Eisenstein polynomials associated to binary codes (II)

Dedicated to the memory of Professor Hidehisa Naganuma

Manabu Oura

Abstract: In the first paper we determined the generators of the ring of Eisenstein polynomials in genus 2, those of which are described in terms of coding theory. In this second paper we go beyond coding theory and clarify the ring of Eisenstein polynomials in arbitarary genus from invariant theory.

1. Introduction. There exist extensive, connected studies between theory of modular forms and that of combinatorics, however, we miss the corresponding theory of Eisenstein series from the combinatorial side. Our approach of the series of papers will give a step to fill this gap. The main theme of this second paper is to clarify the properties of the graded ring of Eisenstein polynomials in connection with the invariant theory which is free from coding theory.

To explain our approach, or to help for the reader to understand the meaning of our work, we shall recall the theory of Eisenstein series from our standpoint. Let g be a positive integer. We denote by Γ_g the integral symplectic group $Sp(g, \mathbf{Z})$ and by $\Gamma_{g,0}$ the subgroup of Γ_g consisting of the elements of Γ_g with left bottom blocks equal to zero. Then Eisenstein series could be defined as

$$\psi_k^{\Gamma_g}(\tau) = \sum \det(c\tau + d)^{-k}$$

for even $k > g + 1$ in which the summation is extended over elements of Γ_g composed of $a,\ b,\ c,\ d$ modulo left multiplications of elements of $\Gamma_{g,0}$. This gives a Siegel modular forms of weight k for Γ_g. Here we take up two properties of this series. First the Eisenstein series could be written as the weighted sum of the theta series of all classes of even unimodular lattices in rank $2k \equiv 0 \pmod 8$. This is a consequence of *Siegel's Hauptsatz*. Secondly

---

key words: Eisenstein polynomial, normalization
Mathematics Subject Classification: Primary 11T71; Secondary 11F46
running title: Eisenstein polynomial

the ring of Siegel modular forms of even weights for Γ_g is the normalization of the ring of Eisenstein series in its field of fractions. This also comes from the work of Siegel. At any rate Eisenstein series are singled out by their importance in the theory of modular forms.

Throughout our investigations, we always have in mind the following dictionary, which might be helpful for the reader. The notations will be explained in the next section.

$$\begin{aligned} \text{“infinite world”} &\longleftrightarrow \text{“finite world”} \\ \Gamma_g &\longleftrightarrow H_g \\ \text{Siegel modular form} &\longleftrightarrow H_g\text{-invariant polynomial} \\ \text{Eisenstein series} &\longleftrightarrow \text{Eisenstein polynomial} \\ \text{lattice} &\longleftrightarrow \text{code} \end{aligned}$$

2. Definition of Eisenstein polynomial and its first properties. Let g be a positive integer. Here we assume that entries of each element of $GL(2^g, \mathbf{C})$ are indexed by the elements of $\mathbf{F}_2^g$. A subgroup D_g of $GL(2^g, \mathbf{C})$ is generated by $\mathrm{diag}(i^{{}^t aSa} : \ a \in \mathbf{F}_2^g)$ for all $S = {}^tS \in \mathrm{Mat}_{g\times g}(\mathbf{Z})$. We denote by H_g, which was studied in [8], a finite subgroup of $GL(2^g, \mathbf{C})$ generated by D_g and

$$\left(\frac{1+i}{2}\right)^g \left((-1)^{a\cdot b}\right)_{a,b\in\mathbf{F}_2^g}.$$

The group H_g contains the subgroups

$$\mathbf{F}_2^g, \ GL(g, \mathbf{F}_2)$$

under appropriate embeddings. As entries of each element of H_g are indexed by the ordered elements of $\mathbf{F}_2^g$, such a matrix naturally acts on the polynomial ring $\mathbf{C}[x] = \mathbf{C}[x_a : a \in \mathbf{F}_2^g]$. An Eisenstein polynomial of weight ℓ for H_g is, by definition,

$$\varphi_\ell^{H_g}(x) = \frac{1}{|H_g|} \sum_{\sigma\in H_g} (\sigma x_0)^\ell.$$

