Note on the Type II codes of length 24

S. Nagaoka and M. Oura

Abstract

We express the weight enumerators of self-dual and doubly even (Type II for short) codes of length 24 with a specified basis. As a consequence, we present some congruence relations among the weight enumerators.

Keywords: code, weight enumerator.
2020MSC: Primary 95B05, Secondary 05E15.

1 Introduction

The main theme of this paper is the weight enumerators of Type II codes of length 24. We shall briefly describe the properties of the weight enumerators and the relationship between coding theory and number theory. The weight enumerators of Type II codes carry the invariance properties under the action of a finite group. In fact, the invariant ring over $\mathbf{C}$ under the action of the unitary reflection group of order 192 can be generated by the weight enumerator of Type II codes [7]. This theorem is generalized in [15, 10]. If we substitute certain theta functions into the weight enumerators of Type II codes, we can get Siegel modular forms [3, 14]. This modular form can be also obtained as follows. For a Type II code $C \subset \mathbf{F}_2^n$, we construct an even unimodular lattice $\frac{1}{\sqrt{2}}\rho^{-1}(C)$ where $\rho : \mathbf{Z}^n \to (\mathbf{Z}/2\mathbf{Z})^n = \mathbf{F}_2^n$ [5]. This correspondence between codes and lattices serves to be of great importance for the development each other. Anyway, the theta function of the lattice $\frac{1}{\sqrt{2}}\rho^{-1}(C)$ is the same as the modular form obtained from the weight enumerator of the code C.

In the paper [8], they studied the theta series of even unimodular lattices of length 24. Among other results, they show that for an even unimodular lattice $\mathcal{L}$ with Coxeter number h, it holds

$$\begin{aligned}\vartheta_{\mathcal{L}}^{(3)} = (E_4^{(3)})^3 + 24(h-30)Y_{12}^{(3)} + 48(h-30)^2 X_{12}^{(3)} \\ +24(h-30)(2h^2+48h+1571)F_{12}\end{aligned}$$

where $E_4^{(3)}, Y_{12}^{(3)}, X_{12}^{(3)}$ are suitable Siegel modular forms in genus 3 with integral Fourier coefficients and F_{12} is Miyawaki's cusp form of weight 12. In particular F_{12} vanishes under the action of Siegel's Phi operator. The purpose of this note is to give the similar results in coding theory. There exist 9 Type II codes of length 24 up to equivalence, denoted by C_i $(i = 1, 2, \ldots, 9)$. We can attach the number h_i for C_i as in the case of lattices. We show, for $i = 1, 2, \ldots, 9$,

$$W_{C_i}^{(2)} = W_{C_9}^{(2)} + 6(4h_i - 7)X_{24} + 24(2h_i + 3)(4h_i - 7)Y_{24}$$

where $X_{24},\ Y_{24}$ are linear combinations of the weight enumerators in genus 2 and $\Phi(X_{24}) = x^4y^4(x^4-y^4)^4,\ \Phi(Y_{24}) = 0$. The Φ applying to polynomials corresponds to Siegel's Phi operator.

2 Preliminaries

Let $\mathbf{F}_2 = \{0,1\}$ be the field of two elements. We sometimes regard it as $\mathbf{F}_2 \subset \mathbf{Z}$. The vector space $\mathbf{F}_2^n$ is equipped with the inner product

$$u \cdot v = u_1v_1 + \cdots + u_nv_n$$

for $u = (u_1,\ldots,u_n),\ v = (v_1,\ldots,v_n) \in \mathbf{F}_2^n$. The weight $wt(u)$ of $u \in \mathbf{F}_2^n$ is the number of non-zero coordinates of u. A subspace C of $\mathbf{F}_2^n$ is called a (linear) code of length n. The dual code of C is defined by

$$C^\perp = \{u \in \mathbf{F}_2^n :\ u \cdot v = 0,\ \forall v \in C\}.$$

If $C = C^\perp$, then C is said to be self-dual. If $wt(u)$ is a multiple of 4 for all $u \in C$, then C is said to be doubly even. In this note, we deal with the self-dual and doubly even codes. We call them Type II codes for short.

