EISENSTEIN POLYNOMIALS ASSOCIATED TO BINARY CODES

Manabu Oura

Abstract. The Eisenstein polynomial is the weighted sum of all classes of Type II codes of fixed length. In this note, we investigate the ring of the Eisenstein polynomials in genus 2.

1. Introduction. The Eisenstein series play an important role in the theory of modular forms. Here we would like to mention two points. One is that the Eisenstein series is, possibly up to a constant factor, the weighted sum of the theta series of all classes of even unimodular lattices of fixed length([20]. *cf.* [21], [19]). Another is that the ring of modular forms of even weights for the full modular group in genus g is the normalization of the graded ring generated over the field $\mathbf{C}$ of complex numbers by the Eisenstein series. This might suggest that the ring of Eisenstein series is close to the ring of modular forms. In the two spacial cases $g = 1, 2$, we know that the ring of modular forms of even weights coincide with the ring of Eisenstein series, however, this is no longer true for $g > 2$. See [7], [8].

The Eisenstein polynomial on the title is analogue to the Eisenstein series, that is, the weighted sum of the weight enumerators of all classes of Type II codes of fixed length. In contrast with Eisenstein series, it is natural to investigate the ring of Eisenstein polynomials. The ring of Eisenstein polynomials is a subring of the ring of the weight enumerators of Type II codes. In the first case $g = 1$, two rings coincide but this does not hold if $g \geq 2$. The objective of this note is to determine the ring of Eisenstein polynomials in the case $g = 2$. We shall show that *the ring of Eisenstein polynomials in genus* 2 *is minimally generated by the ten Eisenstein polynomials of degrees*

$$8,\ 24,\ 32,\ 40,\ 48,\ 56,\ 64,\ 72,\ 80,\ 96$$

and coincides with the ring of weight enumerators in genus 2 *except for homogeneous parts of lower degrees.*

We shall denote by $\mathbf{Z}, \mathbf{F}_2$ the ring of rational integers, the field of two elements, respectively. For a finite set M, we shall denote by $|M|$ the number of elements of M.

2. Eisenstein Polynomial. Let g be a positive integer. We understand that an element of $\mathbf{F}_2^g$ is a row vector. For $A = (e_a : a \in \mathbf{F}_2^g) \in \mathbf{Z}_{\geq 0}^{2^g}$, we put

$$\dim A = \dim_{\mathbf{F}_2} \langle (1a) \in \mathbf{F}_2^{g+1} | e_a > 0 \rangle.$$

We introduce 2^g letters x_a of degree 1 for $a \in \mathbf{F}_2^g$. For $A = (e_a : a \in \mathbf{F}_2^g) \in \mathbf{Z}_{\geq 0}^{2^g}$, a monomial $x^A = \prod_{a \in \mathbf{F}_2^g} x_a^{e_a}$ is called admissible if the degree

$n = \sum_{a \in \mathbf{F}_2^g} e_a$ is a multiple of 8 and

$$\sum_{a \in \mathbf{F}_2^g} aS\ {}^t a \equiv 0 \pmod 4$$

for all integral symmetric $g \times g$ matrices S. Here ${}^t a$ stands for the transpose of a. For $n = 8,\ 16,\ 24, \ldots$, we define the Eisenstein polynomial of degree n in genus g by

$$E_{g,n}(x_a : a \in \mathbf{F}_2^g) = \sum_A \frac{\prod_{j=0}^{n/2-\dim A-1} (2^j + 1)}{\prod_{a \in \mathbf{F}_2^g} e_a!} x^A,$$

in which the summation is extended over the set of all admissible monomials A of degree n. The above definition of the Eisenstein polynomials is formal but the meaning of them is not clear. In order to obtain a better understanding, we interpret the Eisenstein polynomial from coding theory as stated in the introduction.

