DUALITY OF CODES AND THETA FUNCTIONS

SHIGETO NISHIMURA

Received May 29, 2000

ABSTRACT. The weight enumerators of the doubly even selfdual codes change to modular forms by substituting of theta functions of the lattice $\sqrt{2}\mathbf{Z}$ to their variables. In this paper we present the background informations about the connection between weight enumerators of codes and modular forms based on the inversion formula of theta functions of an integral lattice.

1 Introduction Let Γ be a lattice in $\mathbf{R}^n$ and Γ^* be the dual lattice of Γ. Theta functions of the lattice Γ are defined by

$$\vartheta_{\rho+\Gamma}(\tau) = \sum_{x\in\Gamma} e^{\pi i \tau (x+\rho)^2} \quad (\rho \in \mathbf{R}^n).$$

Ordinarily it indicates only the series for $\rho = 0$ but we include translated ones for convenient. Under the assumption that Γ is integral and ρ is chosen from Γ^*, its inversion formula can be written by

$$\vartheta_{\rho+\Gamma}\left(-\frac{1}{\tau}\right) = \frac{1}{\mathrm{vol}(\mathbf{R}^n/\Gamma)} \cdot \left(\sqrt{\frac{\tau}{i}}\right)^n \sum_{\sigma\in\Gamma^*/\Gamma} \chi_\rho(\sigma)\vartheta_{\sigma+\Gamma}(\tau),$$

where $\chi_\rho(\sigma) = e^{2\pi i \sigma\cdot\rho}$ is a character of the finite abelian group Γ^*/Γ. For example, the formulas for $\Gamma = \sqrt{2}\mathbf{Z}$ are

$$\begin{aligned}
&\rho = 0; \quad \vartheta_{\sqrt{2}\mathbf{Z}}(-\tfrac{1}{\tau}) = (\tfrac{\tau}{i})^{\frac{1}{2}} \cdot \tfrac{1}{\sqrt{2}} \left(\vartheta_{\sqrt{2}\mathbf{Z}}(\tau) + \vartheta_{\frac{1}{\sqrt{2}}+\sqrt{2}\mathbf{Z}}(\tau)\right), \\
&\rho = \tfrac{1}{\sqrt{2}}; \quad \vartheta_{\frac{1}{\sqrt{2}}+\sqrt{2}\mathbf{Z}}(-\tfrac{1}{\tau}) = (\tfrac{\tau}{i})^{\frac{1}{2}} \cdot \tfrac{1}{\sqrt{2}} \left(\vartheta_{\sqrt{2}\mathbf{Z}}(\tau) - \vartheta_{\frac{1}{\sqrt{2}}+\sqrt{2}\mathbf{Z}}(\tau)\right).
\end{aligned}$$

Now, let C be a $[n,k]$ binary linear code. The weight enumerator for Hamming weight of C is the polynomial in 2 variables which is defined by

$$\begin{aligned}
W_C(X,Y) &= \sum_{i=0}^{n} A_i X^{n-i} Y^i, \\
A_i &= \#\{c \in C : w_H(c) = i\}
\end{aligned}$$

where $w_H(c) = \#\{i : c_i \neq 0\}$ is the Hamming weight of a codeword $c = (c_1, \cdots, c_n)$.

$(A_0, \cdots, A_n)$ is called the weight distribution of C. As a rough generalizations it is a key factor in calculating ratio of decoding error but often we are forced to compute it through the heavy process to count up the Hamming weight of every codewords. Thus the following

2000 *Mathematics Subject Classification.* 11T71,11F11.
Key words and phrases. theta functions of lattice, MacWilliams identity, selfdual codes.

identity by MacWilliams is the useful tool which yields the weight distribution of a high dimensional code from a low dimensional code([7]).

$$W_{C^\perp}(X,Y) = \frac{1}{2^k} W_C(X+Y, X-Y),$$

where $C^\perp$ is the dual code of C.

