Europ. J. Combinatorics (1999) **20**, 397–410
Article No. eujc.1998.0276
Available online at http://www.idealibrary.com on IDEAL®

Terwilliger Algebras of Cyclotomic Schemes and Jacobi Sums

HARUO ISHIBASHI, TATSURO ITO AND MIEKO YAMADA[†]

We show that the T-module structure of a cyclotomic scheme is described in term of Jacobi sums. It holds that an irreducible T-module of a cyclotomic scheme fails to have maximal dimension if and only if Jacobi sums satisfy certain kind of equations, which are of some number theoretical interest in themselves.

1. INTRODUCTION

Terwilliger algebras, or simply T-algebras, were introduced by Terwilliger [10] under the name subconstituent algebras. T-algebras and their representations are becoming increasingly important in the study of association schemes themselves and of some combinatorial objects defined over association schemes. This is typically seen in Terwilliger's work toward the classification of P- and Q-polynomial schemes and expected in the study of spin models, codes, and designs.

Terwilliger writes, 'To get an intuitive feel for T [T is a Terwilliger algebra], suppose for the moment that the associate classes $R_0, R_1, \dots, R_d$ [of our association scheme $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$] are the orbits of the automorphism group Aut($\mathcal{X}$) acting on the Cartesian product $X \times X$. Then the Bose–Mesner algebra is the centralizer algebra of Aut($\mathcal{X}$). Whether or not Aut($\mathcal{X}$) acts in the above fashion, we may still view the Bose–Mesner algebra as a 'combinatorial analogue' of this centralizer algebra. Similarly, we may view T as a 'combinatorial analogue' of the centralizer algebra of the stabilizer of [the base vertex] x in Aut($\mathcal{X}$).'

Following Terwilliger, let us consider an association scheme $\mathcal{X}$ whose automorphism group Aut($\mathcal{X}$) acts transitively on each associate class R_i, and let us denote by S the centralizer algebra of the stabilizer of the base vertex x in Aut($\mathcal{X}$). It turns out that T is contained in S but does not always coincide with S. Some examples of T that are smaller than S are reported for group association schemes in Ref. [2].

In this paper, we shall choose cyclotomic schemes to discuss whether T coincides with S or not. What we actually do is to determine when an irreducible S-module fails to remain irreducible as a T-module; this suffices to settle the question of whether T coincides with S or not, as the algebras T and S are both semi-simple and in the case of cyclotomic schemes, non-isomorphic irreducible S-modules cannot be isomorphic as T-modules (Corollary 5). As is shown in Corollary 10, the problem turns out to be reduced to a number theoretical problem, which is in itself interesting: let K be a finite field, H a multiplicative subgroup of $K^\times$ with index e, η a generator of the character group of $K^\times/H$. The number theoretical problem is to find all multiplicative characters χ of $K^\times$ such that $\chi|_H \neq 1_H$ and the Gauss sum $g(\eta^i\chi)$ equals $\epsilon^i g(\chi)$ for all i, where ϵ is an eth root of unity independent of i.

In the last section, we shall discuss in detail the case of $e = 2$, i.e., the case where H is of index 2. Let $p = \text{char } K$ and $|K| = p^r$. It holds that $T = S$ if and only if r is odd (Corollaries 13, 14). Moreover, we show that when r is even, the number theoretical condition $g(\eta\chi) = \pm g(\chi)$ is equivalent to a weaker one, namely $g(\eta\chi)$ and $g(\chi)$ generate the same

[†] The author's current address is: Department of Computational Science, Faculty of Science, Kanazawa University, Kakuma-machi, Kanazawa 920-1192, Japan.

0195–6698/99/050397 + 14 $30.00/0

ideal in the ring of integers of $\boldsymbol{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity with n the order of χ (Theorem 16). Given a multiplicative character χ of K, the weaker condition enables us to check $g(\eta\chi) = \pm g(\chi)$ easily, as Stickelberger's theorem tells us the factorization of the ideal generated by a Gauss sum. In case of $r = 2$, Shiratani–Yamada [9] has recently determined all χ for which $g(\eta\chi) = \pm g(\chi)$ holds.

In many ways, the T-algebra is a good combinatorial analogue of the centralizer algebra S. However, it may not be a perfect combinatorial analogue of S. For example, T need not be closed with respect to the Hadamard multiplication, whereas S is. In any case, we think it important to examine how close T is to S for various association schemes. In [6], cyclotomic schemes over Galois rings of characteristic 4 are considered in this respect. It should be noted that the work on Galois rings was motivated by our work on Galois fields.

2. The Centralizer Algebra $\mathrm{Hom}_H(V, V)$

Let $\mathcal{X} = (X, \{R_i\}_{0\le i\le d})$ be an association scheme which may or may not be commutative. Denote the set of y with $(x, y) \in R_i$ by $R_i(x)$. The *standard module* V of $\mathcal{X}$ is the unitary space with X an orthonormal basis: $V = \bigoplus_{x\in X} \boldsymbol{C}x$ and $< x, y >= \delta_{xy}$ for $x, y \in X$. The *adjacency map* f_i with respect to the associate relation R_i is the linear tansformation of V defined by $f_i(x) = \sum_{y\in R_i(x)} y$ for $x \in X$. The *Bose–Mesner algebra* $\mathfrak{A}$ of $\mathcal{X}$ is the subalgebra of the endmorphism ring $\mathrm{End}(V)$ spanned by all f_i.

Fix a base vertex x_0 and let V_i^* be the subspace of V spanned by $R_i(x_0)$. Let e_i^* be the orthogonal projection of V onto V_i^*. The *Terwilliger algebra* T of $\mathcal{X}$, which may depend on the base vertex x_0, is defined to be the subalgebra of $\mathrm{End}(V)$ spanned by all f_i, e_j^*. T and $\mathfrak{A}$ are semi-simple algebras and obviously T contains $\mathfrak{A}$.

Let G be a finite group acting on a set X transitively. Let $R_0, R_1, \ldots, R_d$ be the orbits of G acting on the Cartesian product $X \times X$ in the natural way. Then we have an association scheme $\mathcal{X} = (X, \{R_i\}_{0\le i\le d})$, which may or may not be commutative. It is well known that the Bose–Mesner algebra $\mathfrak{A}$ coincides with the centralizer algebra $\mathrm{Hom}_G(V, V)$ of G, the algebra consisting of all linear transformations of V that commute with the action of G on V.