A linear code C of length n is a subspace of $\mathbf{F}_2^n$. A linear code is called self-dual if it coincides with its dual with respect to the inner product $x \cdot y = \sum x_i y_i$. A linear code is called doubly even if the number of non-zero coordinates for every element of the code is a multiple of 4. A self-dual and doubly even code is simply called Type II. It is known that a Type II code exists if and only if n is a multiple of 8. Two codes are called equivalent if one coincides with another under some coordinate permutation. Up to this equivalence, classifications of Type II codes are completed for $n = 8,\ 16,\ 24,\ 32$([13], [14], [3]. *cf.* [4]). The class invariant polynomial is given by

$$W_{g,C}(x_a : a \in \mathbf{F}_2^g) = \sum_{v_1, v_2, \cdots, v_g \in C} \prod_{1 \le i \le n} x_{(v_{1i}, v_{2i}, \ldots, v_{gi})},$$

which is called the weight enumerator of the code C in genus g. The set of coordinate permutations that map a code C to itself forms a group, called the automorphism group of C. We shall denote this group by $\mathrm{Aut}(C)$. Let M_n denote the set of all Type II codes of length n. Then we have

$$\begin{aligned} E_{g,n}(x_a : a \in \mathbf{F}_2^g) &= \frac{1}{n!} \sum_{C \in M_n} W_{g,C}(x_a : a \in \mathbf{F}_2^g) \\ &= \sum_{[C]} \frac{1}{|\mathrm{Aut}(C)|} W_{g,C}(x_a : a \in \mathbf{F}_2^g), \end{aligned}$$

in which the summation of the second line is extended over the set of all classes $[C]$ of Type II codes of length n. Hence the polynomial $E_{g,n}(x_a : a \in$

$\mathbf{F}_2^g$) is called 'Eisenstein polynomial'. We refer to [20] for the original case of this identity (*cf.* [21], [19]). By [10], the cardinality of M_n is known to be $\prod_{j=0}^{n/2-2}(2^j+1)$. Multiplying $n!/|M_n|$, we get the normalized Eisenstein polynomial

$$\begin{aligned} E^*_{g,n}(x_a : a \in \mathbf{F}_2^g) &= \frac{n!}{|M_n|} E_{g,n}(x_a : a \in \mathbf{F}_2^g) \\ &= \sum_{a \in \mathbf{F}_2^g} x_a^n + \cdots . \end{aligned}$$

We refer to [9], [15], [6] for the general theory of codes, to [1], [17], [18] for the Eisenstein polynomials. See also [11] in which the Eisenstein polynomial plays an important role.

3. Ring of Eisenstein polynomials. Before restricting ourselves to the case $g = 2$, we observe that the ring of Eisenstein polynomials coincides with the ring of weight enumerators of Type II code if and only if $g = 1$. In fact, as we shall see later, this is so for $g = 2$. In the case $g \geq 3$, the dimension of the vector space of weight enumerators for length 24 is at least 5 by [16](see also [17], [11]), whereas the corresponding dimension of the Eisenstein polynomials is at most 3. Therefore two rings in question do not coincide.

In the rest of this note, we assume that $g = 2$ (and may omit $g = 2$ for simplicity). We refer to [5], [17], [12] for the invariant theory of this section.

We shall denote by $\mathfrak{E}$, $\mathfrak{W}$ the ring generated over $\mathbf{C}$ by the Eisenstein polynomials, the ring generated over $\mathbf{C}$ by the weight enumerators of Type II codes, respectively. The ring $\mathfrak{E}$ is a subring of $\mathfrak{W}$. We shall denote by $\mathfrak{E}_w$, $\mathfrak{W}_w$ the homogeneous part of degree w of $\mathfrak{E}$, $\mathfrak{W}$, respectively. The ring $\mathfrak{W}$ can be generated by five elements of degrees 8, 24, 24, 32, 40 and has the dimension formula

$$\begin{aligned} \sum_{w \geq 0} (\dim \mathfrak{W}_w)\, t^w &= \frac{1+t^{32}}{(1-t^8)(1-t^{24})^2(1-t^{40})} \\ &= 1 + t^8 + t^{16} + 3t^{24} + 4t^{32} + 5t^{40} + 8t^{48} + 10t^{56} \\ &\quad + 12t^{64} + 17t^{72} + 21t^{80} + 24t^{88} + 31t^{96} + 37t^{104} \\ &\quad + 42t^{112} + 52t^{120} + 60t^{128} + 67t^{136} + 80t^{144} + 91t^{152} \\ &\quad + 101t^{160} + 117t^{168} + \cdots . \end{aligned}$$

Now, we shall start investigating the graded ring $\mathfrak{E}$ of Eisenstein polynomials. By direct calculations with Magma [2], the dimensions of $\mathfrak{E}_w$ for $w = 24,\ 32,\ \ldots,\ 80$ are

$$2,\ 3,\ 4,\ 6,\ 8,\ 11,\ 15,\ 20$$

and we have that $\mathfrak{E}_w = \mathfrak{W}_w$ for $w = 0, 8, 16, 88, 96, \ldots, 168$. In the course of this calculation, we know that none of the Eisenstein polynomials of degrees

$$8,\ 24,\ 32,\ 40,\ 48,\ 56,\ 64,\ 72,\ 80,\ 96$$

is redundant to generate the ring $\mathfrak{E}$. For $w = 176,\ 184, \ldots$, we can foresee that $\mathfrak{E}_w = \mathfrak{W}_w$. Actually this is the case. The proof is as follows.

