ANNALES DE L'INSTITUT FOURIER

EIICHI BANNAI

Modular invariance property of association schemes, type II codes over finite rings and finite abelian groups and reminiscences of François Jaeger (a survey)

Annales de l'institut Fourier, tome 49, nº 3 (1999), p. 763-782

<http://www.numdam.org/item?id=AIF_1999__49_3_763_0>

Ann. Inst. Fourier, Grenoble
49, 3 (1999), 763–782

MODULAR INVARIANCE PROPERTY OF ASSOCIATION SCHEMES, TYPE II CODES OVER FINITE RINGS AND FINITE ABELIAN GROUPS, AND REMINISCENCES OF FRANÇOIS JAEGER (A SURVEY)

by Eiichi BANNAI

To the memory of François Jaeger

0. Introduction.

This paper is based on my talk at the Jaeger Memorial Conference in Grenoble, August 31-September 4 in 1998. The composition of this paper, though slightly expanded, is essentially the same as my talk in the conference.

First in §1, I briefly recall, from a very personal viewpoint, how we encountered François Jaeger and how our joint work started and progressed. When we think of our mathematical connection with Jaeger, the modular invariance property of association schemes played a central role. In my talk and in this paper we will focus on this subject, as well as a new application of this property to coding theory; namely we define the concept of Type II codes over finite abelian groups, by using the modular invariance property of the association schemes of abelian groups. (See §3 of the present paper for the definition of the modular invariance property of the association schemes of abelian groups.) Then we discuss how to apply these codes to study certain modular forms.

Keywords: Modular invariance – Association scheme – Spin model – Code over finite ring – Type II code – Hermitian modular form.
AMS classification: 05E30 – 94B05 – 11F55.

Our starting point of this research was a joint work of Eiichi and Etsuko Bannai and François Jaeger [7], where we determined completely the solutions of the modular invariance property of the association schemes of finite abelian groups. The original motivation in [7] was to use these solutions to construct 4-weight spin models on finite abelian groups. Our key observation, which will be discussed extensively in this paper, is that these solutions are also used to define the concept of Type II codes over arbitrary finite abelian groups. In addition, we discuss the relations among (multiple) weight enumerators of Type II codes over finite rings and/or finite abelian groups and invariant polynomial rings of certain finite group actions, and then we discuss its applications to modular forms.

We conclude our talk by mentioning how the generators of the hermitian modular forms of genus 2 (due to Freitag and Nagaoka) are interpreted in terms of the (multiple) weight enumerators of Type II codes over the finite ring $Z[i]/2Z[i]$. (This last part is based on an ongoing joint work with Masaaki Harada, Akihiro Munemasa and Manabu Oura.)

Table of Contents

A preliminary version of this paper, in particular the content of Sections 2 and 3 was published in the Proceedings of 14th Algebraic Combinatorics Symposium (In honor of Professor Michio Suzuki's 70th birthday) which was held at International Christian University in Mitaka Tokyo, July 14-17 in 1997, which is regarded as an unofficial publication. Although the main objective of this paper is to give a survey, the content of §3 is new, in the sense that it was not published before in any official publication.

I would like to thank many of my collaborators for their help, which lead to the present paper. In particular, I owe Etsuko Bannai, Steve Dougherty, Masaaki Harada, Akihiro Munemasa, Manabu Oura, Michio Ozeki, for many of the contents presented in this paper. In particular, §4 is based on our joint paper [10] with Masaaki Harada, Akihiro Munemasa,

and Manabu Oura. Also, I feel strongly the influence of François Jaeger on our overall research, and I miss him greatly mathematically and personally.

1. How we met François Jaeger.

In 1991 Professor Louis Kauffman visited Kyushu University to give a colloquium talk (by the invitation of Professor Toshitake Kohno then at Kyushu University). He showed us a preprint of the paper [29] of François Jaeger: Strongly regular graphs and spin models for the Kauffman polynomial, which was later published in Geometriae Dedicata 44 (1992), 23-52. I was fascinated with the paper, and we read the paper very carefully in our weekly seminars. Before that, I knew the name of François Jaeger as a specialist in graph theory and matroids, and I was very much surprised that he was seriously interested in strongly regular graphs and association schemes – usually association schemes and matroids are regarded as very disjoint subjects in combinatorics. I was also surprized to find that Jaeger's understanding of association schemes was quite thorough and quite deep. (Later, he told me that he learned the detailed properties of association schemes from our book [11].) At that time, partly by the influence of Toshitake Kohno, I was interested in some aspect of mathematical physics (though I have to admit that my understanding of the subject was clearly that of a nonexpert), and I had already obtained the following results:

1. Connection between fusion algebras (at the algebraic level) and the character algebras in the sense of Kawada [33] (see also [11], Section 2.5) which is the concept of purely algebraic level of the Bose-Mesner algebras of an association scheme. (Cf. [2].)

2. How the concept of modular invariance property in fusion algebras is interpreted in the context of association schemes. (Cf. [2].)

3. We obtained a family of solutions of the modular invariance property in the Hamming association schemes $H(d,q)$. (Cf. [4].)