Let us fix a base vertex $x_0 \in X$ and let H be the stabilizer of x_0 in G. It can be easily checked that every element of the Terwilliger algebra T with respect to the base vertex x_0 commutes with the action of H on V. So T is contained in the centralizer algebra $\mathrm{Hom}_H(V, V)$ of H. Denoting $\mathrm{Hom}_H(V, V)$ by S, we have three semi-simple algebras $S, T, \mathfrak{A}$ with the inclusion $S \supset T \supset \mathfrak{A}$. Notice that T and $\mathfrak{A}$ are defined combinatorially but S is not. The question is when T coincides with S. As S becomes smaller or is unchanged when we replace G by a bigger subgroup of $\mathrm{Aut}(\mathcal{X})$, we usually assume $G = \mathrm{Aut}(\mathcal{X})$.

As S and T are semi-simple algebras, S and T coincide if and only if every irreducible S-module remains irreducible as a T-module and every pair of non-isomorphic irreducible S-modules remains non-isomorphic as T-modules. Notice that every irreducible S-module (resp. T-module) appears in V, because S (resp. T) is faithful on V. In this section, we briefly review some duality between the S-module V and the H-module V. The following argument is valid for any finite group H acting on V and $S = \mathrm{Hom}_H(V, V)$.

Let $\mathrm{Irr}(H, V)$ be the set of irreducible characters of H which appear in the H-module V.

Proposition 1. *(i) The isomorphism classes of irreducible S-modules are in one-to-one correspondence with $Irr(H, V)$.*

(ii) Let W be an irreducible S-submodule of V corresponding with $\theta \in \mathrm{Irr}(H, V)$. Let U be a H-submodule of V and $m_U(\theta)$ the multipilicity of θ in U. Then we have

$$\dim W \cap U = m_U(\theta).$$

PROOF. For $\theta \in \mathrm{Irr}(H, V)$, let $V(\theta)$ be the homogeneous component of the H-module V affording θ, i.e., the sum of irreducible H-submodules of V affording θ. From Schur's lemma, it is well known that $V(\theta)$ is S-invariant and that for an arbitrary decomposition $V(\theta) = \bigoplus U_i$ with U_i an irreducible H-submodule affording θ, the algebra $S|_{V(\theta)} = \mathrm{Hom}_H(V(\theta), V(\theta))$ has a basis $\{f_{ji}\}$ such that

(1) $\{f_{ji}\}$ vanishes on U_k if $k \neq i$,
(2) $f_{ji}(U_i) = U_j$ affords a H-isomorphism between U_i and U_j,
(3) $f_{lk} f_{ji} = \delta_{kj} f_{li}$.

In particular, $V(\theta)$ is a homogeneous component of the S-module V. The assertions (i) and (ii) immediately follow from the above observation. □

An S-submodule W (resp. T-submodule W) of V is called *thin* if $\dim W \cap V_i^* \leq 1$ for all i, where $V_i^* = \bigoplus_{x \in R_i(x_0)} \boldsymbol{C}x$. The algebra S (resp. T) is *thin* if every irreducible S-submodule (resp. T-submodule) of V is thin. Notice that T is thin whenever S is thin, because isomorphic T-submodules intersect V_i^* with the same dimension, and so it suffices to test the thinness for the irreducible T-submodules which are contained in an irreducible S-submodule.

COROLLARY 2. *S is thin if and only if H is mulitplicity free on every V_i^*, i.e., $m_{V_i^*}(\theta) = 0$ or 1 for all θ.*

Assume that H is a subgroup of another finite group H' which also acts on V, extending the action of H on V. Set $S' = \mathrm{Hom}_{H'}(V, V)$. Then $S \supset S'$. Let W (resp. W') be an irreducible S-submodule (resp. S'-submodule) of V corresponding to $\theta \in \mathrm{Irr}(H, V)$ (resp. $\theta' \in \mathrm{Irr}(H', V)$). By the *multiplicity* of W' in W, we mean $\dim_{\boldsymbol{C}} \mathrm{Hom}_{S'}(W', W)$, and we simply denote it by $(W', W)_{S'}$. So when we decompose W as a direct sum of irreducible S'-modules, the multiplicity is the number of direct summands that are isomorphic to W'. Let $(\theta', \theta)_H$ stand for the inner product of characters $\theta, \theta'|_H$ of H as usual.

PROPOSITION 3. *The multiplicity of W' in W coincides with that of θ in θ', i.e.,*

$$(W', W)_{S'} = (\theta', \theta)_H.$$

PROOF. Let U' be an irreducible H'-submodule of V affording θ'. Consider $\dim W \cap U'$. If we view W as an S'-module, $\dim W \cap U' = (W', W)_{S'}$ by Proposition 1. If we view W as an S-module, $\dim W \cap U' = (\theta', \theta)_H$. □

3. T-MODULES OF CYCLOTOMIC SCHEMES

3.1. Cyclotomic schemes. From now on, we assume that $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is a cyclotomic scheme over a finite field K. So we take a subgroup H of the multiplicative group $K^\times$ and form a group $G = K \rtimes H$, the semi-direct product of the additive group K by H. Set $X = K$. Then G acts transitively on X by $x^{(a,b)} = a + xb$. In other words, G is isomorphic to the subgroup of GL(2, K) consisting of $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ with $a \in K$, $b \in H$. Identifying X with the affine plane consisting of $(1, x) \in K^2$ with $x \in X$, the action of G on X is identical with that of the linear subgroup on the affine plane. The associate relations R_i of the cyclotomic scheme are the orbits of G on $X \times X$.

Let us understand that $K^\times/H$ also means a complete representatives of the H-cosets of $K^\times$ and that K/H is a union of 0 and $K^\times/H$. For $a \in K/H$, let R_a be the set consisting of

$(x, y) \in X \times X$ with $y - x \in aH$. Then the G-orbits on $X \times X$ are R_a $(a \in K/H)$, and the cyclotomic scheme is $\mathcal{X} = (X, \{R_a\}_{a \in K/H})$.

