

On the weight enumerators of the projections of the 2-adic Golay code of length 24 to \mathbb{Z}_{2^e}

Sunghyu Han

School of Liberal Arts, Korea University of Technology and Education

2012 Kias International Conference on Coding Theory and Applications
Nov. 15–17, 2012, Kias 5th floor Seminar room (1503), Seoul

Introduction

- Calderbank and Sloane : Codes over $\mathbb{Z}_p \rightarrow \mathbb{Z}_{p^e} \rightarrow \mathbb{Z}_{p^\infty}$
- Hamming code $[8, 4, 5]_{2^\infty}$, Golay code $[24, 12, 13]_{2^\infty}$, $[12, 6, 7]_{3^\infty}$: Self-dual and MDS.
- Dougherty, Kim, and Park : Weight distribution of the projections of these three codes to \mathbb{Z}_{p^e} , ($e \geq 1$).
- Done : Hamming code $[8, 4, 5]_{2^\infty}$, $[12, 6, 7]_{3^\infty}$
- Open : Golay code $[24, 12, 13]_{2^\infty}$

Codes over \mathbb{Z}_q

- $\mathbb{Z}_q (q = p^e, 1 \leq e \leq \infty)$
- Linear code \mathcal{C} of length n over \mathbb{Z}_q : Submodule of \mathbb{Z}_q^n .
- Weight : $wt(\mathbf{x})$, $\mathbf{x} = (x_1, x_2, \dots, x_n)$, # nonzero components
- Minimum distance $d = d(\mathcal{C})$: the smallest weight among nonzero codewords in \mathcal{C} .
- If q is finite, then the *weight enumerator* of \mathcal{C} is $W_{\mathcal{C}}(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$, where A_i is the number of codewords of weight i in \mathcal{C} .
- $(A_0, A_1, A_2, \dots, A_n)$ is called the *weight distribution* of \mathcal{C} .

Codes over \mathbb{Z}_q

- \mathcal{C} : code over \mathbb{Z}_{p^∞} , \mathbb{Z}_{p^∞} : PID, \mathcal{C} : free, $\text{dimension}(\mathcal{C}) = \text{rank}(\mathcal{C})$
- \mathcal{C} : code over \mathbb{Z}_{p^e} . We only consider a free submodule of \mathcal{C} .
 $\text{dimension}(\mathcal{C}) = \text{rank}(\mathcal{C})$
- $[n, k]$ code, $[n, k, d]$ code
- G : Generator matrix \leftarrow generators of \mathcal{C}

Lifts of codes

- $\mathbb{Z}_{p^e} : \sum_{i=0}^{e-1} a_i p^i = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_{e-1} p^{e-1}$
- $\mathbb{Z}_{p^\infty} : \sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$
- $\Psi_e : \mathbb{Z}_{p^\infty} \rightarrow \mathbb{Z}_{p^e} : \Psi_e(\sum_{i=0}^{\infty} a_i p^i) = \sum_{i=0}^{e-1} a_i p^i.$
- $\Psi_e = \Psi_e^f : \mathbb{Z}_{p^f} \rightarrow \mathbb{Z}_{p^e} : \Psi_e(\sum_{i=0}^{f-1} a_i p^i) = \sum_{i=0}^{e-1} a_i p^i,$
- $1 \leq e_1 < e_2 \leq \infty$. A code C_1 over $\mathbb{Z}_{p^{e_1}}$ *lifts* to a code C_2 over $\mathbb{Z}_{p^{e_2}}$, denoted by $C_1 \prec C_2$, if C_2 has a generator matrix G_2 such that $\Psi_{e_1}(G_2)$ is a generator matrix of C_1 .
- $C : p$ -adic code, $C^e = \Psi_e(C)$ is a code over \mathbb{Z}_{p^e} .
 $C^1 \prec C^2 \prec \cdots \prec C^e \prec \cdots \prec C$

Self-dual codes

- $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n.$
- $\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_q^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in \mathcal{C}\}$
- \mathcal{C} (self-dual) : $\mathcal{C} = \mathcal{C}^\perp.$

