Generalized Relative Difference Sets and PBIBDs Associated with Amorphous Association Schemes over an Extension Ring of $Z/4Z$

Dedicated to the memory of Professor Koichi Yamamoto

Mieko Yamada
Department of Applied Mathematics
Konan University
Okamoto, Higashinada-ku
Kobe 658, Japan

Abstract.

Partially balanced incomplete block designs, PBIBDs, are designs for which the property of balance of BIBD is relaxed. They are based on an association scheme. We introduce the concept of generalized relative difference sets, generalizing the concept of relative difference sets introduced by A.T. Butson[2] in 1963. We obtain a PBIBD from a generalized relative difference set translating by cyclic automorphisms.

On the other hand, certain amorphous association schemes over the extension rings of $Z/4Z$ were classified[6]. In this paper, we give a necessary and sufficient condition for the existence of generalized relative difference sets associated with these amorphous association schemes which give rise to PBIBDs, under some conditions. In the last section, we give examples of generalized relative difference sets associated with amorphous association schemes of

class 3 for the case when the degree of an extension of $Z/4Z$ is 3 and 4.

1 Generalized Relative Difference Sets and PBIBDs

A.T. Butson[2] introduced the concept of relative difference sets in 1963. Relative difference sets are useful for construction of Hadamard matrices and D-optimal designs. See Spence[12,13,14] and Koukouvinos, Kounias and Seberry [9].

We recall the definition of relative difference sets.

Definition. Let G be an additive abelian group of order v and D be a subset of G containing k elements. Let H be a subgroup of G of order h. If for $d \neq 0$, $d \in G$, the number of pairs (r, s) such that $d = r - s$, $r, s \in D$, has fixed values

$$\begin{cases} \lambda & \text{when } d \notin H, \\ 0 & \text{when } d \in H, \end{cases}$$

then D is called a *relative difference set.*

We extend this concept.

Definition. Let G be an additive abelian group of order v and D be a subset of G containing k elements. Let H_1, H_2, ... H_t be subsets of G such that

$$G = \{0\} \cup H_1 \cup H_2 \cup \dots \cup H_t, \quad H_i \cap H_j = \emptyset, \text{ for } i \neq j.$$

If for $d \neq 0$, $d \in G$, the number of pairs (r, s) such that $d = r - s$, $r, s \in D$ has fixed values

$$\begin{cases} \lambda_1 & \text{when } d \in H_1, \\ \lambda_2 & \text{when } d \in H_2, \\ \vdots & \quad \vdots \\ \lambda_t & \text{when } d \in H_t, \end{cases}$$

then $D = R[k, \lambda_1, \lambda_2, \ldots, \lambda_t; v]$ is called a *generalized relative difference set.*

Partially balance incomplete block designs were introduced by Bose and Nair[2] in 1939. They are designs for which the property of balance of a BIBD is relaxed and based on an association scheme.

We give the definition of association schemes first.

Definition. Let X be a v-set and R_i, $0 \leqq i \leqq d$, be subsets of $X \times X$ which satisfy

(i) $R_0 = \{(x, x) \mid x \in X\}$,

(ii) $X \times X = R_0 \cup \ldots \cup R_d$, $R_i \cap R_j = \emptyset$ $(i \neq j)$,

(iii) $R_i^t = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$ where $R_i^t = \{(x, y) \mid (y, x) \in R_i\}$,

(iv) for $i, j, k \in \{0, 1, \ldots, d\}$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is constant whenever $(x, y) \in R_k$. This constant is denoted by p_{ij}^k.

Then $\mathcal{X} = (X, \{R_i\}_{0 \leqq i \leqq d})$ is called an *association scheme of class d on X*. Furthermore, if

(v) $p_{ij}^k = p_{ji}^k$

is satisfied, then $\mathcal{X}$ is called a *commutative association scheme of class d on X*. An association scheme with the property

$i' = i$

is called *symmetric* or *Bose-Mesner type.*

Definition. Let X be a v-set and $B_1, \ldots, B_b$ be subsets of X with k elements which are called blocks. Assume that there exists an association scheme of class t on X. If $B_1, \ldots, B_b$ satisfy

(i) each element of X occurs in exactly r blocks,

(ii) if $(x, y) \in R_i$, then the pair (x, y) occurs in λ_i blocks, then $\mathscr{B} = \{B_1,\dots,B_b\}$ is called a *partially balanced incomplete block design* and is abbreviated to a PBIBD. We denote this by $PB[k, \lambda_1,\dots,\lambda_t;v]$.

There are relations between the parameters of a PBIBD.

Lemma 1. (i) $vr = bk$,

(ii) $\sum_{i=1}^{d} k_i \lambda_i = r(k-1)$,

where k_i *is the number of elements* $y \in X$ *such that* $(x, y) \in R_i$ *for fixed* $x \in X$. *We call* k_i *the valency of* R_i.

