Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 215-220*

Constructive algorithm of self-dual error-correcting codes

Kiyoshi Nagata nagata@ic.daito.ac.jp
Faculty of Business Management, Daito Bunka University,
1-9-1 Takashimadaira, Itabasi-ku,Tokyo 175-8571, JAPAN

Fidel Nemenzo fidel@math.upd.edu.ph
Department of Mathematics, University of the Philippines,
Diliman, Quezon City 1101, PHILIPPINES

Hideo Wada wada@mm.sophia.ac.jp
Department of Science and Technology, Sophia University,
7-1 Kioi-cho, Chiyoda-ku, Tokyo, 102-0094, JAPAN

Abstract. In this paper, we consider self-dual codes over the finite ring $\mathbf{Z}_{p^s}$ of integer modulo p^s for any prime p and for an integer $s \geq 4$. We start with any self-dual code in lower modulo and give an necessary and sufficient condition for the self-duality of induced codes. Then we can give an inductive algorithm for construction of all self-dual codes and the mass formula in case of odd prime p.

1 Introduction

Since the discovery [4] of a relationship between non-linear binary codes and linear quaternary codes, there has been enormous interest in codes over the ring $\mathbf{Z}_m$ of integers modulo m and finite rings in general. We continue the ongoing investigations on the family of self-dual codes, from which many of the best known codes come from. By applying the Chinese Remainder Theorem [2] to self-dual codes over $\mathbf{Z}_m$, it suffices to classify codes over integers modulo prime powers.

We begin by giving the necessary definitions and notions. A *code* of length n over a finite ring R is a R-submodule of R^n. Elements of codes are called *codewords*. Two codewords $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product $\vec{x} \cdot \vec{y} = \sum_i x_i y_i$ is zero. Associated to a code $\mathcal{C}$ is a generator matrix, whose rows span $\mathcal{C}$ and the number of generators is minimal.

The *dual* $\mathcal{C}^\perp$ of a code $\mathcal{C}$ over a ring R consists of all elements of R^n which are orthogonal to every codeword in $\mathcal{C}$. A code $\mathcal{C}$ is said to be *self-dual* (resp. *self-orthogonal*) if $\mathcal{C} = \mathcal{C}^\perp$ (resp. $\mathcal{C} \subseteq \mathcal{C}^\perp$).

2 Condition for self-duality of codes over $\mathbf{Z}_{p^s}$

Every code $\mathcal{C}$ of length n over $\mathbf{Z}_{p^s}$ has a generator matrix which, after a suitable permutation of coordinates, can be written as

$$\mathcal{C} = \begin{bmatrix} T_1 \\ pT_2 \\ p^2T_3 \\ \vdots \\ p^{s-1}T_s \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{11} & A_{12} & \dots & A_{1s-1} & A_{1s} \\ 0 & pI_{k_2} & pA_{22} & \dots & pA_{2s-1} & pA_{2s} \\ 0 & 0 & p^2I_{k_3} & \dots & p^2A_{3s-1} & p^2A_{3s} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & p^{s-1}I_{k_s} & p^{s-1}A_{ss} \end{bmatrix},$$

where I_{k_i} is the $k_i \times k_i$ identity matrix, and the other matrices A_{ij}'s ($1 \le i \le j \le s$) are considered modulo p^{j-i+1}. When we denote the inverse matrix of $[T_i]_{i=1,\dots,s+1}$ with an additional $T_{s+1} = (0\ 0\ \dots\ 0\ I_{k_{s+1}})$ by $[T_i^*]^t_{i=1,\dots,s+1}$, we have $\mathcal{C}^\perp = \left[p^{i-1}T^*_{s+2-i}\right]^t_{i=1,\dots,s}$. Thus we see that a necessary and sufficient condition for the self-duality of $\mathcal{C}$ is $k_1 = k_{s+1},\ \dots\ , k_i = k_{s-i+2},\ \dots$ and $\mathcal{C}$ is self-orthogonal. And we have following proposition and lemma.

Proposition 1 *Let $\mathcal{C} = \left[p^{i-1}T_i\right]_{i=1,\dots,s}$ be a code over $\mathbf{Z}_{p^s}$ with $T_i = (0\ \dots\ 0\ I_{k_i}\ A_{ii} \dots A_{is})$. Then $\mathcal{C}$ is a self-dual code if and only if $k_i = k_{s-i+2}$ for $i = 1, \dots, s+1$ and the following holds:*

$$T_iT_j^t \equiv 0 \qquad \mod p^{s-i-j+2}, \tag{1}$$

for any integers i and j such that $1 \le i \le j \le s$ and $i + j \le s + 1$.