-

$$W_C(x, y) = \sum_{j=0}^{n/2} c_j (x^2 + (p^e - 1)y^2)^j (xy - y^2)^{n/2-2j}.$$

Example : 2-adic Hamming code

- $x^7 - 1 = (x - 1)(x^3 - ax^2 + (a - 1)x - 1)(x^3 - (a - 1)x - ax - 1), \mathbb{Z}_{p^\infty},$
 $a = 0 + 2 + 4 + 32 + 128 + 256 + \dots, a^2 - a + 2 = 0.$
- $[7, 4]$ cyclic code, $x^3 + ax^2 + (a - 1)x - 1.$
- $[8, 4, 5]$ self-dual Hamming code $\mathcal{H}.$
- $G = \begin{pmatrix} -1 & a - 1 & a & 1 & 0 & 0 & 0 & 1 \\ 0 & -1 & a - 1 & a & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & a - 1 & a & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 & a - 1 & a & 1 & 1 \end{pmatrix}.$
- $\mathcal{H}^1 \prec \mathcal{H}^2 \prec \dots \prec \mathcal{H}^e \prec \dots \prec \mathcal{H}$
- $W_{\mathcal{H}^e}(x, y) = \sum_{j=0}^4 c_i (x^2 + (2^e - 1)y^2)^j (xy - y^2)^{8-2j}$

2-adic Golay code

- $x^{23} - 1 = (x - 1)\pi_1(x)\pi_2(x),$

$$\begin{aligned}\pi_1(x) = & x^{11} + ax^{10} + (a - 3)x^9 - 4x^8 - (a + 3)x^7 - (2a + 1)x^6 \\ & - (2a - 3)x^5 - (a - 4)x^4 + 4x^3 + (a + 2)x^2 + (a - 1)x - 1,\end{aligned}$$

$$a = 0 + 2 + 8 + 32 + 64 + 128 + \cdots, a^2 - a + 6 = 0.$$

- $[23, 12]$ cyclic code, $\pi_1(x)$.
- $[24, 12, 13]$ self-dual Golay code \mathcal{G} .
- $\mathcal{G}^1 \prec \mathcal{G}^2 \prec \cdots \prec \mathcal{G}^e \prec \cdots \prec \mathcal{G}$

2-adic Golay code

- $W_{G^1}(x, y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$
-

$$\begin{aligned} W_{G^2}(x, y) = & x^{24} + 759x^{16}y^8 + 12144x^{14}y^{10} \\ & + 172592x^{12}y^{12} + 61824x^{11}y^{13} + 765072x^{10}y^{14} \\ & + 1133440x^9y^{15} + 1239447x^8y^{16} + 4080384x^7y^{17} \\ & + 1445136x^6y^{18} + 4080384x^5y^{19} + 1870176x^4y^{20} \\ & + 1133440x^3y^{21} + 692208x^2y^{22} + 61824xy^{23} + 28385y^{24}. \end{aligned}$$

2-adic Golay code

- $W_{\mathcal{G}^e}(x, y) = \sum_{j=0}^{12} c_j (x^2 + (2^e - 1)y^2)^j (xy - y^2)^{24-2j}$
- 13 unknowns $c_0, c_1, c_2, \dots, c_{12}$
- $(A_0^e, A_1^e, \dots, A_{24}^e)$: Weight distribution of \mathcal{G}^e
- $d(\mathcal{G}^e) = 8$, $A_8^e = 759$, $A_9^e = 0$, for all e .
- $A_{10}^e, A_{11}^e, A_{12}^e$: constant for $e \geq N$, ($N = 7$)
- We only have to calculate $A_{10}^e, A_{11}^e, A_{12}^e$, $e = 3, 4, 5, 6, 7$

Calculation with Magma function

- “WeightDistribution(\mathcal{G}^e)”

$$\begin{aligned} W_{\mathcal{G}^3} = & x^{24} + 759x^{16}y^8 + 12144x^{14}y^{10} + 48576x^{13}y^{11} + 658352x^{12}y^{12} + 3197184x^{11}y^{13} \\ & + 19418256x^{10}y^{14} + 91760064x^9y^{15} + 353026839x^8y^{16} + 1172818944x^7y^{17} \\ & + 3191916816x^6y^{18} + 7043277120x^5y^{19} + 12350180832x^4y^{20} + 16437535488x^3y^{21} \\ & + 15712113648x^2y^{22} + 9555133248xy^{23} + 2788378465y^{24} \end{aligned}$$

- Running time : $W_{\mathcal{G}^1}$, $W_{\mathcal{G}^2}$, and $W_{\mathcal{G}^3}$: 0.000(sec), 0.983(sec), 14653.704(sec)(\approx four hours)
- We expect that the running time of $W_{\mathcal{G}^4}$ is more than two years.

