{2k}(p - 1)$. Since dimension of the torsion code is $k$, there will be $p^k - 1$ codewords of the weight $p^{2k-1}(p - 1)$. Hence the number of codewords having weight $p^{2k-2}(p^2 - 1)$ will be $p^{2k} - p^k$. 
Remark 10:

1. $S^\alpha_k$ is an equidistant code with respect to Homogeneous distance whereas $S_k$ is an equidistant binary code with respect to Hamming distance.
2. The minimum weights are: $d_H = p^{2k-1}(p - 1)$ and $d_{HW} = p^{2k}(p - 1)$
3. $S^\alpha_k$ is of type $\alpha$ as $d_H = \frac{d_{HW}}{p}$.

Symmetrized weight enumerator (swe) of a linear code $C$ over $\mathbb{Z}_{p^2}$

$$swe(x, y, z) = \sum_{c \in C} x^{n_0(c)} y^{n_1(c)} z^{n_p(c)},$$

where $n_0(c) = |\{1 \leq i \leq n \mid c_i = 0\}|$, $n_1(c) = |\{1 \leq i \leq n \mid \gcd(c_i, p^2) = 1\}|$

and

$$n_p(c) = |\{1 \leq i \leq n \mid \gcd(c_i, p^2) = p\}|.$$

Let $\tilde{S}^\alpha_k$ be the punctured code of $S^\alpha_k$ obtained by deleting the zero coordinate. Then the swe of $\tilde{S}^\alpha_k$ is

$$swe(x, y, z) = x^{n(k)} + (p^k - 1)x^{p^{2k-1}}z^{p^{2k}} + p^k(p^k - 1)x^{n(k-1)}y^{(p-1)p^{2k-1}}z^{p^{2k-1}},$$

where $n(k) = p^{2k} - 1$. 

Manish K. Gupta
Type $\beta$ Simplex Code: $S^\beta_k$

Let

$$G_2^\beta = \begin{bmatrix} 1 & (0 \ p \ 2p \ 3p \cdots (p^2 - p)) \\ G_1^\alpha & 1 \end{bmatrix}_{2 \times p^2+p},$$

and for $k > 2$,

$$G_k^\beta = \begin{bmatrix} 1 & (0 \ p \ 2p \ 3p \cdots (p^2 - p)) \otimes 1 \\ G_{k-1}^\alpha & 1 \otimes G_{k-1}^\beta \end{bmatrix},$$

where all the five all 1 vectors i.e, 1’s are of appropriate sizes and tensor product is expanded from right to left.

- No two columns of $G_k^\beta$ are multiples of each other.
- The length of $S^\beta_k$ is $\frac{p^{k-1}(p^k-1)}{p-1}$.
- $S^\beta_k$ is a $\left[\frac{p^{k-1}(p^k-1)}{p-1}, 2k\right]$ code.
Proposition 11: Each row of $G_k^\beta$ contains $p^{2k-2}$ units and
$\forall j \in Z = \{0, p, 2p, \ldots, (p - 1)p\}$ $\omega_j = \frac{p^{k-2}(p^{k-1}-1)}{p-1}$.

Remark 12: If $R_i, 1 \leq i \leq k$ are the rows of the matrix $G_k^\beta$ then
$w_H(R_i) = p^{k-2}(p^k + p^{k-1} - 1)$ and $w_{HW}(R_i) = p^{k-1}(p^k - 1)$.

Lemma 13: Let $c \in S_k^\beta, c \neq 0$.

1. If for at least one $i$, $c_i$ is a unit then $\sum_{i \in U} \omega_i(c) = p^{2k-2}$, and
$\forall j \in Z \omega_j(c) = \frac{p^{k-2}(p^{k-1}-1)}{p-1}$.

2. If $\forall i, c_i \in Z = \{0, p, 2p, \ldots, (p - 1)p\}$ then $\sum_{i \in Z, i \neq 0} \omega_i(c) = p^{2k-2}$ and
$\omega_0(c) = p^{k-1}p^{k-1} - 1 \frac{p-1}{p-1}$ in $c$.