Lemma 1 *When the condition (1) in Proposition 2.1 holds, the rank of $k_i \times (k_1 + \dots + k_i)$ matrix $(A_{is+1-i}A_{is+2-i} \dots A_{is})$ $(1 \le i < \frac{s+1}{2})$ is equal to k_i. Especially when $i = 1$, we have that A_{1s} is invertible.*

Proof. We rewrite the condition (1) using A's, and we have two modulo p conditions $I_{k_i} \equiv -\sum_{l=i}^{s} A_{il}A_{il}^t$ and $A_{ij-1} \equiv -\sum_{l=j}^{s} A_{il}A_{jl}^t$ for $i < \frac{s+1}{2}$. By recursive substitution, we have $A_{ij-1} \equiv \sum_{l=s+1-i}^{s} A_{il}A'^t_{jl}$ $(\exists A'_{jl})$, and $I_{k_i} \equiv (A_{is+1-i}\ \dots\ A_{is})C_i^t$ $(\exists C_i)$. This completes the proof. □

3 Codes over $\mathbf{Z}_{p^s}$ from a code over $\mathbf{Z}_{p^{s-2}}$

Now we consider the code $\mathcal{C}'$ of length $n = k_1 + k_2 + \cdots + k_{s+1}$ over $\mathbf{Z}_{p^{s-2}}$ reduced from a self-dual code $\mathcal{C}$ as

$$\mathcal{C}' = \begin{bmatrix} T'_1 \\ T'_2 \\ pT'_3 \\ \vdots \\ p^{s-3}T'_{s-1} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{11} & A'_{12} & \dots & A'_{1s-2} & A'_{1s-1} & A'_{1s} \\ 0 & I_{k_2} & A_{22} & \dots & A_{2s-2} & A_{2s-1} & A'_{2s} \\ 0 & 0 & pI_{k_3} & \dots & pA_{3s-2} & pA_{3s-1} & pA'_{3s} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & p^{s-3}I_{k_{s-1}} & p^{s-3}A_{s-1s-1} & p^{s-3}A'_{s-1s} \end{bmatrix},$$

To see the self-duality condition, we substitute $s-2$ for s, $i-2$ and $j-2$ for $(3 \leq) i$ and j respectively, and $\begin{bmatrix} T_1 \\ T_2 \end{bmatrix}$ for T_1 in (1). Then we have $T_1 T_1^t \equiv 0 \mod p^{s-2}$, $T_1 T_j^t \equiv 0 \mod p^{s-j}$, and $T_i T_j^t \equiv 0 \mod p^{s-i-j+2}$ $(2 \leq i \leq j \leq s-1)$. The third conditions are the completely same as that for $\mathcal{C}$, and the first and the second conditions hold as the corresponding equations for $\mathcal{C}$ are $T_1 T_j^t \equiv 0 \pmod{p^{s-j+1}}$ for any $j \leq s$. Since we also have $k_1 + k_2 = k_{s+1} + k_s$, $k_3 = k_{s-1}, \ldots$, we see that $\mathcal{C}'$ is again self-dual.

Conversely we start with a self-dual code $\mathcal{C}'$ of length $n = k'_1 + k_3 + \ldots + k_{s-1} + k'_{s+1}$ over $\mathbf{Z}_{p^{s-2}}$. At first, we divide the part of generation vectors modulo p of dimension k'_1 into two parts of dimension k_1 and k_2, and we also divide last $k'_{s+1} (= k_s + k_{s+1} = k_1 + k_2)$ columns into two parts, like as described above. We should notice that different matrix at (1,2)-entry might induce a different code over $\mathbf{Z}_{p^s}$.

Before starting the construction of $\mathcal{C}$ over $\mathbf{Z}_{p^s}$, we need an important permutation operation. From Lemma 1, we see that $(k_s + k_{s+1})$-size square matrix $\begin{pmatrix} A'_{1s-1} & A'_{1s} \\ A_{2s-1} & A'_{2s} \end{pmatrix} \pmod p$ is invertible. So by some column permutation, we can suppose that $A'_{1s} \pmod p$ is invertible. Moreover we need to make some kind of modification by adding $k_1 \times k_i$ matrix times T'_i to T'_1 since A_{1i}s' are to be considered in mod p^i not in mod p^{i-1} in $\mathcal{C}$.

