The dimension formula for the ring of code polynomials in genus 5

By *Manabu Oura*

The purpose of this paper is to study the dimension formula of the invariant ring of the specified group H_5. This ring appears in the theory of Siegel modular forms and in coding theory. As an application of our dimension formula we give another proof of the fact the associated g-th weight enumerators of the 9 self-dual doubly-even codes of length 24 are linearly independent if and only if $g \geq 6$, which is proved in a recent paper by Oura-Poor-Yuen.

Introduction

Let $\mathbf{F}_2 = \{0, 1\}$ be the field of two elements. We will assume the order of elements of $\mathbf{F}_2^g$ is $(0, \cdots, 0, 0), (0, \cdots, 0, 1), (0, \cdots, 1, 0), \cdots, (1, \cdots, 1, 1)$ when we need.

Define 2^g variables F_a for $a \in \mathbf{F}_2^g$. Let $\mathbf{C}[F_a : a \in \mathbf{F}_2^g]$ be the polynomial ring in these variables. The finite subgroup H_g, which we shall define in the next section, of $GL(2^g, \mathbf{C})$ naturally acts on this polynomial ring. Let R_g be the H_g-invariant subring of $\mathbf{C}[F_a : a \in \mathbf{F}_2^g]$ and R_g^m be the vector space of H_g-invariant polynomials of homogeneous degree m. Runge [13] proved that the ring of Siegel modular forms of even weight for $\Gamma_g = Sp(2g, \mathbf{Z})$ is the normalization of the quotient ring of R_g by an ideal of "theta relations" in its field of fractions. We, however, do not go into details of the theory of Siegel modular forms. Besides the space $R_g^m, m \equiv 0 \pmod 8$, is closely connected to coding theory which we shall discuss next.

Let C be a self-dual doubly-even code of length m, i.e. a linear subspace of $\mathbf{F}_2^n$ with the inner product $a \cdot b = \sum a_i b_i$, such that C coincides with its dual and such that the number of non-zero coordinates of every element of C is congruent to $0 \pmod 4$. It is known that a self-dual doubly-even codes of length m exists if and only if the length m is multiple of 8. Two codes are said to be equivalent if one of them coincides with another by a permutation of coordinate positions. The non-equivalent self-dual doubly-even codes are classified upto $m = 32$. The numbers of them are

$$1(m = 8),\ 2(m = 16),\ 9(m = 24),\ 85(m = 32).$$

In this paper we are mainly interested in the case where $m = 24$ and they are denoted by

$$d_{12}^2, d_{10}e_7^2, d_8^3, d_6^4, d_{24}, d_4^6, g_{24}, d_{16}e_8, e_8^3.$$

In particular g_{24} is the extended Golay code of length 24. We refer to [5] for a detailed description of coding theory.

The g-th weight enumerators of a code C is

$$W_C^{(g)}(F) = \sum_{x \in C^g} \prod_{i=1}^{m} F_{\mathrm{row}_i(x)}.$$

We write W_C unless the dependence on g is noteworthy. The problem we are interested in is when the g-th weight enumerators of all self-dual doubly-even codes of the fixed length m are linearly independent. Since equivalent codes have the same weight enumerator, we have only to deal with non-equivalent codes. The first non-trivial case is $m = 16$. Duke [1] and Runge [13] noticed that the g-th weight enumerators of the 2 self-dual doubly-even codes of length 16 are linearly independent if and only if $g \geq 3$. The next case where $m = 24$ is treated in [12]. Actually it is proved that the g-th weight enumerators of the 9 self-dual doubly-even codes of length 24 are linearly independent if and only if $g \geq 6$. We give another proof of this theorem in this paper.

The theorem of Runge [15] says that the space $R_g^m, m \equiv 0 \pmod 8$, can be spanned by the g-th weight enumerators of self-dual doubly-even codes of length m. This fact is one of the reason that coding theory plays a significant role in [6], [12]. We might point out that the *abstractly* defined space R_g^m is identified with the *explicitly* defined space.

On the groups H_5 and $Sp(10, 2)$

We collect the definitions and some properties of the groups which we need later.