From the definition we see that $\varphi_\ell^{H_g}(x)$ is an element of the invariant ring $\mathbf{C}[x]^{H_g}$. Let K_g be a stabilizer of x_0 in H_g which is generated by $GL(g, \mathbf{F}_2)$

and D_g. The group K_g corresponds to $\Gamma_{g,0}$. It is easy to see that

$$\varphi_\ell^{H_g}(x) = \frac{|K_g|}{|H_g|} \sum_{K_g \backslash H_g \ni \sigma} (\sigma x_0)^\ell$$

and we put

$$k_g = |K_g \backslash H_g| = 2^{2+g}(2^g+1)(2^{g-1}+1)\cdots(2^1+1).$$

Here we only mention that this is nothing else but the number of the minimal vectors of Barnes-Wall lattice in dimension 2^{g+1}. We note

$$\begin{aligned}
|H_g| &= 2^{g^2+2g+2}(4^g-1)(4^{g-1}-1)\cdots(4^1-1),\\
|K_g| &= |D_g| \cdot |GL(n, \mathbf{F}_2)|\\
&= 4^g 2^{(g-1)g/2} \cdot 2^{(g-1)g/2}(2^g-1)(2^{g-1}-1)\cdots(2^1-1)\\
&= 2^{g^2+g}(2^g-1)(2^{g-1}-1)\cdots(2^1-1).
\end{aligned}$$

The explicit values of $k_g = |H_g|/|K_g|$ for $g = 1, 2, 3, 4$ are

$$24 = \frac{96}{4},\ 240 = \frac{4680}{192},\ 4320 = \frac{371589120}{86016},\ 146880 = \frac{48514675507200}{330301440}.$$

We add one more finite group. Let G_g be a finite subgroup of $GL(2^g, \mathbf{C})$ generated by H_g and the 8th root of unity. The index of H_g in G_g is 2. Invariant theory of G_g works well in coding theory as we shall recall. The weight enumerator $W_C^g(x)$ of a binary code C in genus g is defined by

$$W_C^g(x) = \sum_{v_1,\ldots,v_g \in C} \prod_{a \in \mathbf{F}_2^g} x_a^{n_a(v_1,\ldots,v_g)}$$

where $n_a(v_1, \ldots, v_g)$ denotes the number of i such that $a = (v_{i1}, \ldots, v_{ig})$. It is then 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 G_g. This theorem started with Gleason [1]. See [6]. Note that the invariant ring of arbitrary finite group is integrally closed.

Till the end of this section we assume $\ell \equiv 0 \pmod 8$. Applying Theorem 6.3 in [5] to the doubly even code generated by all one vector, we have

$$\begin{aligned}
\frac{2^g}{|G_g|} \sum_{\sigma \in G_g} (\sigma x_0)^\ell &= \prod_{0 \le i < \ell/2-1} (2^g + 2^i)^{-1} \sum_C W_C^g(x)\\
&= \prod_{0 \le i < \ell/2-1} (2^g + 2^i)^{-1} \sum_{[C]} \frac{\ell!}{|\mathrm{Aut}C|} W_C^g.
\end{aligned}$$

The summation over C means that C runs through all Type II codes of length ℓ, while that over $[C]$ through all classes of Type II codes of length ℓ. Since the sum $\frac{1}{|G_g|}\sum_{\sigma\in G_g}(\sigma x_0)^\ell$ is $\varphi_\ell^{H_g}(x)$, we get *Siegel's Hauptsatz in coding theory*:*

$$\varphi_\ell^{H_g}(x) = \frac{\ell!}{2^g\prod_{0\le i<\ell/2-1}(2^g+2^i)}\sum_{[C]}\frac{1}{|\mathrm{Aut}C|}W_C^g(x).$$

From this formula we see that $\varphi_\ell^{H_g}$ does not vanish for $\ell \equiv 0 \pmod 8$. Siegel's Φ-operator in number theory could be also considered in our context (*cf.* [8]). Applying our "Φ-operator"

$$\Phi(x_{(a_1a_2\cdots a_g)}) = \begin{cases} x_{(a_1a_2\ldots a_{g-1})} & a_g = 0 \\ 0 & a_g = 1 \end{cases}$$

to the formula, we get

$$\Phi(\varphi_\ell^{H_g}(x)) = \frac{1}{2}\cdot\frac{2^{g-\ell/2+1}+1}{2^g+1}\varphi_\ell^{H_{g-1}}(x).$$

3. Ring of Eisenstein polynomial. In this section the graded ring of Eisenstein polynomials is studied. We shall start with the following finiteness theorem, which is a consequence of the fundamental theorem of symmetric polynomials.