Now, there is the well-know construction of the lattice Γ_C from the code C by

$$\Gamma_C = \frac{1}{\sqrt{2}} \rho^{-1}(C) \text{ where } \rho : \mathbf{Z}^n \longrightarrow (\mathbf{Z}/2\mathbf{Z})^n \cong \mathbf{F}_2^n.$$

This construction is accompanied with the correspondences of some properties, that is, Γ_C is unimodular iff C is selfdual, and Γ_C is even iff C is doubly even. And it can be showed that

$$W_C\left(\vartheta_{\sqrt{2}\mathbf{Z}} \ , \ \vartheta_{\frac{1}{\sqrt{2}}+\sqrt{2}\mathbf{Z}} \right) = \vartheta_{\Gamma_C}.$$

Consequently, if C is a doubly even selfdual code, then $W_C\left(\vartheta_{\sqrt{2}\mathbf{Z}} \ , \ \vartheta_{\frac{1}{\sqrt{2}}+\sqrt{2}\mathbf{Z}} \right)$ is the theta function of the even unimodular lattice, which is to be a modular form. The above theorem by MacWilliams is just inversion formula of ϑ_{Γ_C}. Our concern is to establish the connnection between weight enumerators of codes and modular forms, by seizing the correspondence between a code and its dual as the duality of the finite abelian group Γ^*/Γ.

2 Duality of Codes Let G be a finite additive abelian group. A linear code with length n over G is a subgroup of G^n which is a direct sum of G. Taking $\Gamma = \sqrt{m}\mathbf{Z}$, $\Gamma^*/\Gamma \cong \mathbf{Z}/m\mathbf{Z}$ as an additive group holds for any positive integer m. Thus we can take an integral lattice Γ such that $G^n \cong \Gamma^*/\Gamma$ and take an isomorphism ϕ. Then the symmetric bilinear form $\phi(x) \cdot \phi(y) \bmod \mathbf{Z}$ is induced in G^n. We give the construction of the lattice by

$$\Gamma_C = \bigcup_{c \in C} \phi(c) + \Gamma.$$

Γ_C is a lattice iff C is a linear code. In other words, there is the one-to-one correspondence between the subgroups of G^n and the intermediate lattices Γ' such that $\Gamma \subset \Gamma' \subset \Gamma^*$. Hence there exists the subgroup which is particulary corresponded to the dual lattice Γ_C^*. Put

$$C_\phi^\perp = \{c' \in G^n : \phi(c') \cdot \phi(c) \in \mathbf{Z} \ for \ all \ c \in C\}$$

and we have $\Gamma_C^* = \Gamma_{C_\phi^\perp}$. It follows that Γ_C is unimodular iff $C = C_\phi^\perp$. The definition implies $C_\phi^\perp$ is the annihilator of the character group $\{\chi_{\phi(c)} : c \in C\}$, but we call it a *dual code* with respect to ϕ in aspect of coding theory.

Theorem 1

$$\vartheta_{\Gamma_{C_\phi^\perp}}(\tau) = \frac{1}{\#C} \sum_{c' \in G^n} \left(\sum_{c \in C} \chi_{\phi(c)}(\phi(c')) \right) \vartheta_{\phi(c')+\Gamma}(\tau)$$

(proof) It follows from the definition of Γ_C that $\vartheta_{\Gamma_C} = \sum_{c \in C} \vartheta_{\phi(c)+\Gamma}$. Therefore

$$\vartheta_{\Gamma_C}\left(-\frac{1}{\tau}\right) = \sum_{c \in C} \vartheta_{\phi(c)+\Gamma}\left(-\frac{1}{\tau}\right) = \frac{1}{\mathrm{vol}(\mathbf{R}^n/\Gamma)} \left(\sqrt{\frac{\tau}{i}}\right)^n \sum_{c \in C} \sum_{\sigma \in \Gamma^*/\Gamma} \chi_{\phi(c)}(\sigma) \vartheta_{\sigma+\Gamma}(\tau)$$

$$= \frac{1}{\#G^{\frac{n}{2}}}\left(\sqrt{\frac{\tau}{i}}\right)^n \sum_{\sigma\in\Gamma^*/\Gamma}\left(\sum_{c\in C}\chi_{\phi(c)}(\sigma)\right)\vartheta_{\sigma+\Gamma}(\tau)$$

$$= \frac{1}{\#G^{\frac{n}{2}}}\left(\sqrt{\frac{\tau}{i}}\right)^n \sum_{c'\in G^n}\left(\sum_{c\in C}\chi_{\phi(c)}(\phi(c'))\right)\vartheta_{\phi(c')+\Gamma}(\tau).$$