(The complete determination of the solutions of the modular invariance property in the Hamming association schemes $H(d,q)$ was obtained later by Stanton [46]. Also, it should be remarked that Curtin-Nomura [16] determined the possible solutions of the modular invriance property for self-dual P-polynomial association schemes, or equivalently, self-dual P- and Q-polynomial association schemes. Namely, all the parameters of those association schemes which have a solution of the modular invariance property are described explicitly by using 2 parameters. On the other hand, it is still an interesting open question whether the association schemes with such parameters actually exist or not.)

The theme of Jaeger [29] is summarized as follows. In order to find spin models, association schemes are very useful. In particular, he showed that if an association scheme is associated with a spin model, then it must be a self-dual association scheme. We were interested in constructing more examples of spin models using association schemes. The most notable self-dual association schemes are Hamming association schemes $H(d,q)$, and so we started to find spin models on the Hamming association scheme $H(d,q)$. To our surprise, we discovered that the solutions of the modular invariance property we just found for the Hamming association scheme $H(d,q)$ can be used to construct spin models on $H(d,q)$, and we succeeded in proving the claim. It took us several months to finish our calculations, then we told our result ([6]) to François Jaeger. He appreciated our results, but it turned out that our examples are equivalent to those constructed by the tensor product contruction of spin models of Potts models (a remark due to Jaeger and de la Harpe). So, we were disappointed with the fact that our results were not really new. But also we were encouraged greatly with the fact that it became very clear that the modular invariance property of an association scheme is in fact a key to the construction of spin models. (It was some years later that this fact was rigorously proved by Jaeger [30], Nomura [39] and Jaeger-Matsumoto-Nomura [32].) (Cf. survey papers by Jaeger [30] and Nomura [40].) Encouraged with this observation, we started to find further examples of spin models by trying to find the solutions of the modular invariance property of self-dual association schemes. This also gave a motivation for Nomura to construct his spin models from Hadamard graphs (Cf. [38].) Further developments in the study of spin models will be seen in the survey papers by Jaeger [30] and Nomura [40], and so we will not discuss these topics here.

As I mentioned before, I was very much fascinated with the work of François Jaeger on spin models. I first invited him to visit Japan for 2 weeks in November-December of 1992. He visited Kyoto for a conference (the topic in the conference was centered on algebraic combinatorics including association schemes and spin models), and then visited Kyushu University. Many fruitful collaborations between Jaeger and Japanese mathematicians were started then. For example, [5] was born with the influence of Jaeger. Namely, we generalized (or clarified) the concept of the modular invariance property to non-symmetric commutative association schemes. We invited

Jaeger again for the international conference: Algebraic Combinatorics, Fukuoka,1993, which we organized. Then we arranged him to visit RIMS (Research Institute for Mathematical Sciences) of Kyoto University for 3 months (Oct. 1994-Dec. 1994) in the RIMS Project: The Year of Algebraic Combinatorics, which we organized. At that period, we had very active seminars with Jaeger, and it was while Jaeger was visiting Japan that he proved the breakthrough that to any (symmetric) spin model an association scheme is in fact always associated. (As soon as he arrived in Japan, he told me that he had an idea which may prove this fact, then within a few weeks he suceeded in proving this.) Motivated by this work of Jaeger, Nomura immediately obtained a purely algebraic proof of this fact, and then the joint work of Jaeger-Matsumoto-Nomura [32] was started in this period. (I think this work is a highlight of the work of Jaeger on spin models.) Also, joint work with François Jaeger, Etsuko Bannai and myself in this period, was materialized in the paper [7], where we determined the solutions of the modular invariance property for any finite abelian group, as well as the constructions of 4-weight spin models, among others. (Applications of this work is the main topic in §3 of this paper.)

I visited Jaeger in Grenoble in June 1995 after I visited Hungary for a conference. (Jaeger was also in the conference in Hungary.) When Jaeger was in Fukuoka in 1994, we took him for a hiking to a nearby mountain named Nijotake. We enjoyed it very much. When I visited Grenoble, he took me to the hiking to the top of a nearby mountain named Dent de Crolles. It was an unforgettable visit for me. At that time, it seems that François was basically in a good health and he himself was not aware of any possibility of cancer (although he told me that he has a problem in the nerves in his backbone, and he mentioned a possibility that it might become suddenly fatal.) In January 1996, I received an unexpected and surprising letter from him in India that he got ill. Soon, it turned out that he had cancer. He explained his illness very clearly to me, and he was ready to and willing to fight his illness. I visited him in Grenoble again in September 1996 with Kazumasa Nomura. Although he was fighting with the illness, he could spare a week to work for mathematics. We talked mathematics very extensively. Kazumasa Nomura and I were planning to visit him again in September 1997, but that visit was not realized as François passed away on August 18.

2. Review of codes over F_2.

First, we give a review of the classical results concerning the relations between binary Type II (i.e., self-dual doubly even) codes, even unimodular lattices, invariant rings of certain finite groups, and ordinary modular forms.

Let $V = F_2^n$ be the n-dimensional vector space over the binary field $F_2 = \{0,1\}$. A vector subspace C of V is called a (linear) code. For two elements

$$x = (x_1, x_2, \ldots, x_n) \in V$$

and

$$y = (y_1, y_2, \ldots, y_n) \in V$$

we define

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \in F_2.$$

The *dual code* $C^{\perp}$ is defined by

$$C^{\perp} = \{y \in V | x \cdot y = 0, \forall x \in C\}.$$

We say that C is *self-dual* if $C = C^{\perp}$. We have $k := \dim C = n/2$ for a self-dual code C. We call C *doubly-even* if

$$4 | wt(u), \forall u \in C.$$

Here, for $u = (u_1, u_2, \ldots, u_n) \in C$, we define $wt(u) = |\{j | u_j \neq 0\}|$. We say that a code C is a *Type II code* (over F_2) if C is self-dual and doubly-even.