Calculation with Magma function 2

- $A_{10}^e, A_{11}^e, A_{12}^e, e = 3, 4, 5, 6, 7$
- “NumberOfWords(C, w)”, “PartialWeightDistribution(C, ub)” : codes over Finite Fields. Not applied for codes over a ring.

Algorithm 1

Computation : A_w

- $G = [I|A]$ for $C : [n, k, d]$ code
- $c = a_1 G_{i_1} + a_2 G_{i_2} + \cdots + a_t G_{i_t} (1 \leq t \leq w), (a_i \neq 0)$

Algorithm 2

Computation : A_w

- $G' = [I, A']$, $G'' = [A'', I]$ for $C : [n, k, d]$ code, $n = 2k$,
- $c = (c_1, c_2)$, $wt(c) = w$
 $\Rightarrow wt(c_1) \leq w/2$ or $wt(c_2) < w/2$
- (GNW)
 $c' = a_1 G'_{i_1} + a_2 G'_{i_2} + \cdots + a_t G'_{i_t} (1 \leq t \leq w/2), (a_i \neq 0)$
 $c'' = a_1 G''_{i_1} + a_2 G''_{i_2} + \cdots + a_t G''_{i_t} (1 \leq t < w/2), (a_i \neq 0)$

Algorithm 3

Computation : A_w

- $G' = [I, A']$, $G'' = [A'', I]$ for $C : [n, k, d]$ code, $n = 2k$,
- $c' = (c'_1, c'_2) \Rightarrow wt(c'_1) = t, wt(c'_2) = w - t$
- $c'' = (c''_1, c''_2) \Rightarrow wt(c''_1) = w - t, wt(c''_2) = t$
- A_w : count codewords of weight $w - t$

$$c'_2 = a_1 A'_{i_1} + a_2 A'_{i_2} + \cdots + a_t A'_{i_t} (1 \leq t \leq w/2), (a_i \neq 0)$$

$$c''_2 = a_1 A''_{i_1} + a_2 A''_{i_2} + \cdots + a_t A''_{i_t} (1 \leq t < w/2), (a_i \neq 0)$$

- Number of calculation for $\mathcal{G}^e : [24, 12, 8]$ over \mathbb{Z}_{2^e}

$$\sum_{1 \leq t \leq w/2} \binom{12}{t} (2^e - 1)^t + \sum_{1 \leq t < w/2} \binom{12}{t} (2^e - 1)^t.$$

- If $e = 7$ and $w = 12$ then 2^{et} is 2^{42} .
- For $w = 8$, the running times of $e = 1, 2, 3, 4$ are 0.016, 0.609, 17.109, 340.344 seconds, respectively.
- It is computationally impossible to calculate the number of codewords of weight 12 in $W_{\mathcal{G}^7}$.

Our Method

- $c'_2 = a_1 A'_{i_1} + a_2 A'_{i_2} + \cdots + a_t A'_{i_t}, wt(c'_2) = w - t,$
- \Rightarrow Number of zero's of $c'_2 : k - (w - t)$
- $M = (m_{ij})$ whose rows are $A'_{i_1}, A'_{i_2}, \dots, A'_{i_t}.$
- For $i = 1, 2, \dots, k$, we define

$$Z'_i = \{(x_1, x_2, \dots, x_t) \in (\mathbb{Z}_{p^e} - \{0\})^t \mid m'_{1i}x_1 + m'_{2i}x_2 + \cdots + m'_{ti}x_t = 0\},$$

•

$$f(A', \{i_1, i_2, \dots, i_t\}) = \sum_{I \subseteq \{1, 2, \dots, k\}, |I| = k - (w - t)} \left| \bigcap_{j \in I} Z'_j - \bigcup_{j \notin I} Z'_j \right|.$$