Theorem 1. (1) The ring $\mathbf{C}[\varphi_\ell^{H_g}(x)]$ of Eisenstein polynomials is finitely generated over $\mathbf{C}$.

(2) The ring $\mathbf{C}[\varphi_\ell^{H_g}(x) : \ \ell \equiv 0 \pmod 8]$ of Eisenstein polynomials of weights divisible by 8 is finitely generated over $\mathbf{C}$.

In order to obtain the normalization type theorem, we shall prepare two lemmata.

Lemma 2. $\mathbf{C}[x]^{H_g}$ is integral over $\mathbf{C}[\varphi_\ell^{H_g}(x)]$.

*This formula seems to be known to some experts including Professor A.Munemasa [4].

Proof. First we recall that

$$\sum_{j=1}^{r} z_j^k = 0,\ k = 1, 2, \ldots, r$$

have no common zero other than $z_1 = z_2 = \cdots = z_r = 0$. We apply this to our case. Suppose that $\varphi_{8\cdot 1}(x) = \varphi_{8\cdot 2}(x) = \cdots = \varphi_{8k_g}(x) = 0$, where $k_g = |H_g|/|K_g|$. Since H_g contains $\mathbf{F}_2^g$, $\sigma(x_0) = x_a = 0$ for $\sigma = a \in \mathbf{F}_2^g$. This completes the proof of Lemma 2.

In some parts of the following, we assume non-vanishingness of certain Eisenstein polynomial. This seems very likely true, however, the author does not have its proof in his hand. We give it as a conjecture.

Conjecture: there exists a non-vanishing Eisenstein polynomial of weight $\not\equiv 0 \pmod 8$.

Lamma 3. Assume that Conjecture is true. Then the field of fractions of $\mathbf{C}[\varphi_\ell^{H_g}]$ coincides with the field of fractions of $\mathbf{C}[x]^{H_g}$.

Proof. This is a consequence of Corollary 4.4 in [5]. On the treatment of the graded ring, we refer to [2]. For the graded ring S, we denote by $S^{(d)}$ generated by elements of degrees multiple of d. A quotient field of S is written as $F(S)$ and its degree 0 part as $F_0(S)$.

The Galois group of the extension $\mathbf{C}(x)/\mathbf{C}(x)^{G_g}$ is G_g. If we take an element of σ from the automorphism group of $\mathbf{C}(x)/\mathbf{C}(\varphi_\ell^{H_g})$, then σ should preserve φ_8. By the mentioned corollary, σ is an element of G_g. As a consequence, we have $\mathbf{C}(x)^{G_g} = \mathbf{C}(\varphi_\ell^{H_g} :\ \ell \equiv 0 \pmod 8)$. Write S for $\mathbf{C}[x]^{H_g}$ and take a weight 4 element ξ from $F(S)$.

$$\begin{aligned}
\mathbf{C}(x)^{H_g} &= F(\mathbf{C}[x]^{H_g}) \\
&= F(S) \\
&= F_0(S)(\xi) \\
&= F_0(S^{(8)})(\xi) \\
&= F_0(\mathbf{C}(\varphi_\ell^{H_g}(x) : \ell \equiv 0 \pmod 8)))(\xi) \\
&= F_0(\mathbf{C}(\varphi_\ell^{H_g}))(\xi) \\
&= \mathbf{C}(\varphi_\ell^{H_g})
\end{aligned}$$

This completes the proof of Lemma 3.

Combining the lemmata above, we get

Theorem 4. Assume that Conjecture is true. Then the invariant ring $\mathbf{C}[x]^{H_g}$ of the finite group H_g is the normalization of the ring $\mathbf{C}[\varphi_\ell^{H_g}]$ of Eisenstein polynomials in its field of fractions.