We denote by $\widetilde{\mathfrak{E}}$ a subring of $\mathfrak{E}$ generated by the above ten Eisenstein polynomials. We observe that the ring $\mathfrak{W}$ can be generated by the elements

$$E_8, E_{24}, W_{g_{24}}, E_{32}, E_{40},$$

in which g_{24} denotes the extended Golay code of length 24. Because of $W_{g_{24}}^4 \in \widetilde{\mathfrak{E}}$, we know that $\mathfrak{W}$ is an $\widetilde{\mathfrak{E}}$-module generated by $1,\ W_{g_{24}},\ W_{g_{24}}^2,\ W_{g_{24}}^3$, i.e.,

$$\mathfrak{W} = \widetilde{\mathfrak{E}} + \widetilde{\mathfrak{E}} W_{g_{24}} + \widetilde{\mathfrak{E}} W_{g_{24}}^2 + \widetilde{\mathfrak{E}} W_{g_{24}}^3.$$

We shall show that every element of $\widetilde{\mathfrak{E}} + \widetilde{\mathfrak{E}} W_{g_{24}} + \widetilde{\mathfrak{E}} W_{g_{24}}^2 + \widetilde{\mathfrak{E}} W_{g_{24}}^3$ for degree at least 88 is an element of $\widetilde{\mathfrak{E}}$. As before, we shall denote by $\widetilde{\mathfrak{E}}_w$ the homogeneous part of degree w of $\widetilde{\mathfrak{E}}$. Note that we have already that $\widetilde{\mathfrak{E}}_w = \mathfrak{E}_w = \mathfrak{W}_w$ for $w = 88,\ 96,\ \ldots,\ 168$.

I) Put $\varphi = E_8^a E_{24}^b E_{32}^c E_{40}^d E_{48}^e E_{56}^f E_{64}^g E_{72}^h E_{80}^i E_{96}^j W_{g_{24}}$ and assume that $\deg \varphi \geq 88$. If one of

$$a \geq 8,\ b \geq 3,\ c \geq 2,\ d \geq 2,\ e \geq 2,\ f \geq 2,\ g \geq 1,\ h \geq 1,\ i \geq 1,\ j \geq 1$$

holds, then φ is a product of an element of $\widetilde{\mathfrak{E}}$ with one of

$$E_8^8 W_{g_{24}},\ E_{24}^3 W_{g_{24}}, E_{32}^2 W_{g_{24}},\ E_{40}^2 W_{g_{24}},\ E_{48}^2 W_{g_{24}},$$
$$E_{56}^2 W_{g_{24}},\ E_{64} W_{g_{24}},\ E_{72} W_{g_{24}},\ E_{80} W_{g_{24}},\ E_{96} W_{g_{24}}.$$

The degrees of $E_8^8 W_{g_{24}},\ \ldots,\ E_{96} W_{g_{24}}$ are at most 136 and all of them are in $\widetilde{\mathfrak{E}}$. Therefore φ is an element of $\widetilde{\mathfrak{E}}$. This reduces our consideration to the case

$$a \leq 7,\ b \leq 2,\ c \leq 1,\ d \leq 1,\ e \leq 1,\ f \leq 1$$

and $g = h = i = j = 0$.

The case $f = 1$. At least one of a, b, c, d, e is not zero. We shall denote by E_* one of $E_8,\ \ldots,\ E_{48}$ appearing in $E_8^a E_{24}^b E_{32}^c E_{40}^d E_{48}^e$. Then the degree of $E_* E_{56} W_{g_{24}}$ is at most 128 and this element is in $\widetilde{\mathfrak{E}}$.

The case $e = 1,\ f = 0$. If one of $b,\ c,\ d$ is not zero, we shall denote by E_* one of $E_{24},\ E_{32},\ E_{40}$ appearing in $E_8^a E_{24}^b E_{32}^c E_{40}^d$. The degree of $E_* E_{48} W_{g_{24}}$ is at most 112 and it is an element of $\widetilde{\mathfrak{E}}$. If $b = c = d = 0$, then a is at least 2 and $E_8^2 E_{48} W_{g_{24}}$ is in $\widetilde{\mathfrak{E}}$.