We give some codes with generator matrices (i.e., rows generate each code). We put

$$d_n : \begin{pmatrix} 111100 & \ldots & 0000 \\ 001111 & \ldots & 0000 \\ & \ddots & \\ 000000 & \ldots & 1111 \end{pmatrix}$$

for $n = 4,6,8,\ldots$, and

$$e_7 : \begin{pmatrix} 0111100 \\ 0110011 \\ 1101010 \end{pmatrix},$$

$$e_8 : \begin{pmatrix} 11110000 \\ 00111100 \\ 00001111 \\ 10101010 \end{pmatrix}.$$

We denote by g_{24} the binary Golay code of length 24. The code g_{24} is a unique Type II code of length 24 which contains no element of weight 4, see [5].

It is known that a Type II code of length n exists if and only if $n \equiv 0 \pmod 8$. Two codes are said to be equivalent if one can be obtained from the other by permuting coordinates. Under this equivalence, classification of Type II codes is completed up to $n = 40$, see [12, 13, 4, 1]. Type II codes of length 24 are presented at Table 1. The 7th code in that table is the binary Golay code g_{24}.

For a code C, the weight enumerator of C in genus g is defined by

$$W_C^{(g)}(x_a :\ a \in \mathbf{F}_2^g) = \sum_{u_1,\ldots,u_g \in C} \prod_{a \in \mathbf{F}_2^g} x_a^{n_a(u_1,\ldots,u_g)}$$

Table 1: Classification of Type II codes of length 24.

i	1	2	3	4	5	6	7	8	9
Components	d_{12}^2	$d_{10}e_7^2$	d_8^3	d_6^4	d_{24}	d_4^6	g_{24}	$d_{16}e_8$	e_8^3
h_i	$\frac{5}{4}$	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{11}{4}$	$\frac{1}{4}$	0	$\frac{7}{4}$	$\frac{7}{4}$

where $n_a(u_1, \ldots, u_g) = \sharp\{i : a = (u_{1i}, u_{2i}, \ldots, u_{gi})\}$. In genus 1, we may use x, y instead of x_0, x_1. If C is of length n, we have the usual weight enumerator

$$W_C^{(1)}(x, y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)}.$$

The number h_i is obtained as the number of elements of weight 4 of each component divided by the dimension. This number can be read off from the weight enumerator given below, that is, a coefficient of $x^{n-4}y^4$ divided by n.

In the following, we may write $W_C^{(g)}$ for simplicity. For codes C and C', we have $W_{C \oplus C'}^{(g)} = W_C^{(g)} W_{C'}^{(g)}$.

For a column vector $a \in \mathbf{F}_2^g$, we define a map

$$\Phi : \mathbf{C}[x_a \in \mathbf{F}_2^g] \to \mathbf{C}[x_{a'} : a' \in \mathbf{F}_2^{g-1}]$$
$$x_a \mapsto \begin{cases} x_{a'} & \text{if } a = \begin{pmatrix} a' \\ 0 \end{pmatrix}, \\ 0 & \text{if } a = \begin{pmatrix} a' \\ 1 \end{pmatrix}. \end{cases}$$

It holds $\Phi(W_C^{(g)}) = W_C^{(g-1)}$ (*cf.* [15, 9]).

It is known that the ring generated over $\mathbf{C}$ by the weight enumerators of Type II codes in genus g coincides with the invariant ring of some finite group, see [7, 6, 15]. In particular, a basis of the vector space generated over $\mathbf{C}$ by the weight enumerators of Type II code of length 24 in $g = 1, 2$ is

$$W_{C_9}^{(1)}, W_{C_7}^{(1)}$$

and

$$W_{C_9}^{(2)}, W_{C_7}^{(2)}, W_{C_5}^{(2)}.$$

For completeness, we add here the weight enumerators in genus 1.

$$\begin{aligned}
W_{d_4}^{(1)} &= x^4 + y^4, \\
W_{d_6}^{(1)} &= x^6 + 3x^2y^4, \\
W_{e_7}^{(1)} &= x^7 + 7x^3y^4, \\
W_{d_8}^{(1)} &= x^8 + 6x^4y^4 + y^8, \\
W_{e_8}^{(1)} &= x^8 + 14x^4y^4 + y^8, \\
W_{d_{10}}^{(1)} &= x^{10} + 10x^6y^4 + 5x^2y^8,
\end{aligned}$$

$$W^{(1)}_{d_{12}} = x^{12} + 15x^8y^4 + 15x^4y^8 + y^{12},$$
$$W^{(1)}_{d_{16}} = x^{16} + 28x^{12}y^4 + 70x^8y^8 + 28x^4y^{12} + y^{16},$$
$$W^{(1)}_{d_{24}} = x^{24} + 66x^{20}y^4 + 495x^{16}y^8 + 924x^{12}y^{12} + 495x^8y^{16} + 66x^4y^{20} + y^{24}.$$

