



Title	On the integral ring spanned by genus two weight enumerators
Author(s)	Oura, Manabu
Citation	Hokkaido University Preprint Series in Mathematics, 808, 1-5
Issue Date	2006
DOI	10.14943/83958
Doc URL	<a href="http://hdl.handle.net/2115/69616">http://hdl.handle.net/2115/69616</a>
Type	bulletin (article)
File Information	pre808.pdf



[Instructions for use](#)

ON THE INTEGRAL RING SPANNED BY GENUS TWO WEIGHT  
ENUMERATORS

MANABU OURA

**Abstract.** It is known that the weight enumerator of a self-dual doubly-even code in genus  $g = 1$  can be uniquely written as an isobaric polynomial in certain homogeneous polynomials with *integral* coefficients. We settle the case where  $g = 2$  and prove the non-existence of such polynomials under some conditions.

**1. Introduction.** In this paper we deal with binary self-dual doubly-even codes only. We refer to [3] for the general facts on coding theory. We shall first recall our problem in the case where  $g = 1$ , which explains what this paper concerns about. It is known that the weight enumerator of any self-dual doubly-even code can be uniquely written as an isobaric polynomial in  $\varphi_8 = x^8 + 14x^4y^4 + y^8$  and  $\varphi_{24} = x^4y^4(x^4 - y^4)^4$  with integral coefficients ([5]). We note that  $\varphi_{24}$  itself is not the weight enumerator of a code but a linear combination of the weight enumerators with rational coefficients.

We shall add a few words on this basis. We consider the elements in  $\mathbf{Z}[x, y]$  for simplicity. The choice of  $\varphi_8$  is unique (up to  $\pm 1$ ) since there exists a unique self-dual doubly-even code  $e_8$  of length 8. Next we assume that another homogeneous polynomial  $\xi$  of degree 24 has the property in question, i.e., the weight enumerator of any self-dual doubly-even code can be written as an isobaric polynomial in  $\varphi_8$  and  $\xi$  with integral coefficients. We put  $\xi = ax^{24} + bx^{20}y^4 + \dots$ ,  $a, b \in \mathbf{Z}$ , in which the unwritten part consists of terms of degree less than 20 in  $x$ . There are 85 classes self-dual doubly-even codes of length 32([1], [2]) and the weight enumerator of these classes should be written as  $m\varphi_8^4 + n\varphi_8\xi$ , in which  $m, n$  are integers. Examining these conditions for all classes, we know that  $-42a + b$  must be a divisor of 1. We have that  $\xi = a\varphi_8 \pm \varphi_{24}$  and conversely, such  $\xi$  has the said property.

In the rest of this paper we restrict ourselves to the case where  $g = 2$  when considering the weight enumerators. Let  $C$  be a binary self-dual doubly-even code and  $W_C = W_C(x, y, z, w)$  the weight enumerator of  $C$  in genus 2 (*cf.* [6], [4], [7]). We remark that  $W_C$  is symmetric in  $x, y, z, w$ . We shall denote by  $\mathfrak{W}$  the graded ring over the field  $\mathbf{C}$  of complex numbers generated by  $W_C$  of all self-dual doubly-even codes. The degree  $d$ -part  $\mathfrak{W}_d$  of  $\mathfrak{W}$  is a finite dimensional vector space over  $\mathbf{C}$ . The four elements

$W_{e_8}, W_{d_{24}^+}, W_{g_{24}}, W_{d_{40}^+}$  are algebraically independent over  $\mathbf{C}$  and the graded ring  $\mathfrak{W}$  is a free  $\mathbf{C}[W_{e_8}, W_{d_{24}^+}, W_{g_{24}}, W_{d_{40}^+}]$ -module with a basis  $1, W_{d_{32}^+}$ , where  $g_{24}$  is the extended Golay code of length 24. The dimension formula of this ring is

$$\begin{aligned} \sum_{d \geq 0} (\dim \mathfrak{W}_d) t^d &= \frac{1 + t^{32}}{(1 - t^8)(1 - t^{24})^2(1 - t^{40})} \\ &= 1 + t^8 + t^{16} + 3t^{24} + 4t^{32} + 5t^{40} + 8t^{48} + 10t^{56} + \dots \end{aligned}$$

We always keep this formula in mind through the next section.

**2. Result.** For the proof of our Theorem, we shall construct homogeneous polynomials  $X_8, X_{24}, Y_{24}, X_{32}, X_{40}$  of degrees 8, 24, 24, 32, 40, respectively. This is done by analyzing the vector spaces  $\mathfrak{W}_d$ ,  $d = 8, 24, 32, 40$ .