When we consider $x \in K$ as an element of X, we sometimes denote it by x^* to clarify that it belongs to the standard module V. So $x^* + y^*$ means the sum of x^* and y^* in V, whereas $x + y$ means the sum of x and y in the field K. Thus the adjacency map f_a is the linear transformation of V defined by

$$f_a(x^*) = \sum_{y \in aH} (x + y)^* \tag{1}$$

for $x \in K$.

It is well known [5] that the automorphism group of the cyclotomic scheme $\mathcal{X}$ is no larger than G : Aut$(\mathcal{X}) = G$. As G acts transitively on X, the structure of the Terwilliger algebra does not depend on the choice of the base vertex x_0. So we may assume $x_0 = 0$ without loss of generality. Then $V_a^* = \oplus_{x \in aH} \boldsymbol{C} x^*$ $(a \in K/H)$, and e_a^* is the orthogonal projection of V onto V_a^*. The Terwilliger algebra T of $\mathcal{X}$ is the subalgebra of End(V) spanned by f_a, e_b^* $(a, b \in K/H)$.

3.2. Irreducible S-modules $V(\theta)$. The stabilizer of the base vertex 0 in G is H. As H is abelian, V_a^* $(a \neq 0)$ affords the regular representation of H, and V_0^* affords the trivial representatin of H. Let $\widehat{H}$ be the character group of H. For $\theta \in \widehat{H}$, let $V(\theta)$ be the homogeneous component of the H-module V affording θ. Then for $a \in K^\times/H$ and $\theta \in \widehat{H}$, the 1-dimensional subspace $V(\theta) \cap V_a^*$, which is an irreducible H-module affording θ, is spanned by

$$v_a(\theta) = \sum_{h \in H} \overline{\theta(h)} (ah)^*. \tag{2}$$

Thus we have,

$$\begin{aligned} V_a^* &= \bigoplus_{\theta \in \widehat{H}} \boldsymbol{C} v_a(\theta) \qquad \text{if } a \neq 0, \\ V_0^* &= \boldsymbol{C} 0^*, \\ V(\theta) &= \bigoplus_{a \in K^\times/H} \boldsymbol{C} v_a(\theta) \qquad \text{if } \theta \neq 1_H, \\ V(1_H) &= \bigoplus_{a \in K/H} \boldsymbol{C} v_a(1_H), \end{aligned}$$

where 1_H is the principal character of H and $v_0(1_H) = 0^*$.

Set $S = \mathrm{Hom}_H(V, V)$. By Proposition 1, $V(\theta)$ $(\theta \in \widehat{H})$ is an irreducible S-module, and $V(\theta_1)$, $V(\theta_2)$ are not isomorphic as S-modules if $\theta_1 \neq \theta_2$. As S acts faithfully on V, every irreducible S-module is isomorphic to some $V(\theta)$. We are mainly interested in the following problem.

PROBLEM A. Determine when $V(\theta)$ is reducible as a T-module.

Notice that $S = T$ if and only if $V(\theta)$ is irreducible as a T-module for all $\theta \in \widehat{H}$, because S and T are both semi-simple with $S \supset T$ and every pair of non-isomorphic irreducible S-modules remains non-isomorphic as T-modules (Corollary 5). It is well known that $V(1_H)$ is irreducible as a T-module [10]. So in what follows, we always assume $\theta \neq 1_H$.

3.3. The graph $\Gamma(H, \theta)$. The T-module $V(\theta)$ has an orthogonal basis $v_b(\theta)$ $(b \in K^\times/H)$. Let us express the adjacency map f_a $(a \in K^\times/H)$ in matrix form:

$$f_a(v_b(\theta)) = \sum_{c \in K^\times/H} r_{ab}^c(\theta) v_c(\theta).$$

We define a graph $\Gamma = \Gamma(H, \theta)$ as follows: The vertex set is $K^\times/H$ and (b, c) is an edge $(b \neq c)$ if and only if $r_{ab}^c(\theta) \neq 0$ for some $a \in K^\times/H$. The graph Γ turns out to be undirected (Corollary 6). As T is generated by f_a, e_a^*, the T-module $V(\theta)$ is irreducible if and only if Γ is connected. More precisely, a connected component Σ of Γ gives rise to an irreducible T-module

$$V_\Sigma(\theta) = \bigoplus_{b \in \Sigma} \boldsymbol{C} v_b(\theta),$$

and $V(\theta)$ is decomposed as the direct sum of irreducible T-modules $V_\Sigma(\theta)$ with Σ running through the connected components of Γ.

3.4. Jacobi sums and edges of $\Gamma(H, \theta)$. Let $\widehat{K^\times}$ be the character group of the multiplicative group $K^\times$. For $\chi \in \widehat{K^\times}$, we extend χ to K by defining $\chi(0) = 0$. For $\chi_1, \chi_2 \in \widehat{K^\times}$, the *Jacobi sum* is defined to be

$$J(\chi_1, \chi_2) = \sum_{u \in K} \chi_1(u)\chi_2(1-u).$$

THEOREM 4. *For* $a, b, c \in K^\times/H$ *and* $\theta \in \widehat{H}$ $(\theta \neq 1_H)$, *it holds that*

$$\overline{r_{ab}^c(\theta)} = \frac{1}{|K^\times : H|^2} \sum_{\xi, \chi} \xi(a^{-1}c)\chi(b^{-1}c) J(\xi, \chi),$$

where the sum is taken over $\xi, \chi \in \widehat{K^\times}$ *such that* $\xi|_H = 1_H$ *and* $\chi|_H = \theta$, *and* $\overline{r}$ *stands for the complex conjugate of* r. *In particular,* $K^\times$ *acts on* Γ *as a group of automorphisms.*

PROOF. Put (2) in (1) to obtain

$$f_a(v_b(\theta)) = \sum_{h, h' \in H} \overline{\theta(h)}(ah' + bh)^*.$$

So $r_{ab}^c(\theta)v_c(\theta)$ is the partial sum of the right-hand side over $h, h' \in H$ such that $ah' + bh \in cH$. Set $ah' + bh = cu$ $(u \in H)$. Then $h = u(b^{-1}c - b^{-1}ah'u^{-1}) = u(b^{-1}c - b^{-1}au')$ $(u' = h'u^{-1} \in H)$. Hence, extending θ to K by defining $\theta(x) = 0$ for $x \notin H$, we have

$$r_{ab}^c(\theta) = \sum_{u' \in H} \overline{\theta(b^{-1}c - b^{-1}au')}. \tag{3}$$