The coefficient of $x^{n-4}y^4$ is the number of elements of weight 4 and each component of a Type II code of length 24 has the same number, that is, nh_i. For the Type II codes of length 24, we mention

$$W^{(1)}_{C_5} = x^{24} + 66x^{20}y^4 + 495x^{16}y^8 + 2972x^{12}y^{12} + 495x^8y^{16} + 66x^4y^{20} + y^{24},$$
$$W^{(1)}_{C_7} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

and

$$W^{(1)}_{C_5} = \frac{11}{7}W^{(1)}_{C_9} - \frac{4}{7}W^{(1)}_{C_7}.$$

3 Results

We start with the case $g = 1$. Let $\Delta = x^4y^4(x^4 - y^4)^4$. The vector space of the weight numerators of Type II codes in genus 1 is spanned by $W^{(1)}_{C_9}$ and Δ. By direct calculation, we get the following identity: For $i = 1, 2, \ldots, 9$, we have

$$W^{(1)}_{C_i} = W^{(1)}_{C_9} + 6(4h_i - 7)\Delta.$$

Using this, we obtain

Proposition 1 (1) *Let i and j be distinct integers in $1, 2, \ldots, 8$. If $4h_i \equiv 4h_j \pmod{m}$ for an integer m, then*

$$W^{(1)}_{C_i} \equiv W^{(1)}_{C_j} \pmod{6m}.$$

(2) *Let C_α, C_β be Type II codes of length 24 with $h_\alpha < h_\beta$. Then we have*

$$W^{(1)}_{C_i} = \frac{h_i - h_\beta}{h_\alpha - h_\beta}W^{(1)}_{C_\alpha} + \frac{h_i - h_\alpha}{h_\beta - h_\alpha}W^{(1)}_{C_\beta}$$

for $i = 1, 2, \ldots, 9$.

Proof. We need only to prove (2). Set

$$W^{(1)}_{C_i} = aW^{(1)}_{C_\alpha} + bW^{(1)}_{C_\beta}.$$

Applying (1), we get a system of equations

$$\begin{cases} a + b = 1, \\ 6(4h_\alpha - 7)a + 6(4h_\beta - 7)b = 6(4h_i - 7). \end{cases}$$

Since the determinant of the matrix $\begin{pmatrix} 1 & 1 \\ 6(4h_\alpha - 7) & 6(4h_\beta - 7) \end{pmatrix}$ is $-24(h_\alpha - h_\beta) \neq 0$, we get a and b. This completes the proof of Proposition 1.

Table 2: Possible m in (1) of Proposition 1.

	h_2	h_3	h_4	h_5	h_6	h_7	h_8
h_1	1	2	3	6	4	5	2
h_2		1	2	7	3	4	3
h_3			1	8	2	3	4
h_4				9	1	2	5
h_5					10	11	4
h_6						1	6
h_7							7

We add a few words on (1) of Proposition 1. For $i < j$, we denote by m the number presented at the (h_i, h_j)-entry in Table 2. Then (1) of Proposition 1 says that $(W_{C_i}^{(1)} - W_{C_j}^{(1)})/6m$ is in $\mathbf{Z}[x, y]$. One can say more. By direct calculation, we observe that the resulting $(W_{C_i}^{(1)} - W_{C_j}^{(1)})/6m$ contains a monomial with coefficient 1 or -1.

We consider the case $g = 2$. The vector space of the weight enumerators of Type II codes of length 24 in genus 2 is spanned by $W_{C_9}^{(2)}, W_{C_7}^{(2)}, W_{C_5}^{(2)}$. Let

$$F = aW_{C_9}^{(2)} + bW_{C_7}^{(2)} + cW_{C_5}^{(2)}.$$

Now we consider the action of Φ on F. In order to make our discussion smooth, we set

$$\begin{aligned} X &= \frac{1}{42}\left(W_{C_9}^{(2)} - W_{C_7}^{(2)}\right), \\ Y &= -\frac{11}{7}W_{C_9}^{(2)} + \frac{4}{7}W_{C_7}^{(2)} + W_{C_5}^{(2)}. \end{aligned}$$