We connect this with the inversion formula of Γ_C. Since $\mathrm{vol}(\mathbf{R}^n/\Gamma) = |\Gamma^*/\Gamma|^{\frac{1}{2}} = \#G^{\frac{n}{2}}$, the volume of Γ_C is $\mathrm{vol}(\mathbf{R}^n/\Gamma_C) = \dfrac{1}{|\Gamma_C/\Gamma|}\mathrm{vol}(\mathbf{R}^n/\Gamma) = \dfrac{\#G^{\frac{n}{2}}}{\#C}$. Then we have

$$\vartheta_{\Gamma_C}\left(-\frac{1}{\tau}\right) = \frac{1}{\mathrm{vol}(\mathbf{R}^n/\Gamma_C)}\left(\sqrt{\frac{\tau}{i}}\right)^n \vartheta_{\Gamma_C^*}(\tau) = \frac{\#C}{\#G^{\frac{n}{2}}}\left(\sqrt{\frac{\tau}{i}}\right)^n \vartheta_{\Gamma_{C_\phi^\perp}}(\tau).$$

Finally we have

$$\vartheta_{\Gamma_{C_\phi^\perp}}(\tau) = \frac{1}{\#C}\sum_{c'\in G^n}\left(\sum_{c\in C}\chi_{\phi(c)}(\phi(c'))\right)\vartheta_{\phi(c')+\Gamma}(\tau).$$

■

Note that the correspondence in Theorem 1 between a code and its dual keeps the order of the elements of each codeword. It implies that the theorem may be regarded as the MacWilliams theorem for exact weight enumerator.

Let m be a natural number. We study the weight distribution of C and $C_\phi^\perp$ in case that Γ is the direct sum of $\sqrt{m}\mathbf{Z}$. When m is particularly replaced by a prime number p, the following results are for codes over a prime field with characteristic p. The settings are as follows.

$$\begin{array}{ccccc} \phi: & (\mathbf{Z}/m\mathbf{Z})^n & \longrightarrow & \Gamma^*/\Gamma \\ & \cup & & \cup \\ & \underset{i\text{-th}}{(0,\cdots,1,\cdots,0)} & \longmapsto & \underset{i\text{-th}}{\frac{1}{m}\boldsymbol{e}_i=(0,\cdots,\frac{1}{\sqrt{m}},\cdots,0)} \end{array}$$

We have $\phi(c) = \frac{c_1}{m}\boldsymbol{e}_1 + \cdots + \frac{c_n}{m}\boldsymbol{e}_n$ for a codeword $c = (c_1\cdots c_n)$. Thus we know $(c_1'\cdots c_n') \in C_\phi^\perp$ if and only if $c_1'c_1 + \cdots + c_n'c_n \equiv 0 \mod m$ for all $(c_1,\cdots,c_n)\in C$. When m is a prime number, this means $C_\phi^\perp = C^\perp$.

In this case we have

$$\vartheta_{\Gamma_C}(\tau) = \sum_{c\in C}\vartheta_{\phi(c)+\Gamma}(\tau) = \sum_{c\in C}\prod_{i=1}^n \vartheta_{\frac{c_i}{\sqrt{m}}+\sqrt{m}\mathbf{Z}}(\tau).$$

Collect the terms by notations of complete weight and we have

$$\vartheta_{\Gamma_C}(\tau) = \sum_{\boldsymbol{s}=(s_a)\in\mathbf{Z}^n} A(\boldsymbol{s})\prod_{a=0}^{m-1}\vartheta_{\frac{a}{\sqrt{m}}+\sqrt{m}\mathbf{Z}}(\tau)^{s_a},$$

$$A(\boldsymbol{s}) = \sharp\{c\in C : n(c) = \boldsymbol{s}\},$$
$$n(c) = (n_0,\cdots,n_{m-1}): \text{ the complete weight of } c,$$
$$n_j = \#\{i : c_i \equiv j \mod m\ \}.$$

Replacing τ by $-\dfrac{1}{\tau}$ and applying for the both hands the inversion formulas, we see that

$$\vartheta_{\Gamma_{C_\phi^\perp}}(\tau) = \frac{1}{m^k}\sum_{\boldsymbol{s}} A(s)\prod_{a=0}^{m-1}\left(\sum_{b=0}^{m-1} e^{\frac{2\pi i}{m}ab}\vartheta_{\frac{a}{\sqrt{m}}+\sqrt{m}\mathbf{Z}}(\tau)\right)^{s_a}.$$

It may happen $\vartheta_{\Gamma_{C_1}} = \vartheta_{\Gamma_{C_2}}$ in spite of $C_1 \neq C_2$, since $\vartheta_{\frac{a}{\sqrt{m}}+\sqrt{m}\mathbf{Z}}$ $(a = 0, 1, \cdots, m-1)$ are not always algebraic independent. Replacing $\vartheta_{\frac{a}{\sqrt{m}}+\sqrt{m}\mathbf{Z}}$ by variable X_a, the codes are corresponded to different polynomials in X_a and the above formula changes into the identity which transforms the complete weight enumerator of a code C,

$$W_C(X_0, X_1, \cdots, X_{m-1}) = \sum_{\boldsymbol{s}} A(\boldsymbol{s}) X_0^{s_0} X_1^{s_1} \cdots X_{m-1}^{s_{m-1}}$$

to the complete weight enumerator of its dual code as follows.