The case $d = 1,\ e = f = 0$. If one of $b,\ c$ is not zero, we take E_* appearing in $E_{24}^b E_{32}^c$. The degree of $E_* E_{40} W_{g_{24}}$ is at most 96 and it is an element of $\widetilde{\mathfrak{E}}$. If $b = c = 0$, then a is at least 3 and $E_8^3 E_{48} W_{g_{24}}$ is in $\widetilde{\mathfrak{E}}$.

The case $c = 1,\ d = e = f = 0$. If $b = 2$, then the degree of $E_{24}^2 E_{32} W_{g_{24}}$ is 104 and $E_{24}^2 E_{32} W_{g_{24}}$ is in $\widetilde{\mathfrak{E}}$. If $b = 1$, then a is at least 1. The degree of $E_8 E_{24} E_{32} W_{g_{24}}$ is 88 and $E_8 E_{24} E_{32} W_{g_{24}}$ is in $\widetilde{\mathfrak{E}}$. If $b = 0$, then a is at least 4. The degree of $E_8^4 E_{32} W_{g_{24}}$ is 88 and it is in $\widetilde{\mathfrak{E}}$.

The case $b = 2, c = d = e = f = 0$. a is at least 2. The degree of $E_8^2 E_{24}^2 W_{g_{24}}$ is 88 and φ is in $\widetilde{\mathfrak{E}}$.

The case $b = 1, c = d = e = f = 0$. a is at least 5. The degree of $E_8^5 E_{24} W_{g_{24}}$ is 88 and φ is in $\widetilde{\mathfrak{E}}$.

The case $b = c = d = e = f = 0$. This case can not occur.

II) Put $\varphi = E_8^a E_{24}^b E_{32}^c E_{40}^d E_{48}^e E_{56}^f E_{64}^g E_{72}^h E_{80}^i E_{96}^j W_{g_{24}}^2$ and assume that $\deg \varphi \geq 88$. If one of

$$a \geq 5,\ b \geq 2,\ c \geq 2,\ d \geq 1,\ e \geq 1,\ f \geq 1,\ g \geq 1,\ h \geq 1,\ i \geq 1,\ j \geq 1$$

holds, then φ is a product of an element of $\widetilde{\mathfrak{E}}$ with one of

$$E_8^5 W_{g_{24}}^2,\ E_{24}^2 W_{g_{24}}^2, E_{32}^2 W_{g_{24}}^2,\ E_{40} W_{g_{24}}^2,\ E_{48} W_{g_{24}}^2,$$
$$E_{56} W_{g_{24}}^2,\ E_{64} W_{g_{24}}^2,\ E_{72} W_{g_{24}}^2,\ E_{80} W_{g_{24}}^2,\ E_{96} W_{g_{24}}^2.$$

The degrees of $E_8^5 W_{g_{24}}^2,\ \ldots,\ E_{96} W_{g_{24}}^2$ are at most 144 and all of them are in $\widetilde{\mathfrak{E}}$. Consequently φ is an element of $\widetilde{\mathfrak{E}}$. Suppose, therefore, that $a \leq 4,\ b \leq 1,\ c \leq 1$ and $c = d = e = f = h = i = j = 0$.

The case $c = 1$. One of a, b is not zero. The degrees of $E_8 E_{32} W_{g_{24}}^2, E_{24} E_{32} W_{g_{24}}^2$ are 88, 104, respectively. So φ is in $\widetilde{\mathfrak{E}}$.

The case $b = 1,\ c = 0$. a is at least 2 and the degree of $E_8^2 E_{24} W_{g_{24}}^2$ is 88. φ is in $\widetilde{\mathfrak{E}}$.

The case $b = c = 0$. This case can not occur.