Since $\Phi(W_C^{(g)}) = W_C^{(g-1)}$, we have

$$\begin{aligned} \Phi(F) &= aW_{C_9}^{(1)} + bW_{C_7}^{(1)} + cW_{C_5}^{(1)} \\ &= aW_{C_9}^{(1)} + bW_{C_7}^{(1)} + c\left(\frac{11}{7}W_{C_9}^{(1)} - \frac{4}{7}W_{C_7}^{(1)}\right) \\ &= \left(a + \frac{11}{7}c\right)W_{C_9}^{(1)} + \left(b - \frac{4}{7}c\right)W_{C_7}^{(1)}. \end{aligned}$$

Then

$$\begin{aligned} \Phi(F) = 0 &\Leftrightarrow a + \frac{11}{7}c = b - \frac{4}{7}c = 0 \\ &\Leftrightarrow a = -\frac{11}{7}c, b = \frac{4}{7}c \\ &\Leftrightarrow F = cY. \end{aligned}$$

Also

$$\begin{aligned}\Phi(F)=x^4y^4(x^4-y^4)^4 &\Leftrightarrow a+\frac{11}{7}c=\frac{1}{42}, b-\frac{4}{7}c=-\frac{1}{42}\\ &\Leftrightarrow a=\frac{1}{42}-\frac{11}{7}c, b=-\frac{1}{42}+\frac{4}{7}c\\ &\Leftrightarrow F=X+cY.\end{aligned}$$

We have thus obtained the following proposition.

Proposition 2 (1) $\Phi(F)=0$ *if and only if* $F=cY$ *for some constant* c.

(2) $\Phi(F)=\Delta$ *if and only if* $F=X+cY$ *for some constant* c.

We introduce the following polynomials of $\mathbf{Z}[x_a : a\in \mathbf{F}_2^2]$ from [11]:

$$\begin{aligned}X_{24}&=X-\frac{1}{44}Y,\\ Y_{24}&=\frac{1}{2^4 3\cdot 11}Y.\end{aligned}$$

Polynomials W_{C_9}, X_{24}, Y_{24} form a basis of the vector space of the weight enumerators of Type II codes of length 24. By Proposition 2, we have

$$\begin{aligned}\Phi(X_{24})&=\Phi(X)-\frac{1}{44}\Phi(Y)\\ &=\Delta\end{aligned}$$

and

$$\begin{aligned}\Phi(Y_{24})&=\frac{1}{2^4 3\cdot 11}\Phi(Y)\\ &=0.\end{aligned}$$

The coefficient $c(h_i)$ of Y_{24} in

$$W_{C_i}=W_{C_9}^{(2)}+6(4h_i-7)X_{24}+c(h_i)Y_{24}$$

can be obtained by direct calculation. Therefore we have the following theorem corresponding to that of theta series in [8] mentioned in Introduction.

Theorem 3 (1) $\Phi(X_{24})=\Delta$ *and* $\Phi(Y_{24})=0$.

(2) *For* $i=1,2,\ldots,9$, *we have*

$$W_{C_i}^{(2)}=W_{C_9}^{(2)}+6(4h_i-7)X_{24}+24(2h_i+3)(4h_i-7)Y_{24}.$$

Corollary 4 *Let* i *and* j *be distinct integers in* $1,2,\ldots,8$. *If* $4h_i\equiv 4h_j \pmod m$ *for an integer* m, *then*

$$W_{C_i}^{(2)}\equiv W_{C_j}^{(2)} \pmod{6m}.$$

In order to state the next corollary, we introduce the Lagrange polynomial $\ell_\epsilon(x)$. For $\epsilon\in\{\alpha,\beta,\gamma\}$, we set

$$\ell_\epsilon(x)=\prod_{\substack{\mu\in\{\alpha,\beta,\gamma\}\\ \mu\neq\epsilon}}\frac{x-x_\mu}{x_\epsilon-x_\mu}.$$

Corollary 5 *Let $C_\alpha, C_\beta, C_\gamma$ be Type II codes of length 24 with $h_\alpha < h_\beta < h_\gamma$. Then for $i = 1, 2, \ldots, 9$, the weight enumerator $W^{(2)}_{C_i}$ has the following expression:*

$$W^{(2)}_{C_i} = \ell_\alpha(h_i) W^{(2)}_{C_\alpha} + \ell_\beta(h_i) W^{(2)}_{C_\beta} + \ell_\gamma(h_i) W^{(2)}_{C_\gamma}.$$