DEFINITION (Weight enumerator of a code). — *For a code C, the weight enumerator $W_C(x,y)$ of the code C is defined as follows:*

$$W_C(x,y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \in \mathbb{C}[x,y].$$

(Note that $W_C(x,y)$ is a homogeneous polynomial of degree n in the indeterminates x and y.)

Now, let G be the finite group of order 192 generated by the two elements $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Here note that the group G is a finite unitary reflection group (No. 9 in the list of Shephard and Todd). It is known that for a binary Type II code C, its weight enumerator $W_C(x,y)$ is in the invariant ring $\mathbb{C}[x,y]^G$ (by the action of the group G on the polynomial ring $\mathbb{C}[x,y]$). Moreover, it is known as Gleason's theorem (1970) ([26]) that

(1) the vector space spanned by the weight enumerators of Type II codes coincides with the invariant ring $\mathbb{C}[x,y]^G$, and that

(2) the invariant ring $\mathbb{C}[x,y]^G$ is a polynomial ring $\mathbb{C}[f_1,f_2]$ generated by the following two algebraic independent polynomials f_1 and f_2, where

$$f_1 = W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$$

is the weight enumerator of the $[8,4,4]$-Hamming code e_8, and

$$f_2 = W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

is the weight enumerator of the $[24,12,8]$-Golay code g_{24}.

Now, let us recall the procedure (Construction A) of constructing an integral lattice from a binary code. Let φ be the natural homomorphism from Z^n to $(Z/2Z)^n \cong F_2^n$. For a code C over F_2, define

$$L_C = \frac{1}{\sqrt{2}}\varphi^{-1}(C) \subset R^n.$$

It is known that if C is a binary Type II code, then L_C is an even unimodular lattice. The theta function of a lattice L is defined by

$$\Theta_L(\tau) = \sum_{x\in L} q^{\frac{1}{2}x\cdot x}, \quad (q = e^{2\pi i\tau}).$$

(Here τ takes the value in the upper half plane.) Note that if L is an even unimodular lattice, then $\Theta_L(\tau)$ is a modular form of weight $k = n/2$ with respect to the full modular group $SL(2,Z)$. Here we recall that the complex valued function f defined on the upper half plane $\mathcal{H}$ is called a modular form of weight k (with respect to the full modular group $SL(2,Z)$) if the following three conditions are satisfied:

(1) f is a holomorphic function on $\mathcal{H}$.

(2)

$$f\Big(\frac{a\tau+b}{c\tau+d}\Big) = (c\tau+d)^k f(\tau), \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,Z).$$

(3) $f(\tau)$ has a Fourier expansion

$$f(\tau) = \sum_{r \geqslant 0} a_r q^r \quad (q = e^{2\pi i \tau}).$$

THEOREM (Broué and Enguehard, [14], 1972). — *If C is a Type II code (over F_2), then we have*

$$\Theta_{L_C}(\tau) = W_C(\theta_3(2\tau), \theta_2(2\tau)).$$

(Here note that $\theta_3(2\tau) = A(\tau)$ is the theta series of the 1-dimensional integral lattice $\{\sqrt{2}z | z \in Z\}$ and $\theta_2(2\tau) = B(\tau)$ is the theta series of the translate (by $\frac{1}{\sqrt{2}}$) of the lattice $\{\sqrt{2}z | z \in Z\}$.)

It should be pointed out that by the map

$$\begin{aligned} x &\mapsto \theta_3(2\tau) \\ y &\mapsto \theta_2(2\tau), \end{aligned}$$

we get an isomorphism

$$\mathbb{C}[x, y]^G \cong \mathbb{C}[E_4, \Delta_{12}]$$

where E_4 is the Eisenstein series of weight 4, and Δ_{12} is the cusp form of weight 12. Note that $\mathbb{C}[E_4, \Delta_{12}]$ is a subspace of the space of all the modular forms which is isomorphic to the polynomial ring $\mathbb{C}[E_4, E_6]$ generated by E_4 and E_6 (the Eisenstein series of weight 6). Here, E_4 and E_6 are algebraically independent.

It is interesting to point out (cf. Ozeki [42] or Runge [43]) that if we take the index 2 subgroup H (of order 96) of G defined by

$$H = < \frac{1+i}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} >,$$

then the above map defines an isomorphism

$$\mathbb{C}[x, y]^H \cong \mathbb{C}[E_4, E_6].$$

Moreover, $\mathbb{C}[x, y]^H = \mathbb{C}[f_1, f_3]$, where

$$f_1 = W_{e_8}(x, y)$$

and

$$f_3 = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}.$$

Note that H is another finite unitary reflection group (No.8 in the list of Shephard and Todd.)

The important implication of this fact is that we can understand the space of modular forms completely through the invariant ring of the finite group H. Interestingly enough, this situation can be generalized in several directions. We list some of them in the following table.