Theorem 2. *Assume that there exists a* $PB[k, \lambda_1,\dots,\lambda_t;v]$ *over an additive abelian group and* $v = b$. *Moreover assume that every block* B_l *is a translate of* $B_1 = \{a_1,\dots, a_k\}$, *that is*

$$B_l = B_1 + c = \{a_1+c, a_2+c, \dots, a_k+c\}, \quad c \in X.$$

Then B_1 *is a* $R[k, \lambda_1,\dots,\lambda_t;v]$.

Proof. Let $\mathscr{X} = (X, \{R_i\}_{0 \leq i \leq t})$ be an association scheme associated with $PB[k, \lambda_1,\dots,\lambda_t;v]$. Assume that a pair $(0, d)$, $d \neq 0 \in X$, is contained in a relation R_1. Then the pair $(0, d)$ occurs in exactly λ_1 blocks. Since every block is a translate of B_1, there exist exactly λ_1 pairs (a_i, a_j) in block B_1 such that

$$a_i + l = 0, \qquad a_j + l = d, \qquad l \in X.$$

Namely, it means that there exist exactly λ_1 pairs (a_i, a_j) in B_1 such that $d = a_j - a_i$. We proceed similarly in the cases when a pair $(0, d)$ is contained in $R_2, R_3, \dots, R_t$ respectively. Thus we get $B_1 = R[k, \lambda_1,\dots,\lambda_t;v]$.

The converse of Theorem 2 is not always true.

Theorem 3. *Let* $D = R[k, \lambda_1,\dots,\lambda_t;v]$ *and* $\mathscr{X} = (X, \{R_i\}_{0 \leq i \leq t})$ *be an* *association scheme over an additive abelian group. Assume that a pair* (a, b) *belongs to a relation* R_i *when* $d = a - b \in H_i$, $0 \leq i \leq t$. *Then* D *and translates of* D, $D_l = D + c$, $c \in X$, *become* $PB[k, \lambda_1, \ldots, \lambda_t; v]$.

Proof. There are exactly λ_1 pairs (a, b) in D such that $d = a - b \in H_1$. For these λ_1 pairs (a, b), we have pairs (r, s), $r = a + l$, $s = b + l$, where r and s belong to block B_l. That is, a pair (r, s) which belongs to a relation R_1 occurs λ_1 blocks. Proceeding similarly in cases when $d \in H_2$, ..., $d \in H_t$, we can get the result of the theorem.

We call this *generalized relative difference set associated with an association scheme* $\mathcal{X}$.

2. Amorphous Association Schemes

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a commutative association scheme.

Definition. A partition $\Lambda_0, \Lambda_1, \ldots, \Lambda_e$ of the index set $\{0,1,\ldots,d\}$ of the association relations is said to be *admissible* if $\Lambda_0 = \{0\}$, $\Lambda_i \neq \emptyset$, $1 \leq i \leq e$ and $\Lambda'_i = \Lambda_j$ for some j $1 \leq i,j \leq e$, where $\Lambda'_i = \{\alpha' \mid \alpha \in \Lambda_i\}$, $R_{\alpha'} = \{(x, y) \mid (y, x) \in R_\alpha\}$. Let $R_{\Lambda_i} = \cup_{\alpha \in \Lambda_i} R_\alpha$. If $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq e})$ becomes an association scheme, it is called a *fusion scheme* of $\mathcal{X}$. $\mathcal{X}$ is defined to be *amorphous* if every admissible partition gives rise to a fusion scheme.

Amorphous association schemes are closely related to Hadamard matrices. A.V. Ivanov[8] proved that if $\mathcal{X}$ is amorphous and symmetric, and class d is greater than 2, either $\Upsilon_i = (X, R_i)$ is a stongly regular graph of Latin square type for each i $(i \neq 0)$ or Υ_i is of negative Latin square type for each i $(i \neq 0)$. Moreover it was proved the converse is also true[6]. Goethals-Seidel[5] showed that the existence matrices with constant diagonal is equivalent to the existence of strongly regular graph of Latin square type or of negative Latin square type. In other words, there exist symmetric Hadamard matrices of order $4s^2$ with constant diagonal if and only if there exists a symmetric amorphous association schemes and (X, R_i) belongs to $L_s(2s)$ or $NL_s(2s)$. Ito-Munemasa-Yamada[6] generalize the Goethals-Seidel's theorem partially by introducing the concept of nonsymmetric amorphous association schemes.

There is another relation between Hadamard matrices and amorphous association scheme. A.A. Ivanov-Chuvaeva[7] showed certain amorphous association schemes of class 4 can be obtained from Hadamard matrices.