Now we denote the resulted matrices by A_{1i} $(i = 2, \ldots, s-2)$, and for such a given self-dual code $\mathcal{C}'$ over $\mathbf{Z}_{p^{s-2}}$ in the above form, we will construct the code $\mathcal{C}$ by multiplying p to $p^{i-2}T_i$ $(i = 2, \ldots, s-1)$ and adding a new $p^{s-1}T_s$ in the bottom. All A_{ij}'s except for A_{is} $(i = 1, \ldots, s-1)$ and A_{1s-1} are considered in the same modulo as in $\mathcal{C}'$. For any i, A_{is} is defined modulo p^{s-i+1} and A_{1s-1} is modulo p^{s-1}. Since A'_{is} is defined modulo p^{s-i} for $i \geq 2$, A'_{1s} is modulo p^{s-2}, and A'_{1s-1} is modulo p^{s-2} in $\mathcal{C}'$, we need following extension

$$T_1 = T'_1 + p^{s-2}U_1 + p^{s-1}V \quad \text{and} \quad T_i = T'_i + p^{s-i}U_i \ (2 \leq i \leq s-1) \tag{2}$$

where $U_1 = (0 \ \ldots \ A^{(1)}_{1s-1} \ A^{(1)}_{1s})$, $V = (0 \ \ldots \ 0 \ A^{(2)}_{1s})$, $U_i = (0 \ \ldots \ 0 \ A^{(1)}_{is})$ $(i = 2, \ldots, s-1)$ for some modulo p matrices $A^{(1)}$'s and $A^{(2)}$.

We have remaining two types of conditions in (1) for the self-duality of $\mathcal{C}'$. One is $T_1T_i^t \equiv 0 \mod p^{s-i+1}$ under the codition $T_1'T_i'^t \equiv 0 \mod p^{s-i}$ for $2 \le i$, which becomes $T_1'T_i'^t + p^{s-2}U_1T_i'^t + p^{s-i}T_1'U_i^t \equiv 0 \mod p^{s-i+1}$ by substituting the right-hand sides of (2) and taking the assumption that $4 \le s$ and $2s-i-2 = s-i+1+(s-3)$ in mind. If $3 \le i$, then $s-i+1 \le s-2$ and the equation is $T_1'T_i'^t + p^{s-i}A_{1s}A_{is}^{(1)t} \equiv 0 \mod p^{s-i+1}$, and we have $A_{is}^{(1)t}$ $(3 \le i)$ is uniquely determined as $A_{is}^{(1)t} \equiv -A_{1s}^{-1}\left(\frac{1}{p^{s-i}}T_1'T_i'^t\right) \mod p$. If $i = s$, then $A_{ss}^t \equiv -A_{1s}^{-1}A_{1s-1} \mod p$. If $i = 2$, then $T_1'T_2'^t + p^{s-2}(A_{1s-1}^{(1)}A_{2s-1}^t + A_{1s}^{(1)}A_{2s}^t + A_{1s}A_{2s}^{(1)t}) \equiv 0 \mod p^{s-1}$. Thus we have that $A_{2s}^{(1)t}$ is also uniquely determined as $A_{2s}^{(1)t} \equiv -A_{1s}^{-1}\left(\frac{1}{p^{s-2}}T_1'T_2'^t + A_{1s-1}^{(1)}A_{2s-1}^t + A_{1s}^{(1)}A_{2s}^t\right) \mod p$ for any $A_{1s-1}^{(1)}$ and $A_{1s}^{(1)}$. The other condition can be rewritten as $0 \equiv T_1'T_1'^t + p^{s-2}\widetilde{T_1'U_1^t} + p^{s-1}\widetilde{T_1'V^t} \mod p^s$, with $\widetilde{X} = X + X^t$. This includes the condition for $A_{1s-1}^{(1)}$ and $A_{1s}^{(1)}$, and using them we have following essential condition

$$T_1'T_1'^t + p^{s-2}(\widetilde{A_{1s-1}A_{1s-1}^{(1)t}} + \widetilde{A_{1s}A_{1s}^{(1)t}}) + p^{s-1}\widetilde{A_{1s}A_{1s}^{(2)t}} \equiv 0 \mod p^s. \quad (3)$$