Generalizations.

automorphic forms	codes	invariant rings of finite groups
(ordinary) modular forms	weight enumerator $W_C(x, y)$	$H(\text{or } G) \subset GL(2, C)$ $\mathbb{C}[x, y]^H$
Siegel modular forms (Runge)	multi-weight enumerator	$H = Z_4 * Z_2^{2g+1} Sp(2g, 2)$, $H \subset GL(2^g, C)$
Jacobi forms (Bannai-Ozeki, Runge)	certain joint weight enumerator (Jacobi polynomials in the sense of Ozeki)	simultaneous diagonal action of H (of order 96) $H \subset GL(2r, C)$
Siegel-Jacobi forms	*	*
...	...	...
Hilbert modular forms (Hirzebruch -van der Geer)	Lee weight enumerator (over F_p)	certain finite group G, $G \subset GL(\frac{p-1}{2}, C)$
...	...	...

3. Type II codes over finite rings and finite abelian groups.

Codes are considered not only over binary field F_2 but also over other finite fields $F_3, F_4, \ldots, F_q$, or over $Z/4Z$ (as was studied by many people, including Hammons-Kumar-Calderbank-Sloane-Solé [27], and others), over

$Z/2kZ$ (by M. Harada et al. [19], [9]) and so on. Also, recently, there are many interesting works on codes over some finite rings (by Wood [48], Bachoc [1], etc.).

The purpose of our study is to study codes over finite rings and arbitrary finite abelian groups. I believe that considering (additive) codes over any finite abelian group is the most natural and most reasonable framework for this kind of study. (A preliminary idea is due to Delsarte [17], who considered self-dual codes in this context.) The main purpose of this section is to define Type II codes in this general setting. I believe that the definition given here is reasonable and gives the correct generalization.

Before considering codes over finite abelian groups in general, we review some basic concepts on codes over the finite rings $Z/4Z$ and $Z/2kZ$.

On $Z/4Z$, we define the $E\text{-}wt(a)$ for $a \in Z/4Z$ as follows ($E\text{-}wt$ stands for Euclidean weight):

$$\begin{array}{ccccc} a \in Z/4Z & 0 & 1 & 2 & 3 \\ E\text{-}wt(a) & 0 & 1 & 4 & 1. \end{array}$$

Then for $u = (u_1, u_2, \ldots, u_n) \in (Z/4Z)^n$, we define

$$E\text{-}wt(u) = \sum_{i=1}^{n} E\text{-}wt(u_i).$$

We call C a Type II code over $Z/4Z$ if

(1) C is self-dual, that is $C = C^{\perp}$ with respect to the usual inner product in $(Z/4Z)^n$, namely $C^{\perp} = \{y \in V | x \cdot y = 0, \forall x \in C\}$ with $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n \in Z/4Z$, and

(2) $8 | E\text{-}wt(u), \forall u \in C$.

On $Z/2kZ$, we define the $E\text{-}wt(a)$ for $a \in Z/2kZ$ as follows:

$$\begin{array}{cccccccccc} a \in Z/2kZ & 0 & 1 & 2 & 3 & \cdots & i & \cdots & 2k-2 & 2k-1 \\ E\text{-}wt(a) & 0 & 1 & 4 & 9 & \cdots & i^2 & \cdots & 4 & 1. \end{array}$$

Similarly, we define the code C to be a Type II code, if

(1) C is self-dual with respect to the ordinary inner product in $(Z/2kZ)^n$, and

(2) $4k | E\text{-}wt(u), \forall u \in C$.

In this case, if we define the natural homomorphism from Z^n to $(Z/2kZ)^n$ by φ, then for each code C in $(Z/2kZ)^n$, the set $L_C = \frac{1}{\sqrt{2k}}\varphi^{-1}(C) \subset R^n$ becomes an even unimodular lattice in R^n.

Now let us consider codes on any finite abelian group G. By a code over G, we mean an additive subgroup C of $G^n = G \times G \times \cdots \times G$ (the direct product of n G's).

In order to define the concept of self-dual code, we consider the character table of the abelian group G.

A character table P of the group $G = Z/mZ$ is given as follows:

$$P = \begin{matrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \cdots & \zeta^{m-1} \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \cdots & \zeta^{2(m-1)} \\ 1 & \zeta^3 & \zeta^6 & \zeta^9 & \cdots & \zeta^{3(m-1)} \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{m-1} & \zeta^{2(m-1)} & \zeta^{3(m-1)} & \cdots & \zeta^{(m-1)^2}. \end{matrix}$$

Note that in a character table we can choose, in principle, the orderings of the elements of G and the irreducible characters of G in any order. However, note that here we arranged the character table P in such a way that ${}^tP = P$ holds.

We can take the following matrices P as character tables of the group $Z_2 \times Z_2$:

$$P = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{matrix}$$

or

$$P = \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1. \end{matrix}$$

Again, we arranged so that ${}^tP = P$ holds. Namely, we have $\chi_a(b) = \chi_b(a), \forall a, b \in G$. This is equivalent to saying (in the terminology of [7]) that we fix a duality

$$a \longleftrightarrow \chi_a$$

where χ_a is the (irreducible) linear character corresponding to the element $a \in G$.