(degree 8) The extended Hamming code  $e_8$  of length 8 is a unique self-dual doubly-even code of this length. We put  $X_8 = W_{e_8}$ .  $X_8$  is also characterized by  $x^8 + \dots$ .

(degree 24) Two polynomials  $X_{24}, Y_{24}$  are characterized by

$$\begin{aligned} 0x^{24} + x^{20}(y^4 + \dots) + 0x^{18}(y^2z^2w^2) + \dots, \\ 0x^{24} + 0x^{20}(y^4 + \dots) + x^{18}(y^2z^2w^2) + \dots \end{aligned}$$

As we remarked, the weight enumerator in this paper is symmetric and  $x^{20}(y^4 + \dots)$  stands for  $x^{20}(y^4 + z^4 + w^4)$ . We note that 0 as a coefficient of  $x^{18}(y^2z^2w^2)$  in the first formula is not much of importance. The general form of the elements in  $\mathfrak{W}_{24}$  is

$$a_0x^{24} + a_1x^{20}(y^4 + \dots) + a_2x^{18}(y^2z^2w^2) + \dots$$

and is uniquely written as

$$a_0X_8^3 + (-42a_0 + a_1)X_{24} + (-504a_0 + a_2)Y_{24}.$$

(degree 32) The polynomial  $X_{32}$  is characterized by

$$0x^{32} + 0x^{28}(y^4 + \dots) + 0x^{26}y^2z^2w^2 + x^{24}(y^4z^4 + \dots) + \dots$$

We remark that  $0x^{32} + 0x^{28}(y^4 + \dots) + \dots$  implies that the coefficient of  $x^{24}(y^8 + \dots)$  is 0. The similar remark also holds in the following (degree 40). The general form of the elements in  $\mathfrak{W}_{32}$  is

$$a_0x^{32} + a_1x^{28}(y^4 + \dots) + a_2x^{26}(y^2z^2w^2) + x^{24}(a_3(y^8 + \dots) + a_4(y^4z^4 + \dots)) + \dots$$

and is uniquely written as

$$a_0X_8^4 + (-56a_0 + a_1)X_8X_{24} + (-672a_0 + a_2)X_8Y_{24} + (784a_0 - 33a_1 - 2a_2 + a_4)X_{32},$$

where  $a_3 = 620a_0 + 10a_1$ .

(degree 40) The polynomial  $X_{40}$  is characterized by

$$0x^{40} + 0x^{36}(y^4 + \dots) + 0x^{34}(y^2z^2w^2) + 0x^{32}(y^4z^4 + \dots) + x^{28}(y^4z^4w^4) + \dots.$$

The general form of the elements in  $\mathfrak{W}_{40}$  is

$$a_0x^{40} + a_1x^{36}(y^4 + \dots) + a_2x^{34}(y^2z^2w^2) + x^{32}(a_3(y^8 + \dots) + a_4(y^4z^4 + \dots)) \\ + a_5x^{30}(y^6z^2w^2 + \dots) + x^{28}(a_6(y^{12} + \dots) + a_7(y^8z^4 + \dots) + a_8(y^4z^4w^4)) + \dots$$

and is uniquely written as

$$a_0X_8^5 + (-70a_0 + a_1)X_8^2X_{24} + (-840a_0 + a_2)X_8^2Y_{24} + (1960a_0 - 61a_1 - 2a_2 + a_4)X_8X_{32} \\ + (196560a_0 - 7350a_1 - 880a_2 + 150a_4 + a_8)X_{40},$$

where we have the relations  $a_3 = 285a_0 + 24a_1$ ,  $a_5 = 84a_1 - 8a_2 + 12a_4$ ,  $a_6 = 21280a_0 + 92a_1$ ,  $a_7 = 225a_1 + 32a_2 + 11a_4$ .