Lemma 14: The $p$-ary torsion code of $S_k^\beta$ is equivalent to $p^{k-1}$ copies of the $p$-ary simplex code.
Theorem 15: The Hamming and Homogeneous weight distributions of $S^\beta_k$ are:

1. $A_H(0) = 1$, $A_H \left( p^{2(k-1)} \right) = (p^k - 1)$, $A_H \left( p^{k-2}(p^k + p^{k-1} - 1) \right) = p^k(p^k - 1)$.

2. $A_{HW}(0) = 1$, $A_{HW}(p^{2k-1}) = (p^k - 1)$, $A_{HW}(p^{k-1}(p^k - 1)) = p^k(p^k - 1)$,
   where $A_H(i)$ ($A_{HW}(i)$) denotes the number of vectors of Hamming (Homogeneous) weight $i$ in $S^\beta_k$.

Remark 16:

1. The swe of $S^\beta_k$ is given as

$$swe(x, y, z) = x^{n(k)} + (p^k - 1)x^{pn(k-1)}z^{p^{2k-2}} +$$

$$p^k(p^k - 1)x^{n(k-1)}y^{p^{2k-2}}z^{p^{k-2}(p^{k-1} - 1)},$$

where $n(k) = p^{k-1}\frac{p^{k-1}}{p-1}$.

2. The minimum weights of $S^\beta_k$ are: $d_H = p^{2k-2}$ and $d_{HW} = p^{k-1}(p^k - 1)$. 
Griesmer Bound for Codes over Rings

Theorem 17: Shiromoto and Strome (2001) For a linear code $C$ of length $n$, rank $k$ and minimum Hamming distance $d_H$ over $\mathbb{Z}_{p^s}$ the following inequality holds:

$$n \geq k - 1 \sum_{i=0}^{k-1} \left\lceil \frac{d_H}{p^i} \right\rceil.$$

Application of the above inequality to $S^\beta_k$ for $s = 2$ yields the following.

Proposition 18: The simplex codes of type $\beta$ meet the Griesmer bound for codes over rings.

\[ n = p^{k-1} \frac{p^{k-1}}{p-1} \text{ and } d_H = p^{2(k-1)} \]
Theorem 19: $S_k^\alpha$ satisfies the chain condition and its weight hierarchy is given by

$$d_r(S_k^\alpha) = p^{2k} - p^{2k-r}; 1 \leq r \leq 2k.$$  

Proof: By Remark, Any $r$-dimensional subcode of $S_k^\alpha$ is of constant Homogeneous weight. Hence by definition,

$$d_r(S_k^\alpha) = \frac{1}{(p-1)p^r(p^r-1)p^{2k}(p-1)} = p^{2k} - p^{2k-r}.$$

Let

\begin{align*}
D_1 &= <pR_1>, \\
D_2 &= <pR_1,pR_2>, \\
D_3 &= <R_1,pR_1,pR_2>, \\
D_4 &= <R_1,pR_1,R_2,pR_2>, \ldots, \text{and} \\
D_{2k} &= <R_1,pR_1,\ldots,R_k,pR_k>.
\end{align*}
It is easy to verify that
\[ D_1 \subseteq D_2 \subseteq \cdots \subseteq D_{2k}, \]
and \( w_S(D_r) = d_r(S_k^\alpha) \) for \( 1 \leq r \leq 2k \).

**Theorem 20:** \( S_k^\beta \) satisfies the chain condition and its weight hierarchy is given by
\[
d_r(S_k^\beta) = n(k) - p^{k-r-1}(p^k - p^{\lceil \frac{r}{2} \rceil}) \frac{p-1}{p-1}  \\
1 \leq r \leq 2k.
\]
where \( n(k) = p^{k-1}(p^{k-1}) \frac{p-1}{p-1} \).