We define the concept of self-dual code by considering the following inner product $< x, y >$ on G^n. Fix a character table P of the abelian group G. It is important that we take P in such a way that ${}^tP = P$ holds. As the above example of the group $G = Z/2Z \times Z/2Z$ shows, the choice of duality, i.e., the choice of the character table P with ${}^tP = P$ is not unique in general.

For two elements

$$x = (x_1, x_2, \ldots, x_n) \in G^n$$

and

$$y = (y_1, y_2, \ldots, y_n) \in G^n$$

we define

$$< x, y >= \prod_{i=1}^{n} \chi_{x_i}(y_i).$$

Then we define

$$C^{\perp} = \{y \in G^n | < x, y >= 1, \forall x \in C\}.$$

A code C is called self-dual if $C^{\perp} = C$. The problem we want to discuss here is: how to define the concept of Type II code? Here we give an answer to this question. Now, let us recall our notation again.

G is a finite abelian group of order g. Let P be a character table of G with ${}^tP = P$ (so, P is a $g \times g$-matrix.) That is, we fix a duality

$$a \longleftrightarrow \chi_a.$$

We say that a diagonal matrix

$$T = \begin{pmatrix} t_0 & 0 & \cdot & 0 \\ 0 & t_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & t_{g-1} \end{pmatrix}$$

has the modular invariance property if

$$(PT)^3 = (\text{scalar}) \cdot I.$$

We remark that for each G, the dualities, and the solutions T of the modular invariance property (for each fixed duality) are completely determined. (See Bannai-Bannai-Jaeger [7]. See also [12bis], where it is shown which of the dualities are coming from the dualities of the cyclic groups which appear in the decomposition of the abelian group.)

It is shown in [7] that if the order of the group G is even, then the solution T can be expressed in the following way, by using $\eta = e^{2\pi i \frac{1}{2l}}$, where l is the exponent of the abelian group G. (The exponent is the largest order of the elements of the abelian group G.)

$$T = \begin{pmatrix} \eta^{a_0} & 0 & \cdot & 0 \\ 0 & \eta^{a_1} & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \eta^{a_{g-1}} \end{pmatrix}.$$

Here the $\alpha(\in G)$th diagonal element is η^{a_α}. (If $|G|$ is odd, we can take $\eta = e^{2\pi i \frac{1}{l}}$ and get a similar expression for T.) Also, here we assume that $a_0 = 0$ holds.

Example. — Note that if $G = Z/2kZ$ then we have a solution

$$T = \begin{pmatrix} \eta^0 & 0 & & & 0 \\ 0 & \eta^1 & & & \\ & & \eta^4 & & \\ \vdots & & & \ddots & 0 \\ 0 & & \cdots & 0 & \eta^{(2k-1)^2} \end{pmatrix}.$$

Now, for each solution T of the modular invariance property

$$T = \begin{pmatrix} \eta^{a_0} & 0 & \cdot & 0 \\ 0 & \eta^{a_1} & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \eta^{a_{g-1}} \end{pmatrix},$$

we define for each $\alpha \in G$, $Wt(\alpha) = a_\alpha$. Then for $u = (u_\alpha)_{\alpha \in G}$ we define

$$Wt(u) = \sum_{\alpha \in G} Wt(u_\alpha).$$

Note that in the case of $G = Z/2kZ$, (and for P and T given above), our weight $Wt(u)$ coincides with the Euclidean weight $E\text{-}wt(u)$. So our weight is a generalization of the Euclidean weight.

DEFINITION. — *We define a code C (over an abelian group G of even order) to be a Type II code (over an abelian group G of even order) if C is self-dual and*

$$2l|Wt(u), \forall u \in C.$$

(Note that this definition of Type II codes depends not only on G but also on P and T.)

Complete weight enumerator.

The complete weight enumerator of a code C is defined as follows:

$$W_C(\{x_\alpha|\alpha \in G\}) = \sum_{u \in C} \prod_{\alpha \in G} x_\alpha^{\omega_\alpha(u)},$$

where for $u = (u_1, u_2, \ldots, u_n) \in G^n$, we define

$$\omega_\alpha(u) = |\{j|u_j = \alpha\}|.$$

Then

$$W_C(\{x_\alpha|\alpha \in G\}) \in C[x_\alpha|\alpha \in G]^{\mathcal{G}}$$

where

$$\mathcal{G} := < \frac{1}{\sqrt{g}} P, T > \subset GL(g, C)$$

is a finite group. It can be proved that if $G = Z/2^m Z$, and if P and T are as before, then the group $\mathcal{G}$ is a group of order $192 \cdot 2^{m-1}$. It is very interesting that this group $\mathcal{G}$ is always a finite group for any G, P and T. (This fact will be discussed in a separate paper. See [9] for a discussion of a special case.) It is an interesting question to know the structure of this group explicitly for any G, P and T.

We conclude this section by giving the following remarks.

First we remark that considering codes over a finite abelian group is more general than considering codes over a finite commutative ring. For a code C over a finite ring R, i.e., C is an additive subgroup of R^n, the dual code $C^\perp$ is defined by using the multiplication of the ring

(1) $$C^\perp = \{y \in R^n | x \cdot y = 0, \forall x \in C\},$$

where $x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$. On the other hand, for a code C over an abelian group G, i.e., an additive subgroup of G^n, the dual code $C^\perp$ is defined by

$$C^\perp = \{y \in G^n | < x, y >= 1, \forall x \in C\}.$$

Note that (1), generally corresponds to fixing a duality in the additive abelian group $G = (R, +)$. So codes over a finite ring may be regarded as a special case of codes over a finite abelian group (with a certain choice of duality). (See also Question 4 at the end of this section.)