III) Put $\varphi = E_8^a E_{24}^b E_{32}^c E_{40}^d E_{48}^e E_{56}^f E_{64}^g E_{72}^h E_{80}^i E_{96}^j W_{g_{24}}^3$ and assume that $\deg \varphi \geq 88$. If one of

$$a \geq 2,\ b \geq 1,\ c \geq 1,\ d \geq 1,\ e \geq 1,\ f \geq 1,\ g \geq 1,\ h \geq 1,\ i \geq 1,\ j \geq 1$$

holds, then φ is a product of an element of $\widetilde{\mathfrak{E}}$ with one of

$$E_8^2 W_{g_{24}}^3,\ E_{24} W_{g_{24}}^3, E_{32} W_{g_{24}}^3,\ E_{40} W_{g_{24}}^3,\ E_{48} W_{g_{24}}^3,$$
$$E_{56} W_{g_{24}}^3,\ E_{64} W_{g_{24}}^3,\ E_{72} W_{g_{24}}^3,\ E_{80} W_{g_{24}}^3,\ E_{96} W_{g_{24}}^3.$$

The degrees of $E_8^2 W_{g_{24}}^3, \ \ldots, \ E_{96} W_{g_{24}}^3$ are at most 168 and all of them are in $\widetilde{\mathfrak{E}}$. Therefore φ is an element of $\widetilde{\mathfrak{E}}$. The remaining case, that is, $a \leq 1$ and $b = c = d = e = f = h = i = j = 0$, can not occur.

By what we have proved, we get $\widetilde{\mathfrak{E}_w} = \mathfrak{E}_w = \mathfrak{W}_w$ for any $w \geq 88$. We have thus obtained the following

THEOREM. *The graded ring of Eisenstein polynomials in genus* 2 *is minimally generated over* $\mathbf{C}$ *by the ten Eisenstein polynomials of degrees*

$$8, \ 24, \ 32, \ 40, \ 48, \ 56, \ 64, \ 72, \ 80, \ 96.$$

For $w = 24, 32, \ldots, 80$*, the vector space* $\mathfrak{E}_w$ *is strictly smaller than the vector space* $\mathfrak{W}_w$ *and the dimensions of these* $\mathfrak{E}_w$*'s are*

$$2, \ 3, \ 4, \ 6, \ 8, \ 11, \ 15, \ 20.$$

For $w = 0, 8, 16$ *and* $w \geq 88$*, the vector space* $\mathcal{E}_w$ *coincides with the vector space* $\mathfrak{W}_w$*.*

Acknowledgement. This note was written during the author's stay in RWTH Aachen. He would like to thank Professor Gabriele Nebe for the hospitality.

REFERENCES

[1] Broué, M., Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant +1, Discrete Math. 17, 247-269 (1977).

[2] Cannon, J., et al., The Magma Computational Algebra System for Algebra, Number Theory and Geometry. http://magma.maths.usyd.edu.au/magma/

[3] Conway, J.H., Pless, V., On the enumeration of self-dual codes, J. Comb. Theory, Ser. A 28, 26-53 (1980).

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

[5] Duke, W., On codes and Siegel modular forms, Int. Math. Res. Not. 1993, No.5, 125-136 (1993).

[6] Huffman, W.C., Pless, V., Fundamentals of error-correcting codes, Cambridge University Press (2003).

[7] Igusa, J., On Siegel modular forms of genus two, Am. J. Math. 84, 175-200 (1962).

[8] Igusa, J., On the graded ring of theta-constants, Am. J. Math. 86, 219-246 (1964).

[9] MacWilliams, F.J., Sloane, N.J.A., The theory of error-correcting codes, Part I and II, North-Holland Mathematical Library (1977).

[10] MacWilliams, F.J., Sloane, N.J.A., Thompson, J.G., Good code exist, Good self dual codes exist, Discrete Math. 3, 153-162 (1972).

[11] Nebe, G., Kneser-Hecke-operators in coding theory, Abh. Math. Semin. Univ. Hamb. 76, 79-90 (2006).

[12] Nebe, G., Rains, E.M., Sloane, N.J.A., Self-dual codes and invariant theory, Algorithms and Computation in Mathematics 17, Berlin: Springer (2006).

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

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

[15] Pless, V., Introduction to the theory of error-correcting codes, 3rd ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, Chichester: John Wiley & Sons (1998).

[16] Runge, B., On Siegel modular forms II, Nagoya Math. J. 138, 179-197 (1995).

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

[18] Rains, E.M., Sloane, N.J.A., Self-dual codes, Pless, V. S. (ed.) et al., Handbook of coding theory, Amsterdam: Elsevier, 177-294 (1998).

[19] Serre, J.-P., Cours d'arithmétique, Presses Universitaires de France (1970).

[20] Siegel, C.L., Über die analytische Theorie der quadratischen Formen, Ann. Math. (2) 36, 527-606 (1935).

[21] Witt, E., Eine Identität zwischen Modulformen zweiten Grades, Abh. math. Sem. Hansische Univ. 14, 323-337 (1941).