3. An Extension Ring of $Z/4Z$.

Let $F = GF(2)$ be a finite field with 2 elements and $\varphi(x) = x^s + a_1 x^{s-1} + \dots + a_s$ be a primitive polynomial of degree s over F. Let $\Phi(x) = x^s + \alpha_1 x^{s-1} + \dots + \alpha_s$ be a polynomial over $\boldsymbol{Z}_4 = \boldsymbol{Z}/4\boldsymbol{Z}$ obtained from $\varphi(x)$ such that $\alpha_i \equiv a_i \pmod 2$, $1 \leqq i \leqq s$. There is a unique polynomial $\Phi(x)$ whose root ξ satisfies $\xi^{2^s-1} = 1$.

The ring $\mathcal{R} = \boldsymbol{Z}_4[\xi]$ is an algebraic extension of $\boldsymbol{Z}_4$ and has the radical $\mathcal{P} = 2\mathcal{R}$. The residue class field $\mathcal{R}/\mathcal{P}$ is isomorphic with an extension $K = GF(2^s)$. We can take the Teichmüller system $\mathcal{T} = \{0, 1, \xi, \dots, \xi^{2^s-2}\}$ as a set of representatives of $\mathcal{R}/\mathcal{P}$.

Therefore an arbitrary element α of $\mathcal{R}$ is uniquely represented as

$$\alpha = \alpha_0 + 2\alpha_1 \quad \alpha_0, \alpha_1 \in \mathcal{T}.$$

All the regular elements $\mathcal{R}^*$ of $\mathcal{R}$ forms a multiplicative group of order $2^s(2^s-1)$.

When we put $\alpha_0 = \tau(\alpha)$, then τ is a homomorphism of $\mathcal{R}^*$ into the cyclic group M generated by ξ. The kernel of τ is the group $\mathcal{E}$ of principal units, namely of elements of the form $1 + 2\beta$, $\beta \in \mathcal{I}$. More precisely, τ is given as

$$\tau(\alpha) = \alpha^{2^s}.$$

For a principal unit $\varepsilon = 1 + 2\beta$ we can regard β as an element of K. For $1 + 2l$, $1 + 2m \in \mathcal{E}$, we have

$$(1 + 2l)(1 + 2m) = (1 + 2(l+m)), \quad l,m \in K.$$

Hence the group $\mathcal{E}$ is an elementary abelian group of order 2^s and isomorphic with the additive group of K.

Thus $\mathcal{R}^*$ is a direct product of M and $\mathcal{E}$. That is, an arbitrary element α of $\mathcal{R}^*$ is uniquely represented as

$$\alpha = \xi^m \varepsilon = \xi^m(1 + 2a), \quad \varepsilon \in \mathcal{E}, \quad \varepsilon - 1 \in \mathcal{P}, \quad a \in K.$$

4. Multiplicative Characters and Additive Characters of $\mathcal{R}$.

For any element $\alpha = \alpha_0 + 2\alpha_1 \in \mathcal{R}$, we define the element α^f as

$$\alpha^f = \alpha_0^2 + 2\alpha_1^2.$$

Hence f is a ring-automorphism of $\mathcal{R}$, and we call this the *Frobenius automorphism*. The set of elements of $\mathcal{R}$ invariant under the Frobenius automorphism f is identical with $\mathbf{Z}_4$.

Definition. We define the *relative trace from* $\mathcal{R}$ *to* $\mathbf{Z}_4$:

$$S_{\mathcal{R}/\mathbf{Z}_4}\alpha = \alpha + \alpha^f + \dots + \alpha^{f^{2^{s-2}}}.$$

A multiplicative character χ of $\mathcal{R}^*$ is defined by

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta),$$

and each value of $\chi(\alpha)$ is a $2^s(2^s-1)$-th root of unity. We extend χ as the character of $\mathcal{R}$ by defining $\chi(\alpha) = 0$, for any element α in $\mathcal{P}$. We call this the multiplicative character of $\mathcal{R}$. The principal character χ_0 of $\mathcal{R}$ is defined by $\chi_0(\alpha) = 1$, for any element α in $\mathcal{R}^*$.

We treat multiplicative characters χ of $\mathcal{R}$ which satisfy $\chi^2 = \chi_0$. Since $\chi^2(\xi) = 1$ and $(2, 2^s - 1) = 1$, we have $\chi(\xi) = 1$, and χ induces a character of $\mathcal{E}$. Hence we can regard a multiplicative character χ of $\mathcal{R}$ as an additive character of K, because $\mathcal{E}$ is isomorphic with the additive group of K.

Lemma 4. *All additive characters ϕ_l of a finite filed K are given as follows:*

$$\phi_l(a) = (-1)^{S_{K/F} la}, \quad \text{for } l \in K$$

where $S_{K/F}$ is the relative trace from K to F.

