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
- $\mathbb{Z}_q \ := \{0, 1, 2, \ldots, q-1\}$
- $\mathbb{F}_q^n := \{(x_1, \cdots, x_n) \mid x_i \in \mathbb{F}_q\}$
- $\mathcal{C} : (n, M)$ Code $\quad : \mathcal{C} \subseteq \mathbb{F}_q^n$ 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. $\mathcal{C} =$ row space (G)
- $\#\mathcal{C} = q^k \quad : \quad \mathrm{k} = \dim \mathcal{C}$
- **Parity Check Matrix** $H_{(n-k) \times n}$ (of full rank) over GF(q) s.t. $\mathcal{C} =$ null space (H)
- **Dual Code** $\mathcal{C}^{\perp} = \left\{\mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \in \mathbb{F}_q,\ \forall\, \mathbf{x} \in \mathcal{C}\right\}$
- $\mathcal{C}$: Self orthogonal (Self dual) if $\mathcal{C} \subseteq \mathcal{C}^{\perp} \left(\mathcal{C} = \mathcal{C}^{\perp}\right)$

Various distances:

Hamming distance: (R. W. Hamming 1948)

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

$$= \text{Number of nonzero components in } \mathbf{x}-\mathbf{y} = w_H(\mathbf{x}-\mathbf{y})$$

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

$\mathcal{C} : [n, k, d_H]$ 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

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

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

$$d_L(\mathbf{x},\mathbf{y}) = w_L(\mathbf{x}-\mathbf{y})$$

$$d_L = \min \{ d_L(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y} \}$$

Linear Codes over $\mathbb{Z}_{p^2}$

- Linear Code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^2}$: Additive subgroup of $\mathbb{Z}_{p^2}^n$
- $\mathcal{C} : [n, k, d_H, d_{HW}]$: where $k = 2k_0 + k_1$ and $|\mathcal{C}| = p^{2k_0} p^{k_1}$
- $\mathcal{C}$ has a generator matrix of the form $G = \begin{bmatrix} I_{k_0} & A & B \\ \mathbf{0} & pI_{k_1} & pC \end{bmatrix}_{(k_0+k_1)\times n}$

  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

  $$\mathcal{C}^{(1)} = \{u \mid c \equiv u \pmod{p}, \quad c \in \mathcal{C}\}$$

  Torsion Code

  $$\mathcal{C}^{(2)} = \{v \mid pv \in \mathcal{C}\}$$

- If $k_1 = 0$ then $\mathcal{C}^{(1)} = \mathcal{C}^{(2)}$

p-dimension of Linear Codes over $\mathbb{Z}_{p^2}$:

- **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)
- $S = \{v_1, v_2, \cdots, v_k\}$ 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 $\ni \sum_{i=1}^{k} a_i v_i = \mathbf{0}$

- $\mathcal{B} \subseteq \mathcal{C}$: p-*basis* for $\mathcal{C}$ if
  1. $\mathcal{B}$: p-linearly independent
  2. p-span$(\mathcal{B}) = \mathcal{C}$
- Every vector in $\mathcal{C}$ is a unique p-linear combination of vectors in $\mathcal{B}$
- $p - dim\left(\mathbb{Z}_{p^2}^n\right) = 2n$
- Rows of

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

  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**
- $w_S(\mathcal{D}_r) = |\{i \mid x_i \neq 0 \text{ for some } \mathbf{x} \in \mathcal{D}_r\}|$:**Support size of $\mathcal{D}_r$**
- $d_r(\mathcal{C}) = \min\{w_S(\mathcal{D}_r) \mid \mathcal{D}_r \leq \mathcal{C}\}; 1 \leq r \leq k$
- For r=1, $d_1(\mathcal{C}) = d_H$
- **Weight Hierarchy of $\mathcal{C}$** : $\{d_r(\mathcal{C}) \mid 1 \leq r \leq k\}$
- $\mathcal{C}$ satisfies **Chain Condition** if there exists a chain

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_k,$$

of subcodes of $\mathcal{C}$ satisfying $w_S(D_r) = d_r(\mathcal{C})$, $1 \leq r \leq k$.