The homogeneous polynomials we have obtained can be written as

$$X_8 = W_{e_8}, \\ X_{24} = 5 \cdot 2^{-2}3^{-1}7^{-1}W_{e_8}^3 - 2^{-2}11^{-1}W_{d_{24}^+} - 17 \cdot 2^{-1}3^{-1}7^{-1}11^{-1}W_{g_{24}}, \\ Y_{24} = -2^{-4}3^{-1}7^{-1}W_{e_8}^3 + 2^{-4}3^{-1}11^{-1}W_{d_{24}^+} + 2^{-2}3^{-1}7^{-1}11^{-1}W_{g_{24}}, \\ X_{32} = 67 \cdot 2^{-10}3^{-1}7^{-1}W_{e_8}^4 - 5 \cdot 2^{-7}11^{-1}W_{e_8}W_{d_{24}^+} - 2^{-3}3^{-1}7^{-1}11^{-1}W_{e_8}W_{g_{24}} + 2^{-10}W_{d_{32}^+}, \\ X_{40} = -461 \cdot 2^{-13}3^{-1}5^{-1}7^{-1}41^{-1}W_{e_8}^5 + 13 \cdot 2^{-9}3^{-1}11^{-1}41^{-1}W_{e_8}^2W_{d_{24}^+} \\ + 2^{-6}3^{-1}7^{-1}11^{-1}41^{-1}W_{e_8}^2W_{g_{24}} - 3 \cdot 2^{-13}41^{-1}W_{e_8}W_{d_{32}^+} + 2^{-10}3^{-1}5^{-1}41^{-1}W_{d_{40}^+}.$$

We note that  $X_8, X_{24}, Y_{24}, X_{32}, X_{40}$  are in  $\mathbf{Z}[x, y, z, w]$  and that they generate the ring  $\mathfrak{W}$ .

These being prepared, we prove

**THEOREM.** *There exist no five homogeneous polynomials of degrees 8, 24, 24, 32, 40 in  $\mathfrak{W} \cap \mathbf{Z}[x, y, z, w]$  such that the weight enumerator of any self-dual doubly-even code can be written as an isobaric polynomial in these five elements with integral coefficients.*

*Proof.* Suppose that there exist such homogeneous polynomials of degrees 8, 24, 24, 32, 40 satisfying the property in Theorem. As we discussed in this

section, any element in  $\mathfrak{W} \cap \mathbf{Z}[x, y, z, w]$  of degree at most equal to 40 can be uniquely written as an isobaric polynomial in  $X_8, X_{24}, Y_{24}, X_{32}, X_{40}$  with integral coefficients and the five assumed polynomials are hence integral polynomials in  $X_8, \dots, X_{40}$ . Therefore  $X_8, \dots, X_{40}$  also enjoy the property in Theorem, i.e., the weight enumerator of any self-dual doubly-even code can be written as

$$\sum_{i,j,k,l,m \in \mathbf{Z}_{\geq 0}} a_{ijklm} X_8^i X_{24}^j Y_{24}^k X_{32}^l X_{40}^m,$$

in which all  $a_{ijklm}$  are integers. The weight enumerator of the code  $d_{56}^+$  is, however, written as

$$\begin{aligned} & X_8^7 + 2^3 5 \cdot 7 X_8^4 X_{24} + 2^4 3 \cdot 5 \cdot 7 \cdot 11 X_8^4 Y_{24} + 2^8 7 \cdot 23 X_8^3 X_{32} \\ & + 2^{16} 7 \cdot 139 \cdot 3^{-2} X_8^2 X_{40} + 2^8 7 X_8 X_{24}^2 + 2^{10} 3 \cdot 7 \cdot 11 X_8 X_{24} Y_{24} \\ & + 2^{10} 7 \cdot 6521 \cdot 3^{-2} X_8 Y_{24}^2 + 2^{11} 5 \cdot 7 X_{24} X_{32} + 2^{12} 7 \cdot 227 \cdot 3^{-1} Y_{24} X_{32}. \end{aligned}$$

This expression is unique and we get a contradiction. This completes the proof of Theorem.

If we take a self-dual doubly-even code  $C$  of length 48, and write  $W_C$  as an isobaric polynomial in  $X_8, X_{24}, Y_{24}, X_{32}, X_{40}$ , then we can show that the coefficients in this expression are in  $\mathbf{Z}[\frac{1}{3}]$ . It was, therefore, expected to find a counter example to our assumption in the proof of Theorem at this length, but it did not work out that way.

**Acknowledgement.** The author would like to thank Professor Nebe for her comments on this manuscript. This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Young Scientists (B).

## REFERENCES

- [1] Conway, J. H., Pless, V., On the enumeration of self-dual codes, J. Combin. Theory Ser. A 28 (1980), no. 1, 26–53.
- [2] 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.

- [3] Conway, J. H., Sloane, N. J. A., Sphere packings, lattices and groups, Third edition, Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York, 1999.
- [4] Duke, W., On codes and Siegel modular forms, *Internat. Math. Res. Notices* 1993, no. 5, 125–136.
- [5] 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.
- [6] Huffman, W. C., The biweight enumerator of self-orthogonal binary codes, *Discrete Math.* 26 (1979), no. 2, 129–143.
- [7] Nebe, G., Rains, E.M., Sloane, N.J.A., Self-dual codes and invariant theory, *Algorithms and Computation in Mathematics* 17, Springer-Verlag, Berlin, 2006.