For a H-coset Ht, let φ_{Ht} be the characteristic function of it: $\varphi_{Ht}(x) = 1, 0$ according to whether x belongs to Ht or not. Then φ_{Ht} is a linear combination of characters of $K^\times$ that vanish on H:

$$\varphi_{Ht} = \sum_{\xi \in \widehat{K^\times/H}} \alpha_\xi \xi \qquad (\alpha_\xi \in \boldsymbol{C}).$$

The coefficient α_ξ is

$$\begin{aligned}\alpha_\xi &= (\varphi_{Ht},\ \xi)_{K^\times} \\ &= \frac{1}{|K^\times|} \sum_{h \in H} \overline{\xi(ht)} \\ &= \frac{|H|}{|K^\times|} \overline{\xi(t)}.\end{aligned}$$

Therefore

$$\varphi_{Ht} = \frac{1}{|K^\times : H|} \sum_{\xi \in \widehat{K^\times/H}} \overline{\xi(t)}\xi. \tag{4}$$

Choose a character $\chi_1 \in \widehat{K^\times}$ such that $\chi_1|_H = \theta$. Then by (3), (4), we have

$$\begin{aligned} r^c_{ab}(\theta) &= \sum_{u \in H} \varphi_H(b^{-1}c - b^{-1}au)\overline{\chi_1(b^{-1}c - b^{-1}au)} \\ &= \frac{1}{|K^\times : H|} \sum_{\substack{u \in H \\ \xi \in \widehat{K^\times/H}}} \xi(b^{-1}c - b^{-1}au)\overline{\chi_1(b^{-1}c - b^{-1}au)}, \end{aligned}$$

and so

$$\overline{r^c_{ab}(\theta)} = \frac{1}{|K^\times : H|} \sum_{u,\chi} \chi(b^{-1}c - b^{-1}au), \tag{5}$$

where the sum is taken over $u \in H$ and $\chi \in \widehat{K^\times}$ such that $\chi|_H = \theta$.

Write the partial sum $\sum_{u \in H} \chi(b^{-1}c - b^{-1}au)$ of the right-hand side of (5) as

$$\chi(b^{-1}c) \sum_{t \in K} \varphi_{Hc^{-1}a}(t)\chi(1-t).$$

Then by (4), it equals

$$\frac{\chi(b^{-1}c)}{|K^\times : H|} \sum_{\xi \in \widehat{K^\times/H}} \overline{\xi(c^{-1}a)} \sum_{t \in K} \xi(t)\chi(1-t) = \frac{\chi(b^{-1}c)}{|K^\times : H|} \sum_{\xi \in \widehat{K^\times/H}} \xi(a^{-1}c)J(\xi, \chi).$$

This proves the theorem. □

COROLLARY 5. *For distinct $\theta, \theta' \in \widehat{H}$ $(\theta \neq 1_H, \theta' \neq 1_H)$, the irreducible S-modules $V(\theta)$, $V(\theta')$ are not isomorphic as T-modules.*

PROOF. Suppose there exists a T-module isomorphism $\varphi : V(\theta) \to V(\theta')$.

Applying $\varphi e^*_b = e^*_b \varphi$ to the orthogonal basis $v_b(\theta)$ $(b \in K^\times/H)$ of $V(\theta)$, we have

$$\varphi(v_b(\theta)) = \lambda_b v_b(\theta')$$

for some nonzero $\lambda_b \in \boldsymbol{C}$. Applying $\varphi f_a = f_a \varphi$ to $v_b(\theta)$ $(a, b \in K^\times/H)$, we have

$$\lambda_c r^c_{ab}(\theta) = \lambda_b r^c_{ab}(\theta') \tag{6}$$

for $c \in K^\times/H$.

Choose $\xi_0, \chi_0, \chi'_0 \in \widehat{K^\times}$ such that $\xi_0|_H = 1|_H$, $\chi_0|_H = \theta$, $\chi'_0|_H = \theta'$. Multiply both sides of (6) by $\xi_0(a^{-1}c)\chi_0(b^{-1}c)$ and sum them up over $a, b \in K^\times$. Then by Theorem 4, the left-hand side is

$$\begin{aligned} \frac{\lambda_c}{|K^\times : H|^2} \sum_{\xi,\chi} \overline{J(\xi, \chi)} \left\{ \sum_{a \in K^\times} \overline{\xi(a^{-1}c)}\xi_0(a^{-1}c) \right\} \left\{ \sum_{b \in K^\times} \overline{\chi(b^{-1}c)}\chi_0(b^{-1}c) \right\} \\ = \lambda_c |H|^2 \overline{J(\xi_0, \chi_0)}, \end{aligned}$$

which is nonzero.

The right-hand side is

$$\frac{1}{|K^\times : H|^2}\sum_{\xi,\chi'}\overline{J(\xi,\chi')}\left\{\sum_{a\in K^\times}\overline{\xi(a^{-1}c)}\xi_0(a^{-1}c)\right\}\left\{\sum_{b\in K^\times}\lambda_b\overline{\chi'(b^{-1}c)}\chi_0(b^{-1}c)\right\}$$
$$= \frac{|K^\times|}{|K^\times : H|^2}\sum_{\chi'}\overline{J(\xi_0,\chi')}\left\{\sum_{b\in K^\times}\lambda_b\overline{\chi'(b^{-1}c)}\chi_0(b^{-1}c)\right\},$$

where χ' runs through $\chi' \in \widehat{K^\times}$ such that $\chi'|_H = \theta'$. Write b as $b = th$ $(t \in K^\times/H,\ \ h \in H)$. Then $\lambda_b = \lambda_t$ and $\chi'(b^{-1}c) = \chi'(t^{-1}c)\theta'(h^{-1})$, $\chi_0(b^{-1}c) = \chi_0(t^{-1}c)\theta(h^{-1})$. So we have

$$\sum_{b\in K^\times}\lambda_b\overline{\chi'(b^{-1}c)}\chi_0(b^{-1}c) = \sum_{t\in K^\times/H}\lambda_t\overline{\chi'(t^{-1}c)}\chi_0(t^{-1}c)\left\{\sum_{h\in H}\overline{\theta'(h^{-1})}\theta(h^{-1})\right\} = 0.$$

Therefore the right-hand side is zero and we have a contradiction. □

COROLLARY 6. *For $a, b, c \in K^\times/H$ and $\theta \in \widehat{H}$ $(\theta \neq 1_H)$, it holds that*

$$\overline{r^c_{ab}(\theta)} = r^b_{-ac}(\theta).$$

In particular, Γ is an undirected graph.