We recall the symplectic group $Sp(10, 2)$ of degree 5 over $\mathbf{F}_2$. Let $\Delta = \{\pm 2\xi_i, \pm\xi_i \pm \xi_j (i < j) | 1 \leq i, j \leq 5\}$ be the root system of type C_5, and we choose $\xi_1 - \xi_2, \xi_2 - \xi_3, \xi_3 - \xi_4, \xi_4 - \xi_5, 2\xi_5$ for a fundamental system Π of roots. We denote by Δ^+ the set of positive roots with respect to Π. Let E_{ij} be the matrix whose (i, j)-entry is 1 and all the other entries are 0. For $1 \leq i, j \leq 5$ we put

$$\begin{aligned}
x_{\xi_i+\xi_j} &= 1 + E_{i,5+j} + E_{j,5+i}, (i \neq j) \\
x_{\xi_i-\xi_j} &= 1 + E_{i,j} + E_{5+j,5+i} (i < j) \\
x_{2\xi_i} &= 1 + E_{i,5+i}, \\
x_{-r} &= {}^t x_r (r \in \Delta)
\end{aligned}$$

Note that the above matrices in the right-hand side are defined over the field of two elements. The symplectic group $Sp(10, 2)$ is generated by $x_r (r \in \Delta)$.

The group H_5 is generated by the elements T_5 and $D_S = \text{diag}\,(i^{S[a]})$ for integral symmetric S, where $(T_5)_{a,b} = \left(\frac{1+i}{2}\right)^5 (-1)^{a \cdot b}$. Let H_5 act on $N_5/\langle i \rangle \cong \mathbf{F}_2^5$ by conjugation. This induces a surjective homomorphism

$$\psi : H_5 \rightarrow Sp(10, 2)$$

$$\begin{aligned}
\psi(B) &= 1_{10}, B \in N_5, \\
\psi(\widetilde{A}) &= \begin{pmatrix} A & 0 \\ 0 & {}^t(A^{-1}) \end{pmatrix}, A \in GL(5,2), \\
\psi(T_5) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\psi(D_S) &= \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

Here we need to explain the notation $\widetilde{A}$. Label the basis of $\mathbf{C}^{2^5}$ as $e_v, v \in \mathbf{F}_2^5$. For $A \in GL(5,2)$ we define the unitary transformation $\widetilde{A} \in \mathbf{C}^{2^5}$ by $e_v\widetilde{A} = e_{vA}$.

We have given the definitions of H_5 and $Sp(10,5)$ and the homomorphism between them. In order to proceed our computation conveniently we give some more information. Let e_{ij} be the 5×5 matrices whose (i,j) entry is 1 and all the other entries are 0. For $1 \le i, j \le 5$ we put

$$\begin{aligned}
X_{\xi_i+\xi_j} &= D_{e_{ij}+e_{ji}}, \\
X_{\xi_i-\xi_j} &= \widetilde{1+e_{ij}}(i \ne j) \\
X_{2\xi_i} &= D_{e_{ii}} \\
X_{-r} &= T_5 X_r T_5 (r \in \Delta^+) \\
W_r &= X_r X_{-r} X_r (r \in \Pi)
\end{aligned}$$

Note that the above matrices in the right-hand side are defined over the field of complex numbers. We have $\psi(X_{\xi_i+\xi_j}) = x_{\xi_i+\xi_j}, \psi(X_{\xi_i-\xi_j}) = x_{\xi_i-\xi_j}, \psi(X_{2\xi_i}) = x_{2\xi_i}, \psi(X_{-r}) = x_{-r}$, and $\psi(W_r) = w_r$.

The orders of these groups are not necessary in this paper but we give them for the convenience.

$$\begin{aligned}
|N_5| &= 4,096 = 2^{12}, \\
|Sp(10,2)| &= 24,815,256,521,932,800 = 2^{25}3^6 5^2 7 \cdot 11 \cdot 17 \cdot 31, \\
|H_5| &= 101,643,290,713,836,748,800 = 2^{37}3^6 5^2 7 \cdot 11 \cdot 17 \cdot 31, \\
198 \times |N_5| &= 811,008.
\end{aligned}$$

The meaning of the last number above will be clear in the course of our computation. The number 198 is the number of conjugacy classes of $Sp(10,2)$.

The dimension formula

Theorem. *The dimension formula of the invariant ring of H_5 is given by*

$$\begin{aligned}
\sum_m (\dim R_5^m)\, t^m &= 1 + t^8 + 2t^{16} + 2t^{20} + 8t^{24} + 8t^{28} + 34t^{32} + 60t^{36} \\
&\quad + 203t^{40} + 553t^{44} + 2063t^{48} + 7359t^{52} + 30811t^{56} \\
&\quad + 127416t^{60} + 541644t^{64} + 2235677t^{68} + 8966371t^{72} + \cdots \\
&= \frac{N}{D}
\end{aligned}$$