Next we consider how we may construct lattices, in certain general situation, from codes over finite abelian groups. Let K be a finite Galois extension of the rational number field Q. Let $\mathfrak{o} = \mathfrak{o}_K$ be the ring of the integers of K. Let I be any ideal in $\mathfrak{o}$, and let

$$\mathfrak{o}/I \cong R$$

where R is a finite commutative ring. Let φ be the natural homomorphism from $(\mathfrak{o})^n$ to $(\mathfrak{o}/I)^n$. For a code C in R^n, $\varphi^{-1}(C)$ may be regarded as a lattice in $\mathfrak{o}^n$. Many interesting lattices arise in this way (see for example Bachoc [1], etc.) Finally we emphasize that the following situation is very interesting and worthy of further study.

Example. — $K = Q(i)$ where $i = \sqrt{-1}$. $\mathfrak{o}_K = Z[i]$, $p = 2$, and $I = 2Z[i]$. Then $\mathfrak{o}/I = R$ and $(R, +) \cong Z/2Z \times Z/2Z$. By considering the codes over the ring R or equivalently codes over the abelian group $G = Z/2Z \times Z/2Z$, we can obtain hermitian modular forms. Further details will be treated in a separate paper [10] (see also §4).

We would like to point out that, in this way, we can get many automorphic forms, and also get better understandings of automorphic forms. It is very interesting to note that essentially finite objects such as weight enumerators of codes or polynomial invariants of certain finite groups enable us to control essentially infinite objects such as automorphic forms.

4. Type II codes over $Z[i]/2Z[i]$ and an application to hermitian modular forms.

We will not give the detailed explanations of hermitian modular forms. Instead we refer the reader to Nagaoka [37] for the definition and basic properties of hermitian modular forms. Briefly speaking, a function from the hermitian upper half plane H_g to the complex numbers C is said to be a hermitian modular forms (with respect to the full hermitian modular group $\Gamma_g = \Gamma_g(Q[i])$) if (1) it is holomorphic and (2) if it satisfies an automorphic condition (for weight k). (If the genus g is equal to 1, a further condition on holomorphy at cusps is necessary, but we mostly consider the cases $g \geqslant 2$.) (See [37], pages 526-527, for example.) Here, hermitian upper half plane of genus g is defined as the set of g by g complex matrices Z with $\frac{1}{2i}(Z - Z^*)$ being positive definite, where Z^* denotes the transpose of the complex conjugate of Z. A hermitian modular form ϕ is called symmetric if $\phi(Z) = \phi({}^tZ)$ for all $Z \in H_g$. We denote by $[\Gamma_g, k]$ the space of hermitian modular forms of weight k. We denote by $[\Gamma_g, k]^{(s)}$ the space of symmetric hermitian modular forms of weight k. It is known that dimensions of these spaces are 0 for negative integers k, and finite for positive integers k. The genus $g = 1$ case is nothing but the case of ordinary modular forms, so we will not discuss the case $g = 1$. For $g = 2$, it seems that the dimension formula for symmetric modular forms is known to be given by the following form (cf. Nagaoka [36]):

$$\sum_{k=0}^{\infty}(\dim[\Gamma_g, k]^{(s)})t^k = \frac{1+t^{16}}{(1-t^4)(1-t^8)(1-t^{10})(1-t^{12})^2}.$$

A set of generators of the space of symmetric hermitian modular forms is given by Freitag [24]. Nagaoka [37] gives another set of generators, and also gives a relation satisfied by these generators. (It seems still unknown whether there are further relations among them. This is related with the fact that the dimension formula is as expected above. A set of generators $\psi_4, \chi_8, \chi_{10}, \chi_{12}, \xi_{12}, \chi_{16}$, is given by Nagaoka [37]. Although we will not give the details of our result here, in our joint paper Bannai-Harada-Munemasa-Oura [10] (in preparation), we obtained the following results:

(1) We consider Type II codes over the finite ring $R = Z[i]/2Z[i]$, or equivalently over the finite ring $F_2 + uF_2$ in the sense of Bachoc [1], or Dougherty-Harada-Gaborit-Solé [18]. Bachoc [1] (see also Dougherty-Harada-Gaborit-Solé [18]) defined an analogue of Gray map (over $Z/4Z$) from the codes (of length n) over the ring R to the codes (of length $2n$) over F_2. They also proved that Type II codes over $R(\cong F_2 + uF_2)$ are mapped to Type II codes over F_2, which admit fixed point free involutive automorphism of the code. We prove that the equivalence of such codes over R is determined by the pair of the equivalence in Type II codes over F_2 and the conjugacy classess of fixed point free involutions in the automorphism group of the code.

(2) Since Type II codes over F_2 are determined up to length 32, in principle, this makes it possible to classify Type II codes over R of length up to 16, (though it is not trivial from the computational view point, as the

automorphism groups become very large in some cases.) We expect that we will be able to finish this. (Dougherty-Harada-Gaborit-Solé [18] did this up to length 8. In order to determine them up to the equivalence, they used mass formula, instead of our simple criterion for the equivalence.)