PROOF. By Theorem 4,

$$\overline{r^b_{-a,c}(\theta)} = \frac{1}{|K^\times : H|^2}\sum_{\xi,\chi}\xi(-a^{-1}b)\chi(c^{-1}b)J(\xi,\chi).$$

Here we have

$$\xi(-a^{-1}b)\chi(c^{-1}b)J(\xi,\chi) = \xi(a^{-1}c)\overline{\xi\chi}(b^{-1}c)\xi(-1)J(\xi,\chi)$$

and

$$\xi(-1)J(\xi,\chi) = J(\xi,\ \overline{\xi\chi}).$$

So we have

$$r^b_{-a,c}(\theta) = \frac{1}{|K^\times : H|^2}\sum_{\xi,\chi}\overline{\xi}(a^{-1}c)(\xi\chi)(b^{-1}c)J(\overline{\xi},\ \xi\chi).$$

When χ runs through characters of $K^\times$ such that $\chi|_H = \theta$, so does $\xi\chi$. When ξ runs through $K^\times/H$, so does $\overline{\xi}$. Hence we have the corollary. □

COROLLARY 7. *In Γ, (b, c) is not an edge if and only if*

$$\sum_{\chi}\chi(b^{-1}c)J(\xi,\chi) = 0$$

for all $\xi \in \widehat{K^\times}$ such that $\xi|_H = 1_H$, where the sum is taken over $\chi \in \widehat{K^\times}$ such that $\chi|_H = \theta$.

PROOF. (b, c) is not an edge in Γ if and only if $r^c_{ab}(\theta) = 0$ for all $a \in K^\times/H$. This is equivalent to

$$\sum_{a\in K^\times/H}\xi'(a)\overline{r^c_{ab}(\theta)} = 0$$

for all $\xi' \in \widehat{K^\times/H}$. By Theorem 4, the left-hand side equals

$$\frac{1}{|K^\times : H|^2} \sum_{\xi,\chi} \left\{ \sum_{a \in K^\times/H} \xi'(a)\xi(a^{-1}) \right\} \xi(c)\chi(b^{-1}c)J(\xi,\chi)$$
$$= \frac{1}{|K^\times : H|} \sum_{\chi} \xi'(c)\chi(b^{-1}c)J(\xi',\chi).$$

This proves the corollary. □

3.5. *The fusion scheme.* Let Σ be a connected component of $\Gamma = \Gamma(H,\theta)$ and H' the global stabilizer of Σ in $K^\times$ (recall that $K^\times$ acts on Γ as a group of automorphisms). Then $H \subset H'$, and H' does not depend on the choice of Σ. $K^\times/H'$ is in one-to-one correspondence with the set of connencted components of Γ by the bijection $K^\times/H' \ni b' \mapsto b'H'/H$. The multiplicative subgroup H' gives rise to the cyclotomic scheme $\mathcal{X}' = (X, \{R_{a'}\}_{a' \in K/H'})$, which is a fusion scheme of $\mathcal{X} = (X, \{R_a\}_{a \in K/H})$; $R_{a'}$ is a union of R_a $(a \in a'H'/H)$. Let T' be the Terwilliger algebra of $\mathcal{X}'$ with respect to the base vertex $x_0 = 0$. Then $T' \subset T$; $f_{a'}$ (resp. $e^*_{a'}$) is the sum of f_a (resp. e^*_a) over $a \in a'H'/H$. Set $S' = \mathrm{Hom}_{H'}(V,V)$. Obviously $S' \subset S$. By Proposition 3, we have

$$V(\theta) = \bigoplus_{\theta'} V(\theta'),$$

where the sum is taken over $\theta' \in \widehat{H'}$ such that $\theta'|_H = \theta$. A graph is said to be *discrete* if it has no edges.

THEOREM 8. *For $\theta' \in \widehat{H'}$ with $\theta'|_H = \theta$, the graph $\Gamma(H',\theta')$ is discrete. In other words, every irreducible T'-submodule of $V(\theta')$ is of dimension 1.*

PROOF. The irreducible S'-module $V(\theta')$ has a basis $v_{b'}(\theta')$ $(b' \in K^\times/H')$, where

$$v_{b'}(\theta') = \sum_{h' \in H'} \overline{\theta'(h')}(b'h')^*.$$

Writing $h' = th$ with $t \in H'/H$, $h \in H$, we have

$$v_{b'}(\theta') = \sum_{t \in H'/H} \sum_{h \in H} \overline{\theta'(t)\theta(h)}(b'th)^*$$
$$= \sum_{t \in H'/H} \overline{\theta'(t)} v_{b't}(\theta). \tag{7}$$

In particular, $v_{b'}(\theta')$ belongs to the irreducible T-module $V_\Sigma(\theta)$ corresponding to the connencted component $\Sigma = b'H'/H$ of $\Gamma(H,\theta)$: $V_\Sigma(\theta) = \bigoplus_{b \in b'H'/H} \boldsymbol{C} v_b(\theta)$. As another $v_{c'}(\theta')$ belongs to another irreducible T-module $V_{\Sigma'}(\theta)$ $(\Sigma' = c'H'/H)$, we have

$$V_\Sigma(\theta) \cap V(\theta') = \boldsymbol{C} v_{b'}(\theta').$$

As $T' \subset T$, $V_\Sigma(\theta)$ is T'-invariant. As $T' \subset S'$, $V(\theta')$ is T'-invariant. Hence $V_\Sigma(\theta) \cap V(\theta')$ is T'-invariant. Therefore, the 1-dimensional space $\boldsymbol{C} v_{b'}(\theta')$ is T'-invariant. □

3.6. Discrete $\Gamma(H,\theta)$. Every reducible T-module $V(\theta)$ thus gives rise to a discrete graph $\Gamma(H',\theta')$, and hence Problem A is reduced to the following.