Proof. First we investigate the conjugacy classes of $Sp(10,2)$. More precisely we need a representative and an order of each class. There exist 198 conjugacy classes in $Sp(10,2)$. This is carried out by gap [7]. Since we already know the homomorphism $\psi : H_5 \to Sp(10,2)$ with $\mathrm{Ker}\psi = N_5$ explicitly, we can decompose H_5/N_5 into conjugacy classes $Z_0, Z_1, \cdots, Z_{197}$. If we write a representative of each class Z_i as $z_i N_5$, the dimension formula of the invariant ring is computed as follows.

$$\begin{aligned}\sum_m (\dim R_5^m)\, t^m &= \frac{1}{|H_5|} \sum_{\sigma \in H_5} \frac{1}{\det(1 - t\sigma)} \\ &= \frac{1}{|H_5|} \sum_{i=0}^{197} \sum_{n \in N_5} \frac{|Z_i|}{\det(1 - t z_i n)} \\ &= 1 + t^8 + 2t^{16} + 2t^{20} + 8t^{24} + 8t^{28} + 34t^{32} + 60t^{36} + \cdots .\end{aligned}$$

This completes the proof of the theorem.

Corollary. *The g-th weight enumerators of the* 9 *self-dual doubly-even codes of length* 24 *are linearly independent if and only if the genus g is greater than* 5.

Proof. We already know that the dimension of the space R_5^{24} is 8. Here we observe that a linear relation among weight enumerators in genus g remains in genus $g-1$. This is a consequence of Φ operator

$$\Phi(F_a) = \begin{cases} F_b & \text{if } a = (b0), \\ 0 & \text{if } a = (b1). \end{cases}$$

Therefore in order to prove the corollary, we have only to show that the 6-th weight enumerators of the 9 codes are linearly independent. This is obtained by the fact that the 9×9 matrix M which we shall give in the next section is non-singular. This completes the proof of Corollary.

Some coefficients of $W_C^{(6)}$'s

Determination of all admissible monomials becomes complicated when the associated genus and length increase, however, it is not the case if we need only a few of them. For example, arbitrary g elements of a self-dual doubly-even code gives an admissible monomial. Another construction is "lifting" from one less genus. Let $(a_1, a_2, \ldots, a_{2^{g-1}})$ be an admissible monomial of genus $g-1$. Then $(a_1, 0, a_2, 0, \ldots, a_{2^{g-1}}, 0)$ is admissible in genus g.

We give the 9 admissible monomials below. The choice of monomials is arbitrary, but the resulting matrix M must be non-singular (as a matter of fact, we can do this). The first 8 monomials is obtained from the admissible monomials in genus 5. Only in the following table we use the convention $a^b = \underbrace{a, a, \ldots, a}_{b}$.

$$(0^{62}, 24, 0),$$
$$(0^{32}, 4, 0^{29}, 20, 0),$$
$$(2, 0^{29}, 2, 0, 18, 0^{29}, 2, 0),$$
$$(1, 0, 1, 0^{25}, 1, 0, 1, 0, 17, 0, 1, 0^{25}, 1, 0, 1, 0),$$
$$(0^{28}, 2, 0, 2, 0, 16, 0^{27}, 2, 0, 2, 0),$$
$$(0^{24}, 1, 0, 1, 0, 1, 0, 1, 0, 16, 0^{23}, 1, 0, 1, 0, 1, 0, 1, 0),$$
$$(2, 0^{29}, 2, 0^{3}, 2, 0, 2, 0, 2, 0^{23}, 14, 0),$$
$$(2, 0^{7}, 12, 0^{19}, 2, 0^{5}, 2, 0, 2, 0, 2, 0^{21}, 2, 0^{3}),$$
$$(1, 0, 1, 0^{13}, 1, 0, 1, 0^{4}, 4, 0^{12}, 2^{2}, 0^{6}, 1, 0, 1, 0^{5}, 1^{4}, 0^{5}, 3, 2, 1)$$

The following 9×9 matrix M is rank 9. The rows correspond to the 9 self-dual doubly-even codes of length 24. The columns correspond to the 9 admissible monomials given above. The order of columns and of rows are the one given in this paper. The matrix entry is the coefficient of the weight enumerator of the corresponding code at the corresponding monomial.

$$M = \begin{pmatrix}
1 & 30 & 240 & 0 & 720 & 0 & 1440 & 1440 & 16588800 \\
1 & 24 & 144 & 336 & 120 & 0 & 120 & 0 & 27095040 \\
1 & 18 & 72 & 0 & 72 & 0 & 0 & 0 & 23887872 \\
1 & 12 & 24 & 0 & 0 & 0 & 0 & 0 & 18164736 \\
1 & 66 & 1320 & 0 & 11880 & 0 & 95040 & 665280 & 0 \\
1 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 7741440 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 42 & 504 & 1344 & 1848 & 1344 & 6720 & 20160 & 0 \\
1 & 42 & 504 & 4032 & 504 & 4032 & 0 & 0 & 0
\end{pmatrix}$$

From the matrix M, we know that the dimension of the space R_5^{24} is greater than or equal to 8, but we can not conclude that it is exactly 8.