**Proof:**
\[
d_r(S_k^\beta) = pd_r(S_{k-1}^\beta) + d_r(S_{k-1}^\alpha)
\]
\[
D_1 = < pR_1 >, \\
D_2 = < R_1, pR_1 >, \\
D_3 = < R_1, pR_1, pR_2 >, \\
D_4 = < R_1, pR_1, R_2, pR_2 >, \ldots, \text{and} \\
D_{2k} = < R_1, pR_1, \ldots, R_k, pR_k >.
\]
Theorem 21: The codes $S_k^\alpha (k \geq 1)$ and $S_k^\beta (k \geq 3)$ are self orthogonal.

Proof: By Induction on $k$. 
Let $x \in \mathbb{Z}_{p^2}$. Thus $x = a + lp$, where $0 \leq a, l \leq p - 1$.

For $k = 0, \ldots, p - 1$ Define

$$
\phi_k(x) = (ka + l) \pmod{p}
$$

Then $\phi$, a map from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p^p$, is defined as:

$$
\phi(x) = (\phi_0(x), \ldots, \phi_{p-1}(x)).
$$

$\phi$ has natural extension from $\mathbb{Z}_{p^2}^n$ into $\mathbb{Z}_p^{pn}$.
**Example:** For \( p = 3 \):

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \phi(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
</tr>
<tr>
<td>1</td>
<td>012</td>
</tr>
<tr>
<td>2</td>
<td>021</td>
</tr>
<tr>
<td>3</td>
<td>111</td>
</tr>
<tr>
<td>4</td>
<td>120</td>
</tr>
<tr>
<td>5</td>
<td>102</td>
</tr>
<tr>
<td>6</td>
<td>222</td>
</tr>
<tr>
<td>7</td>
<td>201</td>
</tr>
<tr>
<td>8</td>
<td>210</td>
</tr>
</tbody>
</table>

**Proposition 22:** Asch and Tilborg (2001)

\( \phi \) is isometric injection from \((\mathbb{Z}_p^2, w_{HW})\) into \((\mathbb{Z}_p^p, w_H)\)
**Generalized Gray Images**

**Theorem 23:** \( \phi(\overline{S}_k^\alpha) \) and \( \phi(S_k^\beta) \) are non-linear \( p \)-ary families of codes for all \( k \).

**Remark 24:**

1. \( \phi(\overline{S}_k^\alpha) \) is a \( p \)-ary non-linear code of length \( p^{2k+1} - p \) and minimum Hamming distance \( p^{2k}(p-1) \). It meets the \( p \)-ary Plotkin bound and \( n < \frac{p}{p-1}d_H \).

2. \( \phi(S_k^\beta) \) is a \( p \)-ary non-linear code of length \( p^k \left(\frac{p^k-1}{p-1}\right) \) and minimum Hamming distance \( p^{k-1}(p^k - 1) \). This is an example of a code having \( n = \frac{p}{p-1}d_H \).
Conclusions / Summary

- $\phi(GK_{p^2,m}) : (p^{m+1}, p^{2m+2}, \geq (p - 1)(p^m - (p - 1)p^{m-2})$
- $\phi(GP_{p^2,m}) : (p^{m+1}, p^{2p^m-2m-2}, 3(p - 1))$
- Generalized Kerdock and Preparata Codes ($p^2$-ary linear) miss some of their nice combinatorial properties when $p$ is odd. For e.g. $\phi(GP_{p^2,m})$ does not meet the Johnson Bound. A fortiori: This code is not uniformly packed. (Asch and Tilborg 2001)

Question 1:
- Does the generalized Gray map of Hamming code over $\mathbb{Z}_{p^2}$ is uniformly packed? (we know that it is true for $p = 2$)

Answer:

$$\phi(S_{2^\beta}^{\perp}) : (p^3 + p^2, p^{2p^2+2p-4}, 3(p - 1)) .$$