PROBLEM B. Determine when $\Gamma(H,\theta)$ is discrete.

THEOREM 9. $\Gamma(H,\theta)$ *is discrete if and only if*

$$J(\xi,\chi_1)=J(\xi,\chi_2)$$

for all $\xi,\chi_1,\chi_2\in\widehat{K^\times}$ *such that* $\xi|_H=1_H$, $\chi_1|_H=\chi_2|_H=\theta$.

PROOF. By Corollary 7, the graph $\Gamma(H,\theta)$ is discrete if and only if

$$\sum_{\chi}\chi(t)J(\xi,\chi)=0$$

for all $\xi\in\widehat{K^\times/H}$ and all $t\in K^\times/H-\{H\}$. Throughout the proof, we understand that χ runs through characters of $K^\times$ such that $\chi|_H=\theta$.

Suppose that $\Gamma(H,\theta)$ is discrete. For $\chi'\in\widehat{K^\times}$ such that $\chi'|_H=\theta$, we have

$$\begin{aligned}\frac{1}{|K^\times:H|}&\sum_{t\in K^\times/H-\{H\}}\overline{\chi'(t)}\left(\sum_{\chi}\chi(t)J(\xi,\chi)\right)\\&=\left(1-\frac{1}{|K^\times:H|}\right)J(\xi,\chi')-\frac{1}{|K^\times:H|}\sum_{\chi\neq\chi'}J(\xi,\chi)\\&=J(\xi,\chi')-\frac{1}{|K^\times:H|}\sum_{\chi}J(\xi,\chi)\\&=0.\end{aligned}\tag{8}$$

Therefore

$$J(\xi,\chi')=\frac{1}{|K^\times:H|}\sum_{\chi}J(\xi,\chi),$$

and $J(\xi,\chi')$ is independent of χ'.

Conversely, suppose $J(\xi,\chi')$ is independent of χ' such that $\chi'|_H=\theta$. Fix a character χ_1 such that $\chi_1|_H=\theta$, and write $\chi'=\chi_1\xi'$ with $\xi'\in\widehat{K^\times/H}$. For $t'\in K^\times/H-\{H\}$, we have from (8) that

$$\begin{aligned}\frac{1}{|K^\times:H|}\sum_{\xi'\in\widehat{K^\times/H}}\xi'(t')&\left\{\sum_{t\in K^\times/H-\{H\}}\overline{\xi'(t)\chi_1(t)}\sum_{\chi}\chi(t)J(\xi,\chi)\right\}\\&=\overline{\chi_1(t')}\sum_{\chi}\chi(t')J(\xi,\chi)=0.\end{aligned}$$

This proves the theorem. □

Let p be the characteristic of K and $\zeta=e^{2\pi\sqrt{-1}/p}$. For $\chi\in\widehat{K^\times}$, the *Gauss sum* is defined to be

$$g(\chi)=\sum_{u\in K}\chi(u)\zeta^{\mathrm{Tr}u},$$

where Tr denotes the absolute trace from K.

Rewriting Theorem 9 in terms of the Gauss sum, we have the following.

COROLLARY 10. *Let η be a generator of the character group $\widehat{K^\times/H}$, and set $e = |K^\times : H|$. For $\theta \in \widehat{H}$ $(\theta \neq 1_H)$, choose $\chi \in \widehat{K^\times}$ such that $\chi|_H = \theta$. Then $\Gamma(H, \theta)$ is discrete if and only if*

$$g(\eta^i\chi) = \epsilon^i g(\chi) \qquad \text{for all } i,$$

where ϵ is an eth root of unity independent of i.

PROOF. By Theorem 9, $J(\eta, \chi) = J(\eta, \eta^i\chi)$ for all i. As it holds that

$$J(\eta, \eta^i\chi) = \frac{g(\eta)g(\eta^i\chi)}{g(\eta^{i+1}\chi)},$$

we have

$$\frac{g(\chi)}{g(\eta\chi)} = \frac{g(\eta^i\chi)}{g(\eta^{i+1}\chi)} \qquad \text{for all } i,$$

and hence

$$\left(\frac{g(\chi)}{g(\eta\chi)}\right)^{i+1} = \frac{g(\chi)}{g(\eta^{i+1}\chi)}.$$

Set $\epsilon = g(\eta\chi)/g(\chi)$. Then

$$g(\eta^i\chi) = \epsilon^i g(\chi).$$

As $\eta^e = 1$, we have $\epsilon^e = 1$.

Conversely, if $g(\eta^k\chi) = \epsilon^k g(\chi)$ for all k, then

$$\begin{aligned} J(\eta^i, \eta^j\chi) &= \frac{g(\eta^i)g(\eta^j\chi)}{g(\eta^{i+j}\chi)} \\ &= \frac{g(\eta^i)}{\epsilon^i}, \end{aligned}$$

which does not depend on j. □

4. THE CASE OF $|K^\times : H| = 2$

Let us assume that H is of index 2. So, we are dealing with the case where the cyclotomic scheme is a strongly regular graph. Let η be the quadratic character, i.e., the generator of the character group $\widehat{K^\times/H}$. Let θ be an irreducible character of H such that $\theta \neq 1_H$ and χ an irreducible character of $K^\times$ such that $\chi|_H = \theta$. Denote the order of χ by n.

In this case, what we have already proved can be summarized as follows.

COROLLARY 11. *The following are equivalent to each other.*

(i) *The T-module $V(\theta)$ is reducible.*
(ii) $J(\eta, \chi) = J(\eta, \eta\chi)$.
(iii) $g(\eta\chi) = \pm g(\chi)$.

It can also be shown fairly easily (see the proof of Lemma 12) that the above statements are equivalent to

(iv) $J(\eta, \chi) \in \mathbf{Q}$.

Let p = char K and $|K| = p^r$.