(3) It is shown that the (symmetric) biweight enumerators of Type II codes over R are invariant by the group action of G, which is defined in [18].

Also, substituting the indeterminates of the polynomials by certain appropriate theta series, we can conclude that (symmetric) biweight (of multi-weight of genus g) enumerators of Type II codes over R always give symmetric hermitian modular forms of genus 2 (of genus g). We can show that the generators of weight multiple of 4 by Freitag and Nagaoka are expressed by using the symmetric biweight enumerators of Type II codes. For example, we have the following results. For $n = 4$ there are 2 nonequivalent Type II codes over R. Both of them give the Nagaoka's generator ψ_4. For $n = 8$ there are 10 nonequivalent Type II codes over R. 6 of them are coming from an indecomposable Type II code d_{16}^{+} over F_2, and each of them gives ψ_8. Another 4 of them are coming from the decomposable Type II code $e_8 \oplus e_8$. 3 of them give the Nagaoka's generator ψ_4^2 and the remaining one gives $(15\psi_8 - 7\psi_4^2)/8$. Further details will be given in [10].

It is hoped that the study of codes over finite rings and finite abelian groups are useful to study various automorphic forms. We are particularly interested in the following questions:

Question 1. Can we determine, or characterize, which finite rings are obtained as the quotient ring o_K/I for an ideal I of the ring of integers o_K with K a finite Galois extension of the rational number field Q? It seems that many partial answers are available in the book [36] or the papers referred there, but it seems that the complete solution is not yet obtained.

Question 2. For each finite abelian group and its fixed duality, when (how many ways) can one associate a ring structure on it where the duality with respect to this ring structure corresponds to the given duality in the abelian group.

Question 3. Although we noticed that the solutions of the modular invariance property (for the character table of a finite abelian group) are used very nicely to define the concept of Type II codes (over the abelian group), so far we do not know any real (or intrinsic) reason why this works. Can one give a reason to explain why this works?

Question 4. We need to study more on the relations between codes over a ring and codes over an abelian group (in which the additive group of the ring is isomorphic to the abelian group.) It is observed that in many cases the ring structure is characterized by a single duality of the abelian group. However, this seems not always be the case, and it might be necessary to consider the set of dualities. Also, for some rings, the better Type II condition may use more than one solutions of the modular invariance property (possibly corresponding to different dualities of the abelian group). Here we remark that we do not know how many nonisomorphic ring structures exist for a fixed abelian group, but we know how may dualities and how many solutions of the modular invariance properties exist for each fixed duality. This seems to give an advantage in considering codes over finite abelian groups over considering the codes over general finite rings.

BIBLIOGRAPHY

[1] C. BACHOC, Applications of coding theory to the construction of modular lattices, J. Combinatorial Theory, (A) 78 (1997), 173-187.

[2] E. BANNAI, Association schemes and fusion algebras (an introduction), J. Algebraic Combinatorics, 2 (1993), 327-344.

[3] E. BANNAI, Invariant rings of finite groups and automorphic forms (a survey) (in Japanese), Algebra Symposium Proceedings (at Yamagata University, July 24-27,1996), 42 (1996), 173-187.

[4] E. BANNAI and E. BANNAI, Modular invariance of the character table of the Hamming association scheme $H(d,q)$, J. Number Theory, 57 (1994), 79-92.

[5] E. BANNAI and E. BANNAI, Generalized spin models and association schemes, Memoire of Fac. Sci. Kyushu University, Ser (A), 47 (1993), 379-409.

[6] E. BANNAI, E. BANNAI, T. IKUTA and K. KAWAGOE, Spin models constructed from Hamming association schemes, Proceedings of 10th Algebraic Combinatorics Symposium at Gifu, 1992, 91-106.

[7] E. BANNAI, E. BANNAI and F. JAEGER, On spin models, modular invariance, and duality, J. Algebraic Combinatorics, 6 (1997), 203-228.

[8] E. BANNAI, E. BANNAI, M. OZEKI and Y. TERANISHI, On the ring of simultaneous invariants of the Gleason-MacWilliams group (preprint).

[9] E. BANNAI, S. DOUGHERTY, M. HARADA and M. OURA, The II codes, even unimodular lattices and invariant rings, IEEE Trans. Inform. Theory (to appear).

[10] E. BANNAI, M. HARADA, A. MUNEMASA and M. OURA, Type II codes over F_2+uF_2 and applications to hermitian modular forms (a tentative title), in preparation.

[11] E. BANNAI and T. ITO, Algebraic Combinatorics, I, Benjamin/Cummings, 1984.

[12] E. BANNAI and M. OZEKI, Construction of Jacobi forms from certain combinatorial polynomials, Proc. Japan Acad. (A), 72 (1996), 12-15.

[12bis] Etsuko BANNAI and A. MUNEMASA, Duality maps of finite abelian groups and their applications to spin models, J. Algebraic Combinatorics, 8 (1998), 223-234.

[13] A. BONNECAZE, P. SOLÉ, C. BACHOC and B. MOURRAIN, Type II codes over Z_4, IEEE Trans. Inform. Theory, 43 (1997), 969-976.