•

$$\begin{aligned} & \sum_{1 \leq t \leq w/2} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A', t)} f(A', \{i_1, i_2, \dots, i_t\}) \\ & + \sum_{1 \leq t < w/2} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A'', t)} f(A'', \{i_1, i_2, \dots, i_t\}). \end{aligned}$$

Result

Table : A_w^e

	$e = 1$	$e = 2$	$e = 3$	$e = 4$	$e = 5$	$e = 6$	$e = 7$
$w = 8$	759	759	759	759	759	759	759
$w = 9$	0	0	0	0	0	0	0
$w = 10$	0	12144	12144	12144	12144	12144	12144
$w = 11$	0	0	48576	48576	48576	48576	48576
$w = 12$	2576	172592	658352	1629872	2504240	3281456	3281456

- PC with 2.3GHz and 3.00GB RAM.(Magma)
- The running time for $e = 7$ with $w = 8, 9, 10, 11, 12$ are 15, 27, 43, 60, 135 seconds, respectively.
- We can quickly calculate $\bigcap_{j \in I} Z'_j$ since we can view $\bigcap_{j \in I} Z'_j$ as a homogeneous system of linear equations with $|I|$ equations and t unknowns.

Example

- \mathcal{H}^2, A_4^2

- $G = \begin{pmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 & 1 \end{pmatrix}.$

- $G' = (I, A'), G'' = (A'', I),$

$$A' = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 2 & 1 & 1 & 3 \\ 1 & 1 & 3 & 2 \\ 3 & 2 & 3 & 3 \end{pmatrix}, A'' = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 3 & 3 & 3 & 2 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 2 & 1 \end{pmatrix}.$$

-

$$\begin{aligned} A_4^2 = & \sum_{t=1,2} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A', t)} f(A', \{i_1, i_2, \dots, i_t\}) \\ & + \sum_{t=1} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A'', t)} f(A'', \{i_1, i_2, \dots, i_t\}). \end{aligned}$$

Example

- The first part :

$$\sum_{t=1} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A', t)} f(A', \{i_1, i_2, \dots, i_t\}),$$

- The second part :

$$\sum_{t=2} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A', t)} f(A', \{i_1, i_2, \dots, i_t\}),$$

- The third part :

$$\sum_{t=1} \sum_{\{i_1, i_2, \dots, i_t\} \in LC(A'', t)} f(A'', \{i_1, i_2, \dots, i_t\}).$$

Example : The first part

-

$$\begin{aligned} & \sum_{\{i_1\} \in LC(A', 1)} f(A', \{i_1\}) \\ &= f(A', \{r_1\}) + f(A', \{r_2\}) + f(A', \{r_3\}) + f(A', \{r_4\}). \end{aligned}$$

- $f(A', \{r_1\}) : M' = \begin{pmatrix} 3 & 1 & 2 & 1 \end{pmatrix}$

-

$$\begin{aligned} Z'_1 &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid m'_{11}x_1 = 0\} \\ &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid 3x_1 = 0\} = \phi. \\ Z'_2 &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid m'_{12}x_1 = 0\} \\ &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid x_1 = 0\} = \phi. \\ Z'_3 &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid m'_{13}x_1 = 0\} \\ &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid 2x_1 = 0\} = \{2\}. \\ Z'_4 &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid m'_{14}x_1 = 0\} \\ &= \{(x_1) \in (\mathbb{Z}_4 - \{0\}) \mid x_1 = 0\} = \phi. \end{aligned}$$

Example : The first part

•

$$\begin{aligned} f(A', \{r_1\}) &= \sum_{I \subseteq \{1,2,3,4\}, |I|=1} \left| \bigcap_{j \in I} Z'_j - \bigcup_{j \notin I} Z'_j \right| \\ &= \left| Z'_1 - \bigcup_{j \in \{2,3,4\}} Z'_j \right| + \left| Z'_2 - \bigcup_{j \in \{1,3,4\}} Z'_j \right| \\ &\quad + \left| Z'_3 - \bigcup_{j \in \{1,2,4\}} Z'_j \right| + \left| Z'_4 - \bigcup_{j \in \{1,2,3\}} Z'_j \right| \\ &= 0 + 0 + 1 + 0 = 1. \end{aligned}$$