The following "Theorem" could be obtained as "Corollary" of Theorem 4 if we drop the assumption in Theorem 4. The proof is the same as that of Theorem 4.

Theorem 5. The ring $\mathbf{C}[x]^{G_g}$ of the weight enumerators of Type II codes is the normalization of $\mathbf{C}[\varphi_\ell^{H_g} : \ell \equiv 0 \pmod 8]$ in its field of fractions.

4. Concluding remarks. (1) For $g = 1, 2$, the ring $\mathbf{C}[x_a]^{H_g}$ could be generated by Eisenstein polynomials. In our paper [7], we gave the generators of $\mathbf{C}[\varphi_\ell^{H_2} : \ell \equiv 0 \pmod 8]$, the weights ℓ of which are

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

This ring is strictly smaller than $\mathbf{C}[x]^{G_2}$ and Theorem 5 says that if we take the normalization, we get the whole ring $\mathbf{C}[x]^{G_2}$. In order to see this, take the Golay code g_{24} of length 24. If we add the weight enumerator $W_{g_{24}}^2$ to the ring of Eisenstein polynomial, we get the whole ring. This means that $W_{g_{24}}^2$ is integral over the ring of Eisenstein polynomial and is contained in the field of Eisenstein polynomials. It is easy to find such isobaric polynomials P, Q, P', Q' as, omitting H_2 in the notation of $\varphi_\ell^{H_2}$,

$$(W_{g_{24}}^2)^2 + P(\varphi_8, \varphi_{24})W_{g_{24}}^2 + Q(\varphi_8, \varphi_{24}, \varphi_{32}, \varphi_{40}, \varphi_{48}) = 0,$$
$$W_{g_{24}}^2 = P'(\varphi_8, \varphi_{24}, \varphi_{32}, \varphi_{40}, \varphi_{48}, \varphi_{56})/Q'(\varphi_8, \varphi_{24}, \varphi_{32}).$$

(2) The approach of this paper suggests the theory of Eisenstein polynomials for arbitrary finite group. Along this line Yano [9] studied the rings of Eisenstein polynomials for finite unitary reflection groups.

(3) Suppose $g = 1$. Under the theta map, an Eisenstein polynomial is transformed into a modular form for $SL(2, \mathbf{Z})$. Due to some computations, the derived modular forms seem to enjoy properties similar to Eisenstein

series. For further investigations of Eisenstein polynomials, consult Miezaki [3].

Acknowledgment. The author would like to thank a referee for helpful comments. He was partially supported by JSPS KAKENHI (C) 25400014.

References

[1] Gleason, A.M., Weight polynomials of self-dual codes and the MacWilliams identities. Actes du Congrs International des Mathmaticiens (Nice, 1970), Tome 3, pp. 211215. Gauthier-Villars, Paris, 1971.

[2] Igusa, J., Theta functions, Die Grundlehren der mathematischen Wissenschaften, Band 194. Springer-Verlag, New York-Heidelberg, 1972.

[3] Miezaki, T., in preparation.

[4] Munemasa, A., Codes, invariant polynomials and modular forms(in japanese), The first spring conference "The rings of automorphic forms" (Organizers:T.Ibukiyama, et al.), Hamana lake, Japan, 2002, 135–161.

[5] Nebe, G., Rains, E., Sloane, N.J., The invariants of the Clifford groups. Des. Codes Cryptogr. 24 (2001), no. 1, 99–121.

[6] Nebe, G., Rains, E., Sloane, N.J., Self-dual codes and invariant theory. Algorithms and Computation in Mathematics, 17. Springer-Verlag, Berlin, 2006.

[7] Oura, M., Eisenstein polynomials associated to binary codes, Int. J. Number Theory 5(2009), no.4, 635–640.

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

[9] Yano, S., Master thesis, Kochi University (2011).

Department of Mathematics
Kochi University
Akebono-cho 2-5-1
Kochi, 780-8520

Japan
email: oura@kochi-u.ac.jp

Current address:
Division of Mathematical and Physical Sciences
Graduate School of Natural Science and Technology
Kanazawa University
Kakuma-machi, Kanazawa
Ishikawa 920-1192
Japan
email: oura@se.kanazawa-u.ac.jp