[14] M. BROUÉ and M. ENGUEHARD, Polynômes des poids de certains codes et fonctions theta de certains réseaux, Ann. Sci. Ecole Norm. Sup., 5 (1972), 157-181.

[15] J. H. CONWAY and N. J. A. SLOANE, Sphere Packings, Lattices and Groups, Springer-Verlag, 1988.

[16] B. CURTIN and K. NOMURA, Some formulas for spin models for distance-regular graphs (to appear).

[17] P. DELSARTE, An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplments, 10 (1973), 125-136.

[18] S. T. DOUGHERTY, P. GABORIT, M. HARADA and P. SOLÉ, Type II codes over $F_2 + uF_2$, IEEE Trans. Inform. Theory (to appear).

[19] S. T. DOUGHERTY, T. A. GULLIVER and M. HARADA, Type II self-dual codes over finite rings and even unimodular lattices, J. Algebraic Combinatorics (to appear).

[20] W. DUKE, On codes and Siegel modular forms, International Math. Res. Notes, (1993), 125-136.

[21] W. EBELING, Lattices and Codes, a course partially based on lectures by F. Hirzebruch, Vieweg, 1994.

[22] M. EICHLER and D. ZAGIER, The Theory of Jacobi Forms, Birkhauser, 1985.

[23] E. FREITAG, Siegelsche Modulfunktionen, Springer, 1983.

[24] E. FREITAG, Modulformen zweiten Grades zum rationalen und Gausssehen Zahlkorper, Sitzungsber. Heidelberg Akad. Wiss., 1967, 3-49.

[25] P. GABORIT, Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings, IEEE Trans. on Inf. Theory, 42 (1996), 1222-1228.

[26] A. M. GLEASON, Weight polynomials of self-dual codes and the MacWilliams identities, Actes Congrès Intern. Math., 3 (1970), 211-215.

[27] A. R. HAMMONS, Jr., P. V. KUMAR, A. R. CALDERBANK, N. J. A. SLOANE and P. SOLÉ, The Z_4-linearlity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. on Inf. Theory, 40 (1994), 301-319.

[28] J. IGUSA, On Siegel modular forms of genus 2, (1) and (II), Amer. J. Math., 84, 88 (1962) (1966), 175-200, 221-236.

[29] F. JAEGER, Strongly regular graphs and spin models for the Kauffman polynomial, Geomet. Dedicata, 44 (1992), 23-52.

[30] F. JAEGER, Spin models for link invariants, in "Survey in Combinatorics, 1995", London Math. Soc., Lecture Notes Series, 218 (1995), 71-101.

[31] F. JAEGER, Towards a classification of spin models in terms of association schemes, in Progress in Algebraic Combinatorics, Advanced Studies in Pure Math., 24 (1996), 197-225.

[32] F. JAEGER, M. MATSUMOTO and K. NOMURA, Bose-Mesner algebras related to Type II matrices and spin models, J. Algebraic Combinatorics, 8 (1998), 39-72.

[33] Y. KAWADA, Uber den Dualitatssatz der Charactere nichtcommutativer Gruppen, Proc. Phys, Math. Soc. Japan, 24 (1942), 97-109.

[34] A. KRIEG, Modular Forms on Half-Spaces of Quaternions, Springer Lecture Note Series, 1143 (1985).

[35] F. J. MACWILLIAMS and N. J. A. SLOANE, The Theory of Error Correcting Codes, North-Holland, 1977.

[36] B. R. MCDONALD, Finite Rings with Identity, Marcel Dekker, 1974.

[37] S. NAGAOKA, A note on the structure of the ring of symmetric Hermitian modular forms of degree 2 over the Gaussian field, J. Math. Soc. Japan, 48 (1996), 525-549.

[38] K. NOMURA, Spin models constructed from Hadamard matrices, J. Combinatorial Theory (A), 68 (1994), 251-261.

[39] K. NOMURA, An algebra associated with a spin model, J. Algebraic Combinatorics, 6 (1997), 53-58.

[40] K. NOMURA, Spin models and Bose-Mesner algebras, Europ. J. Comb., (to appear).

[41] M. OURA, The dimension formula for the ring of code polynomials in genus 4, Osaka J. Math., 34 (1997), 53-72.

[42] M. OZEKI, On the notion of Jacobi polynomials for codes, Math. Proc. Cambridge Phil. Soc., 121 (1997), 15-30.

[43] B. RUNGE, On Siegel modular forms, part I, J. reine angew. Math., 436 (1993), 57-85.

[44] B. RUNGE, Theta functions and Siegel-Jacobi forms, Acta Mathematica, 175 (1995), 165-196.

[45] G. C. SHEPHARD and J. A. TODD, Finite unitary reflection groups, Canad. J. Math., 6 (1954), 274-304.

[46] D. STANTON, A matrix equation for association schemes, Graphs and Combinatorics, 11 (1995), 103-108.

[47] S. TSUYUMINE, On Siegel modular forms of degree three, Amer. J. Math., 108 (1986), 755-862.

[48] J. A. WOOD, Duality for modules over finite rings and applications to coding theory (preprint).

Eiichi BANNAI,
Kyushu University
Graduate School of Mathematics
Hakozaki 6-10-1 Higashi-ku
Fukuoka 812-8581 (Japan).