All linear relations among $W_C^{(g)}$'s, $g \geq 3$

We collect all relations among the g-th weight enumerators of the 9 self-dual doubly-even codes of length 24, $g \geq 3$. We refer to [4] for the cases $g = 1, 2$. The dimensions of R_g^{24} are as follows.

g	1	2	3	4	5	$g \geq 6$
$\dim R_g^{24}$	2	3	5	7	8	9

$\underline{g = 3}$ We take $W_{C_1}, W_{C_2}, W_{C_3}, W_{C_4}, W_{C_5}$ as a basis.

$$\begin{aligned}
54W_{C_6} &= 30W_{C_1} - 135W_{C_3} + 160W_{C_4} - W_{C_5},\\
72W_{C_7} &= 132W_{C_1} - 495W_{C_3} + 440W_{C_4} - 5W_{C_5},\\
9W_{C_8} &= 6W_{C_1} + 36W_{C_2} - 54W_{C_3} + 20W_{C_4} + W_{C_5},\\
27W_{C_9} &= -66W_{C_1} + 324W_{C_2} - 351W_{C_3} + 116W_{C_4} + 4W_{C_5},
\end{aligned}$$

$\underline{g=4}$(Proposition 1.5 fo [6]) We take $W_{C_1}, W_{C_2}, W_{C_3}, W_{C_4}, W_{C_6}, W_{C_7}, W_{C_8}$ as a basis.

$$\begin{aligned}
W_{C_5} &= 66W_{C_1} - 495W_{C_3} + 880W_{C_4} - 594W_{C_6} + 144W_{C_7},\\
W_{C_9} &= -14W_{C_1} + 70W_{C_3} - 112W_{C_4} + 70W_{C_6} - 16W_{C_7} + 3W_{C_8}.
\end{aligned}$$

$\underline{g=5}$(opy [12]) We take $W_{C_1}, W_{C_2}, W_{C_3}, W_{C_4}, W_{C_5}, W_{C_6}, W_{C_7}, W_{C_8}$ as a basis.

$$99W_{C_9} = -924W_{C_1} + 3465W_{C_3} - 4928W_{C_4} - 7W_{C_5} + 2772W_{C_6} - 576W_{C_7} + 297W_{C_8}.$$

References

duke [1] Duke, W., On codes and Siegel modular forms, Internat. Math. Res. Notices (1993), 125–136.

bfw [2] Borcherds, R.E., Freitag, E., Weissauer, R., A Siegel cusp form of degree 12 and weight 12, J. reine angew. Math. **494**(1998), 141–153.

cck [3] Calderbank, A.R., Cameron, P.J., Kantor, W.M., Z4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. London Math. Soc.(3)**75**(1997), 436–480.

co [4] Choie, Y., Oura, M., The joint weight enumerators and Siegel modular forms, to appear in Proc. Amer. Math. Soc.

cs [5] Conway, J.H., Sloane, N.J.A., Sphere packings, lattices and groups, Third edition, Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York, 1999.

fo [6] Freitag, E., Oura, M., A theta relation in genus 4, Nagoya Math. J. **161**(2001), 69–83.

gap [7] GAP,

herrmann [8] Herrmann, N., Höhere Gewichtsazähler von Codes und deren Beziehung zur Theorie der Siegelschen Modulformen, Diplomarbeit, Bonn, 1991.

huffman [9] Huffman, W.C., The biweight enumerator of self-orthogonal binary codes. Discrete Math. **26**(1979), 129–143.

nrs [10] Nebe, G., Rains, E., Sloane, N.J.A.,

oura [11] Oura, M., The dimension formula for the ring of code polynomials in genus 4, Osaka J. Math. **34**(1997), 53–72.

opy [12] Oura, M., Poor, C., Yuen, D., Identities among second order theta constants, preprint.

rungeI [13] Runge, B., On Siegel modular forms, I, J. Reine Angew. Math. **436**(1993), 57–85.

rungeII [14] Runge, B., On Siegel modular forms, II, Nagoya Math. J. **138**(1995), 179–197.

rungeIII [15] Runge, B., Codes and Siegel modular forms, Discrete Math. **148**(1996), 175–204.

vardi [16] Vardi, I., Coding theory(Multiple weight enumerators of codes), preprint, 1998.