Proof. We set

$$W^{(2)}_{C_i} = aW^{(2)}_{C_\alpha} + bW^{(2)}_{C_\beta} + cW^{(2)}_{C_\gamma}.$$

We apply the expression in Theorem 3 to each $W^{(2)}_{C_\alpha}, W^{(2)}_{C_\beta}, W^{(2)}_{C_\gamma}$, we get a system of equations

$$A \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ c_0(h_i) \\ c_1(h_i) \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1 & 1 & 1 \\ c_0(h_\alpha) & c_0(h_\beta) & c_0(h_\gamma) \\ c_1(h_\alpha) & c_1(h_\beta) & c_1(h_\gamma) \end{pmatrix}$$

and

$$\begin{aligned} c_0(h) &= 6(4h-7), \\ c_1(h) &= 24(2h+3)(4h-7). \end{aligned}$$

Since $\det A = -4608(h_\alpha - h_\beta)(h_\alpha - h_\gamma)(h_\beta - h_\gamma) \neq 0$, we can solve the system of equations and get the result. This completes the proof of Corollary 5.

There are two classes of Type II codes of length 16. A remark is that their weight enumerators are distinct in $g = 3$. This remark is important in number theory and we only mention a reference [14]. Inequality of the mentioned weight enumerators in $g = 3$ leads to $W^{(3)}_{C_8} \neq W^{(3)}_{C_9}$. Combining this with $h_8 = h_9$, we see that Theorem 3 (2) can not be extended to the case $g = 3$.

Acknowledgment. Calculations are done with the help of Maple and Magma [2]. We thank T. Chaochanglek and A. Munemasa for comments to this manuscript. The first named author is supported by JSPS KAKENHI Grant Number 20K03547.

References

[1] Betsumiya, K., Harada, M., Munemasa, A., A complete classification of doubly even self-dual codes of length 40, Electron. J. Combin. 19 (2012), no. 3, Paper 18, 12 pp.

[2] W. Bosma, J. Cannon, C. Playoust: The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3-4, 235-265.

[3] Broué, M., Enguehard, M., Polynômes des poids de certains codes et fonctions thêta de certains réseaux. Ann. Sci. École Norm. Sup. (4)5(1972), 157-181.

[4] Conway, J. H., Pless, V., Sloane, N. J. A., The binary self-dual codes of length up to 32: a revised enumeration, J. Combin. Theory Ser. A 60 (1992), no. 2, 183-195.

[5] Conway, J. H., Sloane, N. J. A., Sphere packings, lattices and groups. Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov Grundlehren Math. Wiss., 290, Springer-Verlag, New York, 1999.

[6] Duke, W., On codes and Siegel modular forms. Internat. Math. Res. Notices 1993, no. 5, 125-136.

[7] Gleason, A. M., Weight polynomials of self-dual codes and the MacWilliams identities, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, pp. 211-215. Gauthier-Villars, Paris, 1971.

[8] Nagaoka, S., Takemori, S., Notes on theta series for Niemeier lattices, Ramanujan J. 42 (2017), no. 2, 385-400.

[9] Nebe, G., Kneser-Hecke-operators in coding theory, Abh. Math. Sem. Univ. Hamburg 76 (2006), 79-90.

[10] Nebe, G., Rains, E., Sloane, N. J. A., Self-dual codes and invariant theory. Algorithms Comput. Math., 17 Springer-Verlag, Berlin, 2006.

[11] Oura, M., On the integral ring spanned by genus two weight enumerators, Discrete Math. 308(2008), 3722-3725.

[12] Pless, V., A classification of self-orthogonal codes over GF(2), Discrete Math. 3 (1972), 209-246.

[13] Pless, V., Sloane, N. J. A., On the classification and enumeration of self-dual codes, J. Combinatorial Theory Ser. A 18 (1975), 313-335.

[14] Runge, B., On Siegel modular forms. I, J. Reine Angew. Math. 436 (1993), 57-85.

[15] Runge, B., Codes and Siegel modular forms, Discrete Math. 148 (1996), no. 1-3, 175-204.

Shoyu Nagaoka
Yamato University, Japan
Emeritus Professor, Kindai University, Japan
shoyu1122.sn@gmail.com

Manabu Oura
Kanazawa University, Japan
oura@se.kanazawa-u.ac.jp