•

$$f(A', \{r_2\}) = f(A', \{r_3\}) = f(A', \{r_4\}) = 1.$$

•

$$\sum_{\{i_1\} \in LC(A', 1)} f(A', \{i_1\}) = 4.$$

Example : The second part

-

$$\begin{aligned} & \sum_{\{i_1, i_2\} \in LC(A', t)} f(A', \{i_1, i_2\}) \\ &= f(A', \{r_1, r_2\}) + f(A', \{r_1, r_3\}) + f(A', \{r_1, r_4\}) \\ &+ f(A', \{r_2, r_3\}) + f(A', \{r_2, r_4\}) + f(A', \{r_3, r_4\}). \end{aligned}$$

- $M' = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 2 & 1 & 1 & 3 \end{pmatrix}$

-

$$\begin{aligned} Z'_1 &= \{(x_1, x_2) \in (\mathbb{Z}_4 - \{0\})^2 \mid m'_{11}x_1 + m'_{21}x_2 = 0\} \\ &= \{(x_1, x_2) \in (\mathbb{Z}_4 - \{0\})^2 \mid 3x_1 + 2x_2 = 0\} \\ &= \{(2, 1), (2, 3)\} \end{aligned}$$

-

$$\begin{aligned} Z'_2 &= \{(x_1, x_2) \in (\mathbb{Z}_4 - \{0\})^2 \mid m'_{12}x_1 + m'_{22}x_2 = 0\} \\ &= \{(x_1, x_2) \in (\mathbb{Z}_4 - \{0\})^2 \mid x_1 + x_2 = 0\} \\ &= \{(1, 3), (2, 2), (3, 1)\}. \end{aligned}$$

Example : The second part

- $Z'_3 = \{(1, 2), (3, 2)\}, Z'_4 = \{(1, 1), (2, 2), (3, 3)\}$

-

$$\begin{aligned} f(A', \{r_1, r_2\}) &= \sum_{I \subseteq \{1, 2, 3, 4\}, |I|=2} \left| \bigcap_{j \in I} Z'_j - \bigcup_{j \notin I} Z'_j \right| \\ &= |Z'_1 \cap Z'_2 - Z'_3 \cup Z'_4| + |Z'_1 \cap Z'_3 - Z'_2 \cup Z'_4| \\ &\quad + |Z'_1 \cap Z'_4 - Z'_2 \cup Z'_3| + |Z'_2 \cap Z'_3 - Z'_1 \cup Z'_4| \\ &\quad + |Z'_2 \cap Z'_4 - Z'_1 \cup Z'_3| + |Z'_3 \cap Z'_4 - Z'_1 \cup Z'_2| \\ &= 0 + 0 + 0 + 0 + 1 + 0 = 1. \end{aligned}$$

-

$$\begin{aligned} f(A', \{r_1, r_3\}) &= f(A', \{r_1, r_4\}) = f(A', \{r_2, r_3\}) \\ &= f(A', \{r_2, r_4\}) = f(A', \{r_3, r_4\}) = 1. \end{aligned}$$

-

$$\sum_{\{i_1, i_2\} \in LC(A', 2)} f(A', \{i_1, i_2\}) = 6.$$

Example : The third part

- The third part calculation is similar to the first part.

-

$$\sum_{\{i_1\} \in LC(A'', 1)} f(A'', \{i_1\}) = 4.$$

- In summary, we have $A_4^2 = 4 + 6 + 4 = 14$.

References

1. W. Bosma, J. Cannon, and C. Playoust, “The Magma Algebra System I: The User Language,” *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.
2. A.R. Calderbank, N.J.A. Sloane, “Modular and p -adic Cyclic Codes,” *Designs Codes Cryptogr.* vol. 6, pp.21–35, 1995.
3. S.T. Dougherty, S.Y. Kim, Y.H. Park, “Lifted codes and their weight enumerators,” *Discr. Math.*, vol. 305, pp. 123–135, 2005.
4. P. Gaborit, C.-S. Nedeloaia, A. Wassermann, “On the Weight Enumerators of Duadic and Quadratic Residue Codes,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 402–407, 2005.

Thank you very much for your attention.