LEMMA 12. *If $J(\eta, \chi) = J(\eta, \eta\chi)$, then the power r is even.*

PROOF. As $J(\eta, \eta\chi) = \eta(-1)J(\eta, \overline{\chi})$, it follows from $J(\eta, \chi) = J(\eta, \eta\chi)$ that

$$J(\eta, \chi) = \eta(-1)J(\eta, \overline{\chi}).$$

As $J(\eta, \chi)\overline{J(\eta, \chi)} = p^r$, we have

$$J(\eta, \chi)^2 = \eta(-1)p^r.$$

The Jacobi sum $J(\eta, \chi)$ is an element of $\boldsymbol{Q}(\zeta)$, where ζ is a primitive $(p^r - 1)$th root of unity. The prime p does not ramify in $\boldsymbol{Q}(\zeta)$. Therefore r must be even. □

COROLLARY 13. *If r is odd, then the T-module $V(\theta)$ is irreducible for all $\theta \in \widehat{H}$ $(\theta \neq 1_H)$. In particular, if r is odd, then $S = T$.*

In what follows, we assume that r is even. Let F be the subfield of K such that $[K : F] = 2$. Set $|F| = q$ and $|K| = q^2$.

STICKELBERGER'S THEOREM ([8]). *Suppose the order n of $\chi \in \widehat{K^\times}$ $(\chi \neq 1_{K^\times})$ divides $q + 1$. Then*

$$g(\chi) = \begin{cases} q & \text{if } n \text{ is odd or } \frac{q+1}{n} \text{ is even,} \\ -q & \text{if } n \text{ is even and } \frac{q+1}{n} \text{ is odd.} \end{cases}$$

COROLLARY 14. *If r is even, then $S \supsetneqq T$.*

PROOF. As $K^\times$ has a subgroup H of index 2, q is odd. Choose χ to be, for example, a character of order $q + 1$. Then $\eta\chi$ is also of order $q + 1$. By Stickelberger's theorem, $g(\chi) = g(\eta\chi) = -q$. Obviously $\theta = \chi|_H$ is not the principal character 1_H. By Corollary 11, $V(\theta)$ is reducible as a T-algebra. Hence $S \supsetneqq T$. □

It is a difficult but interesting number theoretical problem to be precise about which χ satisfies $g(\eta\chi) = \pm g(\chi)$. The problem was recently settled for the case of $r = 2$ by Shiratani–Yamada [9]. Experiments by computer based on our Theorem 16 were helpful for them to pin χ down.

COROLLARY 15. *For $\chi \in K^\times$ such that $\chi|_{F^\times} = 1_{F^\times}$, we have*

$$g(\eta\chi) = \pm g(\chi).$$

PROOF. Both χ and $\eta\chi$ have order dividing $q + 1$. □

In what follows, we assume $\chi|_{F^\times} \neq 1_{F^\times}$.

THEOREM 16. *If $\frac{g(\chi)}{g(\eta\chi)}$ is a unit of $\boldsymbol{Q}$ (ζ_n), then $\frac{g(\chi)}{g(\eta\chi)} = \pm 1$, where ζ_n is a primitive nth root of unity with n the order of χ.*

We delay the proof of Theorem 16 and prepare for relative Gauss sums, as they play a crucial role in the proof. Let χ_F be the multiplicative character of F obtained by restricting χ to F. The ratio of the two Gauss sums

$$\tau(\chi) = \frac{g(\chi)}{g(\chi_F)}$$

is called a *relative Gauss sum* associated with χ.

THEOREM 17 ([11]). *It holds that*

$$\tau(\chi) = \sum_{\alpha\in K^\times/F^\times} \overline{\chi}(\mathrm{Tr}_{K/F}\alpha)\chi(\alpha),$$

where $\mathrm{Tr}_{K/F}\alpha$ *is the relative trace from* K *to* F*. Furthermore, we have*

$$\tau(\chi) = \sum_{\mathrm{Tr}_{K/F}\beta=1} \chi(\beta).$$

The norm of $\tau(\chi)$ *is given by*

$$\tau(\chi)\overline{\tau(\chi)} = q.$$

For any integer c prime to n, let σ_c be the automorphism of $\boldsymbol{Q}(\zeta_n)$ defined by $\sigma_c : \zeta_n \mapsto \zeta_n^c$.

PROOF OF THEOREM 16. As two characters χ and $\eta\chi$ coincide on F, we have

$$\frac{\tau(\chi)}{\tau(\eta\chi)} = \frac{g(\chi)}{g(\eta\chi)}.$$

We shall show that $\frac{\tau(\chi)}{\tau(\eta\chi)} = \pm 1$ on the assumption that $\frac{\tau(\chi)}{\tau(\eta\chi)}$ is a unit of $\boldsymbol{Q}(\zeta_n)$. Let us set $\mu(\chi) = \frac{\tau(\chi)}{\tau(\eta\chi)}$. By Theorem 17, the absolute value of $\mu(\chi)$ and the absolute value of any conjugate of $\mu(\chi)$ is 1. Therefore $\mu(\chi)$ is an nth root of unity by Kronecker's theorem. Put $\mu(\chi) = \zeta_n^m$.

First assume that n is odd. Apply σ_c with $c = 2$ to $\mu(\chi)$. Then by Theorem 17, we have

$$\mu(\chi)^{\sigma_2} = \frac{\tau(\chi^2)}{\tau(\eta^2\chi^2)} = 1.$$

Hence $\zeta_n^{2m} = 1$ and so $\zeta_n^m = 1$, i.e., $\mu(\chi) = 1$.

Next assume that $n \equiv 2 \pmod 4$. Then $n/2$ is odd. As $\eta = \chi^{n/2}$, we have $(\eta\chi)^{n/2} = \eta^{n/2}\chi^{n/2} = \eta\eta = 1$. So $\eta\chi$ is of odd order. The argument in the previous paragraph is valid for $\eta\chi$ instead of χ. Hence $\mu(\chi) = 1$.

