EISENSTEIN POLYNOMIALS ASSOCIATED TO BINARY CODES

Manabu Oura

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

1. Introduction. Eisenstein series play important roles 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 dimension([20]. *cf.* [21], [19]). Another is that the ring $A(\Gamma_g)$ generated over the field $\mathbf{C}$ of complex numbers by modular forms of even weights for the full modular group in genus g is the normalization of the graded ring B_g generated over $\mathbf{C}$ by Eisenstein series. This might suggest that B_g is close to $A(\Gamma_g)$. In the two special cases $g = 1, 2$, we know that $A(\Gamma_g)$ coincides with B_g, however, this is no longer true for $g > 2$. See [7], [8].

The Eisenstein polynomial in 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. By analogy with Eisenstein series, it is natural to investigate the ring $\mathfrak{E}^{(g)}$ generated over $\mathbf{C}$ by Eisenstein polynomials. It is a subring of the ring $\mathfrak{W}^{(g)}$ generated over $\mathbf{C}$ by weight enumerators of Type II codes. In the first case $g = 1$, these two rings coincide but this does not hold if $g \geq 2$. The objective of this note is to determine $\mathfrak{E}^{(2)}$. We shall show that $\mathfrak{E}^{(2)}$ *is minimally generated by the ten Eisenstein polynomials of degrees*

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

and coincides with $\mathfrak{W}^{(2)}$ *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 variables 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

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

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 x^A of degree n. The above definition of the Eisenstein polynomials is formal and their meaning does not become 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 the other after some coordinate permutation. Up to this equivalence, the Type II codes are classified for $n = 8,\ 16,\ 24,\ 32$ ([13], [15], [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 by [17] (*cf.* [1], [18]) 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

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

We refer to [9], [14], [6] for the general theory of codes. See also [11] in which the Eisenstein polynomial plays an important role.

3. Ring generated by Eisenstein polynomials. Before restricting ourselves to the case $g = 2$, we observe that $\mathfrak{E}^{(g)} = \mathfrak{W}^{(g)}$ holds if and only if $g = 1$. In fact, the two algebraically independent Eisenstein polynomials $E_{1,8}$ and $E_{1,24}$ generate $\mathfrak{W}^{(1)}$. As we shall see later, the two rings do not coincide for $g = 2$. In the case $g \geq 3$, the dimension of the vector space of spanned by the weight enumerators of Type II codes of length 24 is at least 5 by [16](see also [17], [11]), whereas there are only 3 products of Eisenstein polynomials of degree 24. Therefore the 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 Eisenstein polynomials, the ring generated over $\mathbf{C}$ by 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 the five elements of degrees 8, 24, 24, 32, 40 and has the dimension formula

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

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 $w = 88,\ 96,\ \ldots,\ 168$.

It is enough to consider monomials

$$\varphi = E_8^a E_{24}^b E_{32}^c E_{40}^d E_{48}^e E_{56}^f E_{64}^g E_{72}^h E_{80}^i E_{96}^j W_{g_{24}}^k, \text{ for } k = 1, 2, 3$$

and we shall show that each monomial of degree ≥ 88 is contained in $\widetilde{\mathfrak{E}}$. For each $k = 1, 2, 3$ we argue[1] by induction and assume that φ is a minimal counterexample of degree $n \geq 88$. Then $n \geq 176$ since $\widetilde{\mathfrak{E}}_w = \mathfrak{W}_w$ for $w = 88, \ldots, 168$ by calculation. Either $\varphi = E_\ell F$ for some Eisenstein polynomial E_ℓ of degree $\ell = 8, 24, \ldots, 80$ or $\varphi = E_{96}^j W_{g_{24}}^k$. In the first case the degree of F is

$$n - \ell \geq n - 80 \geq 176 - 80 = 96 > 88$$

hence by minimality of φ we have $F \in \widetilde{\mathfrak{E}}$ and then also $\varphi \in \widetilde{\mathfrak{E}}$. In the second case $\varphi = E_{96}^{j-1} F$ has a factor $F = E_{96} W_{g_{24}}^k$ of degree

$$88 < 96 + 24k \leq 96 + 72 = 168$$

which lies in $\widetilde{\mathfrak{E}}$, hence also $\varphi \in \widetilde{\mathfrak{E}}$.

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

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

[1] The following argument was suggested by the referee. The author's original contained extra computations.

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 Prof. Gabriele Nebe for the hospitality. He would also like to thank Prof. Nebe and the referee for the comments on this note.

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

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

[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).