Proposition 1 *Let C be a code over $\mathbf{Z}/m\mathbf{Z}$. Then*

$$W_{C_\phi^\perp}(X_0, X_1, \cdots, X_{m-1}) = \frac{1}{\#C} W_C\left(\sum_{a=0}^{m-1} X_a,\ \sum_{a=0}^{m-1} e^{\frac{2\pi i}{m}a} X_a,\ \cdots,\ \sum_{a=0}^{m-1} e^{\frac{2\pi i}{m}(m-1)a} X_a\right).$$

3 Modular Forms In this section we study ϑ_{Γ_C} as modular form. Recall that $\mathrm{SL}_2(\mathbf{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. For their actions by linear fractional transfromations, ϑ_{Γ_C} satisfies

$$\vartheta_{\Gamma_C}(S\tau) = \left(\sqrt{\frac{\tau}{i}}\right)^n \vartheta_{\Gamma_C}(\tau) \text{ iff } C = C_\phi^\perp,$$

$$\vartheta_{\Gamma_C}(T^N\tau) = \sum_{c\in C} \vartheta_{\phi(c)+\Gamma}(\tau + N) = \sum_{c\in C}\sum_{x\in\Gamma} e^{\pi i \tau (x+\phi(c))^2} \cdot e^{N\pi i (x^2+\phi(c)^2)}.$$

Note that $\phi(c)^2 \in \mathbf{Z}$ holds iff $C \subset C_\phi^\perp$. Thus we know modular invariance of ϑ_{Γ_C}.

Proposition 2 *Let $C = C_\phi^\perp$ with length $n \equiv 0 \bmod 8$. Then ϑ_{Γ_C} is a modular form of weight $\frac{n}{2}$ for the congruent subgroup of level 2 generated by S, T^2. If Γ is particularly an even lattice and $\phi(c)^2 \in 2\mathbf{Z}$ for all $c \in C$, ϑ_{Γ_C} is a modular form for $\mathrm{SL}_2(\mathbf{Z})$ of weight $\frac{n}{2}$.*

When Γ is the direct sum of $\sqrt{2}\mathbf{Z}$, $\phi(c)^2$ is equal to the half of the Hamming weight of c. That is why the weight enumerators of the binary doubly even selfdual codes have connection with modular forms for $\mathrm{SL}_2(\mathbf{Z})$. As generalization of such codes, selfdual codes over $\mathbf{Z}/2k\mathbf{Z}$ with $\phi(c)^2 \in 2\mathbf{Z}$ are named Type II([2]).

Denote a prime field with characteristic p by $\mathbf{F}_p$. We show that selfdual codes over $\mathbf{F}_p$ are related to modular forms when $p \equiv 3 \bmod 4$, .

Lemma 1 *Let $k/\mathbf{Q}$ is a Galois extension field and $\mathcal{P}$ is a prime ideal lying over p. Denote the trace of x by $\mathrm{Tr}_{k/\mathbf{Q}}(x)$. If the decomposition field $k_Z = \mathbf{Q}$, then*

$$\left\{\mathrm{Tr}_{k/\mathbf{Q}}(x) : x \in \mathcal{P}\right\} \subset p\mathbf{Z}.$$

(proof) Take an arbitary $x \in \mathcal{P}$ and an arbitary $\sigma \in Gal(k/\mathbf{Q})$. Since the decomposition group is equal to $Gal(k/\mathbf{Q})$, $\mathrm{Tr}_{K/\mathbf{Q}}(x) \in \mathcal{P}$. Thus $\mathrm{Tr}_{K/\mathbf{Q}}(x) \in \mathcal{P} \cap \mathbf{Z} = p\mathbf{Z}$. ■

Take $k = \mathbf{Q}(\sqrt{-p})$ and $\mathcal{P} = (\sqrt{-p})$. Since p is ramified, $\mathcal{O}_k/\mathcal{P} \cong \mathbf{F}_p$ where $\mathcal{O}_k$ is the integer ring of k. The reduction map of $\mathcal{O}_k$ is given by

$$\begin{array}{ccc} \mathcal{O}_k & \longrightarrow & \mathcal{O}_k/\mathcal{P} \\ \cup & & \cup \\ a + b\omega & \mapsto & a + \frac{b}{2} \bmod p \end{array}$$

where 1, $\omega = \frac{1+\sqrt{-p}}{2}$ are the integral basis and $\frac{1}{2}$ means the inverse element of 2 in $\mathbf{F}_p$.