Finally assume that $n \equiv 0 \pmod 4$. Apply σ_c with $c = n/2 + 1$ to $\mu(\chi)$. Notice that c is an odd number prime to n. By Theorem 17, we have

$$\mu(\chi)^{\sigma_c} = \frac{\tau(\chi^c)}{\tau(\eta^c\chi^c)} = \frac{\tau(\chi^c)}{\tau(\eta\chi^c)}.$$

As $\eta = \chi^{n/2}$, we have $\chi^c = \eta\chi$ and $\eta\chi^c = \chi$. Hence

$$\mu(\chi)^{\sigma_c} = \mu(\chi)^{-1}.$$

This implies $m(n/2 + 2) \equiv 0 \pmod n$. In particular, $4m \equiv 0 \pmod n$. Therefore $\mu(\chi)^4 = \zeta_n^{4m} = 1$, i.e., $\mu(\chi) \in \{\pm 1, \pm\sqrt{-1}\}$.

According to Theorem 17, let us write

$$\tau(\chi) = \tau^+ + \tau^-,$$
$$\tau(\eta\chi) = \tau^+ - \tau^-,$$

where

$$\tau^+ = \sum_{\substack{\mathrm{Tr}\,\beta=1\\ \eta(\beta)=1}} \chi(\beta),$$
$$\tau^- = \sum_{\substack{\mathrm{Tr}\,\beta=1\\ \eta(\beta)=-1}} \chi(\beta).$$

Then

$$\mu(\chi) = \frac{\tau^+ + \tau^-}{\tau^+ - \tau^-}.$$

Suppose $\mu(\chi) = \pm\sqrt{-1}$. Then $\tau^+ = \mp\sqrt{-1}\tau^-$, and so $\tau(\chi) = (1 \mp \sqrt{-1})\tau^-$. As $\tau(\chi)\overline{\tau(\chi)} = q$ by Theorem 17, we obtain

$$2\tau^-\overline{\tau^-} = q.$$

This contradicts the fact that q is a power of the odd prime p. □

Rather than $\frac{g(\chi)}{g(\eta\chi)} = \pm 1$, it is easier to check the equivalent condition in Theorem 16 that $g(\chi)$ and $g(\eta\chi)$ generate the same ideal in the ring of integers of $\boldsymbol{Q}(\zeta_n)$, as it is well known how to find the factorization of the ideal generated by a Gauss sum: let ω be a Teichmüller character and put $\chi = \omega^{-k}$ $(k = \frac{q^2-1}{n})$. Let $\vartheta(k)$ be the Stickerberger element:

$$\vartheta(k) = \sum_{c \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times} \langle \frac{kc}{q^2-1} \rangle \sigma_c^{-1},$$

where $< t >$ is the fractional part of a real number t, $0 \leq< t >< 1$, and $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ is the multiplicative group of $\boldsymbol{Z}/n\boldsymbol{Z}$. Let $\mathfrak{p}$ be a prime ideal lying above p in $\boldsymbol{Q}(\zeta_{q^2-1})$ and $\mathfrak{P}$ a prime ideal lying above $\mathfrak{p}$ in $\boldsymbol{Q}(\zeta_{q^2-1}, \zeta_p)$. We then have the the factorization of the Gauss sum

$$g(\omega^{-k}) \sim \mathfrak{P}^{(p-1)\vartheta(k)} \sim \mathfrak{p}^{\vartheta(k)}.$$

The prime $\sigma_c^{-1}\mathfrak{p}$ occurs in the ideal $\mathfrak{p}^{\vartheta(k)}$ with the multiplicity

$$\sum_{j=0}^{r-1} \left\langle \frac{kcp^j}{q^2-1} \right\rangle,$$

where $|K| = q^2 = p^r$.

For an integer l, write the canonical p-adic expantion $l = l_0 + l_1 p + \cdots + l_{r-1}p^{r-1}$ $(\mathrm{mod}\ q^2-1)$, $0 \leq l_i \leq p-1$, and define $s(l) = l_0 + l_1 + \cdots + l_{r-1}$. Then the multiplicity is given by

$$\frac{1}{p-1}s(kc) = \sum_{j=0}^{r-1} \left\langle \frac{kcp^j}{q^2-1} \right\rangle.$$

As $\eta\chi = \omega^{-k+\frac{q^2-1}{2}}$, the Gauss sums $g(\chi)$ and $g(\eta\chi)$ have the same factorization in $\boldsymbol{Q}(\zeta_{q^2-1}, \zeta_p)$ if and only if

$$s(kc) = s(kc + \frac{q^2-1}{2}c) \qquad (\forall c \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times).$$

Given q and k, it is easy for a computer to check the above equality for all $c \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times$.

ACKNOWLEDGEMENTS

The authors are very much grateful to Dr A. Munemasa for useful discussions during the preparation of this paper.

References

1. E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin-Cummings, New York, 1984.
2. E. Bannai and A. Munemasa, The Terwilliger algebras of group association schemes, *Kyushu J. Math.*, **49** (1995), 93–102.
3. B. C. Berndt and R. J. Evans, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer, *Illinois J. Math.*, **23** (1979), 374–437.
4. B. C. Berndt and R. J. Evans, The determination of Gauss sums, *Bull. A.M.S.*, **6** (1981), 107–129.
5. A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance Regular Graphs*, Springer-Verlag, New York, 1989.
6. H. Ishibashi, The Terwilliger algebras of certain association schemes over the Galois rings of characteristic 4, *Graphs Combin.*, **12** (1996), 39–54.
7. S. Lang, *Cyclotomic Fields I, II*, Springer-Verlag, New York, 1980.
8. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1994.
9. K. Shiratani and M. Yamada, On rationality of Jacobi sums, *Colloquium Mathematicum*, **73** (1997), 251–260.
10. P. Terwilliger, The subconstituent algebra of an association scheme. I, II, III, *J. Algebraic Combin.*, **1, 2** (1992, 1993), 363–388, 73–103, 177–210.
11. K. Yamamoto and M. Yamada, Williamson Hadamard matrices and Gauss sums, *J. Math. Soc. Japan*, **37** (1985), 703–717.

Received 3 May 1997 and accepted 27 November 1998

Haruo Ishibashi and Mieko Yamada
Graduate School of Mathematics,
Kyushu University,
Fukuoka 812-81,
Japan

Tatsuro Ito
Department of Computational Science,
Faculty of Science,
Kanazawa University,
Kakuma-machi,
Kanazawa 920-11,
Japan