From now on, we consider the equation above only in odd p case. $\widetilde{A_{1s}A_{1s}^{(1)t}} \equiv -\left(\frac{1}{p^{s-2}}T_1'T_1'^t + \widetilde{A_{1s-1}A_{1s-1}^{(1)t}}\right) \mod p$ is given by reducing (3) modulo p^{s-1}. We put $(x_{ij}) = A_{1s}A_{1s}^{(1)t}$ and put (d_{ij}) the right-hand side of the equation for any $k_1 \times k_2$ matrix $A_{1s-1}^{(1)}$. Then the necessary and sufficient condition for x_{ij} are $x_{ji} = d_{ij} - x_{ij} \mod p$ $(i < j)$, and $x_{ii} = \frac{1}{2}d_{ii}$. For any $p^{\frac{1}{2}k_1(k_1-1)}$ number of (x_{ij}) satisfying above, $A_{1s}^{(1)t}$ is uniquely detemined by $A_{1s}^{-1}(x_{ij}) \pmod p$. Once $A_{1s}^{(1)t}$ is determined, the condition (3) is just equivalent to $\widetilde{A_{1s}A_{1s}^{(2)t}} \equiv -\frac{1}{p}\left(\frac{1}{p^{s-2}}T_1'T_1'^t + \widetilde{A_{1s-1}A_{1s-1}^{(1)t}} + \widetilde{A_{1s}A_{1s}^{(1)t}}\right) \mod p$. We also put $(y_{ij}) = A_{1s}A_{1s}^{(2)t}$ and put (f_{ij}) the right-hand side of the equation. Then the necessary and sufficient condition for y_{ij} are $y_{ji} = f_{ij} - y_{ij} \mod p$ $(i < j)$, and $y_{ii} = \frac{1}{2}f_{ii}$. For any $p^{\frac{1}{2}k_1(k_1-1)}$ number of (y_{ij}) satisfying this, $A_{1s}^{(2)t}$ is uniquely detemined by $A_{1s}^{-1}(y_{ij}) \pmod p$. Thus we have self-dual codes over $\mathbf{Z}_{p^s}$ and the following lemma.

Lemma 2 *The number of self-dual codes over $\mathbf{Z}_{p^s}$ of type $(k_1, k_2, \ldots, k_{s+1})$ induced from a self-dual code over $\mathbf{Z}_{p^{s-2}}$ of type $(k_1+k_2, k_3, \ldots, k_s+k_{s+1})$ is*

$$\rho(k_1+k_2, k_1) \times p^{k_1\sum_{i=3}^{s-1}k_i} \times p^{k_1k_2+k_1(k_1-1)} = \rho(k_1+k_2, k_1)p^{k_1(n-k_1-k_2-1)},$$

where $\rho(n,k) = \prod_{j=1}^{k}(p^n - p^{j-1})/\prod_{j=1}^{k}(p^k - p^{j-1})$, the number of subspace of dimension k of a vector space over $\mathbf{F}_p = \mathbf{Z}_p$ of dimension n.

Proof. The number of possible partitions $\begin{bmatrix} T'_1 \\ T'_2 \end{bmatrix}$ in $\mathcal{C}'$ is given by considering the map $\mathcal{C}' \xrightarrow{p^{s-1}} p^{s-1}\mathcal{C}' \to 0$. The kernel is $< pT'_1, pT'_2, pT'_3, ..., p^{s-3}T'_{s-1} >$ and noticing that the submodule is to be considered in $< T'_1, pT'_2, p^2T'_3, ..., p^{s-1}T'_s >$, we should count the multiple of the number of partitions in the vector space $p^{s-1}\mathcal{C}'$ and a kind of modifications of T'_1 by T'_3,..., T'_{s-1}. The number of partitions in the vector space is just $\rho(k_1 + k_2, k_1)$ from the lemma3.2 in [5]. As the modifications are done by adding any $k_1 \times k_i$ matrix times T'_i to T'_1, the number of such modification is just equal to $p^{k_1 \times k_3} \times p^{k_1 \times k_4} \times \cdots \times p^{k_1 \times k_{s-1}} = p^{k_1 \sum_{i=3}^{s-1} k_i} = p^{k_1(n-2(k_1+k_2))}$. □

When we calculate the product of $\rho(n_i, k_i)$, we have following lemma.

Lemma 3

$$\prod_{i=1}^{m} \rho(n_i, k_i) = \frac{\prod_{i=1}^{n_m}(p^i - 1)}{\prod_{i=1}^{m}\prod_{j=1}^{k_i}(p^j - 1)}, \quad \textit{with } n_i = k_1 + \cdots + k_i \quad (i = 1, ..., m).$$

Now we have the following formulae.

Theorem 1 *Let $N_{p^s}(n; k_1, ..., k_{s+1})$ be the number of self-dual codes over $\mathbf{Z}_{p^s}$ of type $(k_1, ..., k_{s+1})$ for an odd prime p and for an integer s $(1 < s)$. And put $n_i = k_1 + \cdots + k_i$ for $i = 1, ..., \left[\frac{s+1}{2}\right]$, and put $m_u = \sum_{i=1}^{u} n_i(n - n_{i+1} - 1)$.*

1. *If $s(= 2u)$ even, then*

$$N_{p^s}(n; k_1, ..., k_{s+1}) = D_{n,n_u} \frac{\prod_{i=1}^{n_u-1}(p^{n-2i-\delta} - 1)}{\prod_{i=1}^{u}\prod_{j=1}^{k_i}(p^j - 1)} \cdot p^{m_u - \frac{1}{2}n_u(n_u-1)},$$

where $D_{n,n_u} = \left(p^{\frac{n}{2}-n_u} + \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right)\left(p^{\frac{n}{2}} - \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right)$ and $\delta = 0$ if n is even, and $D_{n,n_u} = \delta = 1$ if n is odd.