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 $\mathcal{D} : [n, r]$ linear code over $\mathbb{Z}_{p^2}$

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

Proof: The $(p^r \times n)$ array of all the codewords in $\mathcal{D}$ 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 $1 \leq r \leq k$

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

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

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

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

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

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

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

$$d_{HW} \leq \frac{n(p-1)p^k}{p^k - 1}.$$

Type α Simplex Code: S_k^α

Let G_k^α be a matrix over $\mathbb{Z}_{p^2}$ consisting of all possible distinct columns of length k.

$$G_k^\alpha = \left[\begin{array}{c} (0\ 1\ 2\ 3 \cdots (p^2-1)) \otimes \mathbf{1} \\ \hline \mathbf{1} \otimes G_{k-1}^\alpha \end{array}\right]_{k \times p^{2k}} \quad k \geq 2 \text{ and } G_1^\alpha = [0\ 1\ 2\ 3 \cdots (p^2-1)],$$

where $\mathbf{1}$ (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_k^α is a $\left[p^{2k}, 2k\right]$ code.
- Each entry of $\mathbb{Z}_{p^2}$ occurs equally often in every row of G_k^α.

  Remark 6: If $R_i, 1 \leq i \leq k$ are the rows of the matrix G_k^α 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 α simplex code

  $$G(P_k^{\alpha}) = \left[\frac{(0\ 1\ 2\ 3 \cdots (p-1)) \otimes \mathbf{1}}{\mathbf{1} \otimes G(P_{k-1}^{\alpha})}\right]_{k \times p^k} \quad k \geq 2 \text{ and } G(P_1^{\alpha}) = [0\ 1\ 2\ 3 \cdots (p-1)].$$

  Lemma 8: The torsion code of S_k^{α} is equivalent to the p^k copies of p-ary type α simplex code.

Theorem 9: The Hamming and Homogeneous weight distribution of S_k^α 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^α.

Proof: By Lemma 7, each nonzero codeword of S_k^α 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_k^α 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_k^α is of type α as $d_H = \frac{d_{HW}}{p}$.

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

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

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

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

Let $\bar{S_k^\alpha}$ be the punctured code of S_k^α obtained by deleting the zero coordinate. Then the swe of $\bar{S_k^\alpha}$ 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 $n(k) = p^{2k} - 1$.

Type β Simplex Code: S_k^β

Let

$$G_2^\beta = \left[\begin{array}{c|c} \mathbf{1} & (0\ p\ 2p\ 3p \cdots (p^2-p)) \\ \hline G_1^\alpha & \mathbf{1} \end{array}\right]_{2\times p^2+p},$$

and for $k > 2$,

$$G_k^\beta = \left[\begin{array}{c|c} \mathbf{1} & (0\ p\ 2p\ 3p \cdots (p^2-p)) \otimes \mathbf{1} \\ \hline G_{k-1}^\alpha & \mathbf{1} \otimes G_{k-1}^\beta \end{array}\right],$$

where all the five all 1 vectors i.e, $\mathbf{1}$'s are of appropriate sizes and tensor product is expanded from right to left.

- No two columns of G_k^β are multiples of each other.
- The length of S_k^β is $\frac{p^{k-1}(p^k-1)}{p-1}$.
- S_k^β is a $\left[\frac{p^{k-1}(p^k-1)}{p-1}, 2k\right]$ code.

Proposition 11: Each row of G_k^β 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^β 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 $\mathbf{c} \in S_k^\beta, \mathbf{c} \neq 0$.