The positive definite symmetric bilinear form on $\mathcal{O}_k$ is defined by

$$(x,y) := \mathrm{Tr}_{k/\mathbf{Q}}\left(\frac{x\bar{y}}{p}\right) = \frac{1}{p}(x\bar{y}+\bar{x}y) \quad (x,y \in \mathcal{O}_k)$$

where $\bar{x}$, $\bar{y}$ is the complex conjugate. Since

$$(x,x) = \frac{2}{p}\left(a^2+ab+(\frac{p+1}{4})b^2\right) \qquad (x = a+b\omega),$$

$\mathcal{P}$ with this form is an even integral lattice by Lemma 1. Since

$$\#\mathcal{P}^*/\mathcal{P} = \det\begin{pmatrix} (\sqrt{-p},\sqrt{-p}) & (\sqrt{-p},\frac{-p+\sqrt{-p}}{2}) \\ (\frac{-p+\sqrt{-p}}{2},\sqrt{-p}) & (\frac{-p+\sqrt{-p}}{2},\frac{-p+\sqrt{-p}}{2}) \end{pmatrix} = p$$

and the inclusion $\mathcal{O}_k \subset \mathcal{P}^*$ follows from Lemma 1, the dual lattice of $\mathcal{P}$ is $\mathcal{O}_k$. Therefore we have $\mathcal{P}^*/\mathcal{P} = \mathcal{O}_k/\mathcal{P} \cong \mathbf{F}_p$.[1] Let

$$\phi : \mathbf{F}_p^n \longrightarrow (\mathcal{O}_k/\mathcal{P})^n$$

be the mapping to representatives of the reduction mod $\mathcal{P}$ in each coordinate. ϕ maps a linear code C into $(\mathcal{O}_k/\mathcal{P})^n$ and we can construct the lattice Γ_C which is associated with the theta function

$$\vartheta_{\Gamma_C} = \sum_{c\in C} \vartheta_{\phi(c)+\mathcal{P}^n}$$

Theorem 2 *Let $W_C(X_0,\cdots,X_{p-1})$ is the complete weight enumerator of a selfdual code of length n over $\mathbf{F}_p$. If $p \equiv 3 \bmod 4$ and $n \equiv 0 \bmod 4$,*

$$W_C\left(\vartheta_{\mathcal{P}}, \vartheta_{1+\mathcal{P}}, \cdots, \vartheta_{p-1+\mathcal{P}}\right)$$

is a modular form of weight n, where $\vartheta_{j+\mathcal{P}}(\tau) = \sum_{x\in j+\mathcal{P}} e^{\pi i \tau\, Tr_{k/\mathbf{Q}}(\frac{x\bar{x}}{p})}$.

(proof) $C_\phi^\perp = C^\perp$ is easily checked. It remains to show $\phi(c)^2 \in 2\mathbf{Z}$. Since

$$\vartheta_{j+\mathcal{P}}(\tau) = \sum_{a,b\in\mathbf{Z}} e^{\pi i\tau\cdot 2\left(a^2+ab+(\frac{p+1}{4})b^2-jb+\frac{j^2}{p}\right)} \qquad (j=0,1,\cdots,p-1),$$

we have $\vartheta_{j+\mathcal{P}}(\tau+1) = e^{\frac{2j^2}{p}\pi i}\vartheta_{j+\mathcal{P}}(\tau)$. Therefore $\vartheta_{\phi(c)+\mathcal{P}}(\tau+1) = \vartheta_{\phi(c)+\mathcal{P}}(\tau)$ holds if and only if $c_1^2+c_2^2+\cdots+c_n^2 \equiv 0 \bmod p$. ■

Finally we show some examples of selfdual codes over $\mathbf{F}_p$.

Examples.