2. *If $s(= 2u + 1)$ odd, then n must be even and*

$$N_{p^s}(n; k_1, ..., k_{s+1}) = \left(1 + \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right) \prod_{i=1}^{\frac{n}{2}-1}(p^i + 1) \frac{\prod_{i=0}^{n_u-1}(p^{n-i} - 1)}{\prod_{i=1}^{u}\prod_{j=1}^{k_i}(p^j - 1)} \cdot p^{m_u}.$$

Proof. ¿From the lemma 2 and the lemma 3,

$$N_{p^s}(n; k_1, ..., k_{s+1}) = N_{p^{s-2}}(n; n_2, k_3, ..., k_{s-1}, n_2)\rho(n_2, k_2)p^{n_1(n-n_2-1)}$$

$$= \begin{cases} N_{p^2}(n; n_u, k_{u+1}, n_u) \dfrac{\prod_{i=1}^{n_u}(p^i - 1)}{\prod_{i=1}^{u}\prod_{j=1}^{k_i}(p^j - 1)} \cdot p^{m_{u-1}} & \text{(if s is even)} \\ N_{p^3}(n; n_u, k_{u+1}, k_{u+1}, n_u) \dfrac{\prod_{i=1}^{n_u}(p^i - 1)}{\prod_{i=1}^{u}\prod_{j=1}^{k_i}(p^j - 1)} \cdot p^{m_{u-1}} & \text{(if s is odd)} \end{cases}.$$

If s is even, then from Theorem 3.5 in [1]

$$N_{p^2}(n; n_u, k_{u+1}, n_u) = D_{n,n_u} \frac{\prod_{i=1}^{n_u-1}(p^{n-2i-\delta}-1)}{\prod_{i=1}^{n_u}(p^i-1)} p^{\frac{1}{2}n_u(n_u-1)},$$

and we have the resulted formula. If s is odd, then from Theorem 4.1 in [5]

$$\begin{aligned} & N_{p^3}(n; n_u, k_{u+1}, k_{u+1}, n_u) \\ = & \left(1 + \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right) \prod_{i=1}^{\frac{n}{2}-1} (p^{\frac{n}{2}-i}+1) \frac{\prod_{i=0}^{n_u-1}(p^{n-i}-1)}{\prod_{i=1}^{n_u}(p^i-1)} \cdot p^{n_u(n-n_{u+1}-1)}, \end{aligned}$$

and we have the resulted formula. □

4 Conclusions

We suceeded to give a formula for the number of self-dual codes of a given type for an odd prime p and for any integers $s \geq 4$. In order to obtain the mass formula for the self-dual codes of length n, we have only to add up the formulae in theorem 1. Since we already have the mass formula for each $\mathbf{Z}_p$, $\mathbf{Z}_{p^2}$, and $\mathbf{Z}_{p^3}$ [1, 3, 5], the mass formula problem for any odd prime is completely solved.

In case of $p = 2$, Gaborit [3] had the two types of mass formula for the doubly even binary code and for type II quarternary code. Our construction algorithm is similarly applied to this case, but somehow complicated because we need douby even property. We are now under investigating the mass formula for codes over $\mathbf{Z}_{2^s}$.

References

[1] Balmaceda, J., Betty, R., and Nemenzo, F. Mass formula for self-dual codes over $\mathbf{Z}_{p^2}$, *Discrete Mathematics* (to appear).

[2] Dougherty, S., Harada, H., and Solé, P. Self-dual codes over rings and the Chinese remainder theorem, *Hokkaido Math. J.* 28, 1999, 253-283.

[3] Gaborit, P. Mass formulas for self-dual codes over $\mathbf{Z}_4$ and $\mathbf{F}_q + u\mathbf{F}_q$ rings, *IEEE Trans. Inform. Theory* 42, 1996, 1222-1228.

[4] Hammons, A., Kumar, P., Calderbank, A., Sloane, N., and Solé, P. The $\mathbf{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* 40, 1994, 301-319.

[5] Nagata, K., Nemenzo, F., and Wada, H. The number of self-dual codes over $\mathbf{Z}_{p^3}$, (under review)