1. If for at least one i, c_i is a unit then $\sum_{i \in U} \omega_i(\mathbf{c}) = p^{2k-2}$,and $\forall j \in Z$ $\omega_j(\mathbf{c}) = \frac{p^{k-2}(p^{k-1}-1)}{p-1}$.
2. If $\forall i$, $c_i \in Z = \{0, p, 2p, \ldots, (p-1)p\}$ then $\sum_{i \in Z, i \neq 0} \omega_i(\mathbf{c}) = p^{2k-2}$and $\omega_0(\mathbf{c}) = p^{k-1}\frac{p^{k-1}-1}{p-1}$ in $\mathbf{c}$.

Lemma 14: The p-ary torsion code of S_k^β is equivalent to p^{k-1} copies of the p-ary simplex code.

Theorem 15: The Hamming and Homogeneous weight distributions of S_k^β 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_k^β.

Remark 16:

1. The swe of S_k^β is given as

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

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

2. The minimum weights of S_k^β 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 $\mathcal{C}$ of length n, rank k and minimum Hamming distance d_H over $\mathbb{Z}_{p^s}$ the following inequality holds:

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

Application of the above inequality to S_k^{β} for $s = 2$ yields the following.

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

$n = p^{k-1} \frac{p^k - 1}{p-1}$ and $d_H = p^{2(k-1)}$

Generalized Hamming Weights

Theorem 19: S_k^{α} 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^{α} 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

$$\begin{aligned}
D_1 &= < pR_1 >, \\
D_2 &= < pR_1, pR_2 >, \\
D_3 &= < R_1, pR_1, pR_2 >, \\
D_4 &= < R_1, pR_1, R_2, pR_2 >, \ldots, \text{and} \\
D_{2k} &= < R_1, pR_1, \ldots, R_k, pR_k > .
\end{aligned}$$

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^β satisfies the chain condition and its weight hierarchy is given by

$$d_r(S_k^\beta) = n(k) - p^{k-r-1}\frac{(p^k - p^{\lceil \frac{r}{2} \rceil})}{p-1} \quad 1 \leq r \leq 2k.$$

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

Proof:

$$d_r(S_k^\beta) = pd_r(S_{k-1}^\beta) + d_r(S_{k-1}^\alpha)$$

$$\begin{aligned} D_1 &= < pR_1 >, \\ D_2 &= < R_1, pR_1 >, \\ D_3 &= < R_1, pR_1, pR_2 >, \\ D_4 &= < R_1, pR_1, R_2, pR_2 >, \ldots, \text{and} \\ D_{2k} &= < R_1, pR_1, \ldots, R_k, pR_k > . \end{aligned}$$

Theorem 21: The codes S_k^{α} $(k \geq 1)$ and S_k^{β} $(k \geq 3)$ are self orthogonal.

Proof: By Induction on k.

Generalized Gray Map

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

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

ϕ has natural extension from $\mathbb{Z}_{p^2}^n$ into $\mathbb{Z}_p^{pn}$.

Example: For $p = 3$:

x	$\phi(x)$
0	000
1	012
2	021
3	111
4	120
5	102
6	222
7	201
8	210

Proposition 22: Asch and Tilborg (2001)
ϕ is isometric injection from $(\mathbb{Z}_{p^2}, w_{HW})$ into $\left(\mathbb{Z}_p^p, w_H\right)$

Generalized Gray Images

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

Remark 24:

1. $\phi(\bar{S_k^\alpha})$ 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 $p^k \frac{(p^k-1)}{p-1}$ 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

- $\phi(GK_{p^2,m}) : \left(p^{m+1}, p^{2m+2}, \geq (p-1)(p^m - (p-1)p^{\frac{m}{2}}\right)$
- $\phi(GP_{p^2,m}) : \left(p^{m+1}, p^{2p^m-2m-2}, 3(p-1)\right)$
- 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:

$$\phi(S_2^{\beta^\perp}) : \left(p^3 + p^2, p^{2p^2+2p-4}, 3(p-1)\right).$$