1. Suppose that $a^2+b^2+c^2 \equiv 0 \bmod p$. If $abc \not\equiv 0$, then there exists [4,2] selfdual codes over $\mathbf{F}_p$ defined by the generator matrix

$$G = \begin{pmatrix} a & 0 & b & c \\ 0 & a & c & -b \end{pmatrix}.$$

[1] Let k be an algebraic field such that $[k:\mathbf{Q}] = n$. If $\mathcal{P}$ is a prime ideal of degree f and the discriminant of k is p^{n-f}, then $\mathcal{P}^*/\mathcal{P} = \mathcal{O}_k/\mathcal{P} \cong \mathbf{F}_{p^f}$. We have the case $n=2, f=1$. The case $n=p-2, f=1$ is studied in [4]

2. Suppose that $a^2+2b^2+2c^2 \equiv 0 \mod p$. If $abc \not\equiv 0$, then there exists [8,4] selfdual codes over $\mathbf{F}_p$ defined by the generator matrix

$$G = \begin{pmatrix} a & 0 & 0 & 0 & b & -b & c & c \\ 0 & a & 0 & 0 & b & b & -c & c \\ 0 & 0 & a & 0 & -c & c & b & b \\ 0 & 0 & 0 & a & c & c & b & -b \end{pmatrix}.$$

3. Let $p \equiv 1 \mod 4$. If $m \not\equiv 0 \mod p$, there exists [2m,m] selfdual codes over $\mathbf{F}_p$ defined by the generator matrix

$$G = \begin{pmatrix} a & 0 & \dots & 0 & -(m-2) & 2b & \dots & 2b \\ 0 & a & & 0 & 2b & -(m-2)b & & 2b \\ \vdots & & \ddots & & \vdots & & \vdots & \\ 0 & 0 & & a & 2b & 2b & & -(m-2)b \end{pmatrix}.$$

where $a^2+m^2b^2 \equiv 0 \mod p$.

Remark. The equation $a^2+b^2+c^2 \equiv 0 \mod p$ has non trivial solutions by the theorem of Chevalley-Warning([9]). If $abc \equiv 0$, the code defined by G is constructed from codes of smaller length. It is true for $a^2+2b^2+2c^2 \equiv 0 \mod p$. For $p = 8m+1$ or 3, under the assumption that $b^2+c^2 = 4m+1$ has the solution such that $bc \neq 0$, we may take $a^2 \equiv -1$ or 1 so that $a^2+2b^2+2c^2 \equiv 0 \mod p$. For $p = 8m+5$ or 7, under the assumption that $a^2+2b^2 = 8m+3$ has the solution such that $ab \neq 0$, we may take $c^2 \equiv 1$ or 2 respectively. Note that 4 positions of the check bits of G gives a 2-(4,3,2) design.

References

[1] E.Bannai, *Invariant rings of finite groups and automorphic forms(a survey)(in Japanese)*, Proc.Symp.on Algebra (at Yamagata Univ.July24-27,1996),41(1996),p173-187.

[2] ——, *Codes over finite rings and finite abelian groups (a survey)*,Proc.Symp.on Algebraic geometryENumber theory and CodesECriptography (at Tokyo Univ.January 5-7,1998),p97-107.

[3] M.Broue and M.Enguehard, *Polynômes des poids de certains codes et fonctions thêta de certain réseaux*,Ann.Sci.École.Norm.Sup.6(1973),p157-181.

[4] Ebeling, *Lattice and Codes*, a course partially based on lectures by F.Hirzebruch, Vieweg,1994.

[5] A.M.Gleason, *Weight polynomial of selfdual codes and the MacWilliams identities*,in Actes Congrés International des Mathematiciens,Nice,1970,Tomes 3,Gauthier-Villards,Paris, 1971,211-215.

[6] F.J.A.MacWilliams,C.L.Mallow and N.J.A.Slone, *Generalization of Gleason's theorem on weight enumerators of self dual codes*,IEEE trans.Inform.Theory 18(1972),p794-805.

[7] F.J.MacWilliams-N.J.A.Sloane, *The Theory of Error-Correcting Codes*,North-Holland, Amsterdam,1977

[8] D.P.Maher, *Modular forms from codes*,Can.J.Math.32.(1980),p40-58

[9] J.P.Serre, *Cours d'Arithmétique* (Press Univ.de France,1970).Japanese translation published by Iwanami-Shoten,1979

Department Of System Engineering, Hosei University
Kajino 3-7-2,Koganei,Tokyo,184-8584,Japan
i9508502@k.hosei.ac.jp
SHIGETO NISHIMURA