Thus the multiplicative character $\chi = \chi_l$ of $\mathcal{R}$ which satisfies $\chi^2 = \chi_0$ is given by

$$\chi(\alpha) = \chi_l(1+2a) = \phi_l(a) = (-1)^{S_{K/F} la}.$$

Next we consider additive characters of $\mathcal{R}$.

Lemma 5. *All the additive characters λ_β of $\mathcal{R}$ are represented as*

$$\lambda_\beta(\alpha) = i^{S_{\mathcal{R}/Z_4} \beta\alpha} \qquad \text{for } \beta \in \mathcal{R}$$

where i is the primitive fourth root of unity.

Proof. See [17].

Next we define three kinds of Jacobi sums associated with multiplicative characters over $\mathcal{R}$.

Definition. For multiplicative characters χ_l and χ_m, we define three kinds of *Jacobi sums*:

$$J(\chi_l, \chi_m) = \sum_{\alpha \in \mathcal{R}} \chi_l(\alpha)\chi_m(1-\alpha),$$

$$J_2(\chi_l, \chi_m) = \sum_{\alpha \in \mathcal{R}} \chi_l(\alpha)\chi_m(2-\alpha),$$

$$J_0(\chi_l, \chi_m) = \sum_{\alpha \in \mathcal{R}} \chi_l(\alpha)\chi_m(-\alpha).$$

The following theorem gives explicit forms of Jacobi sums.

Theorem 6. *For the multiplicative character* χ_l *and* χ_m *such that* $\chi_l, \chi_m, \chi_{l+m} \neq \chi_0$, *we get*

$$(1)\quad \begin{cases} J(\chi_0, \chi_0) = 2^s(2^s-2), \\ J(\chi_l, \chi_0) = 0, \\ J(\chi_l, \chi_l) = 0, \\ J(\chi_l, \chi_m) = \chi_{lm}(-1)2^s, \end{cases} \qquad (2)\quad \begin{cases} J_2(\chi_0, \chi_0) = 2^s(2^s-1), \\ J_2(\chi_l, \chi_0) = 0, \\ J_2(\chi_l, \chi_l) = -\chi_l(-1)2^s, \\ J_2(\chi_l, \chi_m) = 0, \end{cases}$$

$$(3)\quad \begin{cases} J_0(\chi_0, \chi_0) = 2^s(2^s-1), \\ J_0(\chi_l, \chi_0) = 0, \\ J_0(\chi_l, \chi_l) = \chi_l(-1)2^s(2^s-1), \\ J_0(\chi_l, \chi_m) = 0. \end{cases}$$

Proof. See [17].

The following thoerem on character sum is useful.

Lemma 7.

$$\sum_{\beta \in \mathcal{R}^*} \chi_l(\beta)\chi_m(\alpha - \beta) = \begin{cases} \chi_l\chi_m(\alpha)J(\chi_l, \chi_m) & \text{when } \alpha \in \mathcal{R}^*, \\ \chi_l\chi_m\left[\frac{\alpha}{2}\right]J_2(\chi_l, \chi_m) & \text{when } \alpha \in \mathcal{P} \text{ and } \alpha \neq 0, \\ J_0(\chi_l, \chi_m) & \text{when } \alpha = 0. \end{cases}$$

Proof. See [17].

6 Amorphous Association Schemes over $\mathcal{R}$

Now we consider association schemes over $\mathcal{R}$. Let $\mathcal{X} = (\mathcal{R}, \{R_\alpha\}_{\alpha \in \mathcal{R}})$ be the association scheme for which $(\beta, \gamma) \in \mathcal{R} \times \mathcal{R}$ is in R_α if $\beta - \gamma = \alpha$. Let E_a be a coset by M in $\mathcal{R}$ containing $1 + 2a$, namely the direct product of M and a principal unit $\varepsilon = 1 + 2a$:

$$E_a = \{\xi^m \varepsilon = \xi^m(1 + 2a), m=0, \dots, 2^s-2, \ a \in K\}.$$

For a subgroup H of the additive group K, form a subgroup $M(1 + 2H) = \cup_{a \in H} E_a$ of $\mathcal{R}^*$. Denote the coset of $M(1 + 2H)$ by $C_a = M(1 + 2(H+a))$. We fuse the association relations of $\mathcal{X}$ to form

$$\begin{aligned} R_0 &= \{(\alpha, \alpha) \mid \alpha \in \mathcal{R}\}, \\ R_2 &= \cup_{\alpha \in \mathcal{P}-\{0\}} R_\alpha, \\ R_a &= \cup_{\alpha \in C_a} R_\alpha. \end{aligned} \tag{1}$$

Let us introduce a nondegenerate symmetric bilinear form on K over F by

$$(a, b) = S_{K/F}ab$$

For a subgroup H of K, $H^\perp$ denotes the orthogonal complement of H , i.e.

$$H^\perp = \{a \in K \mid S_{K/F}(a, b) = 0 \quad \text{for all } b \in H\}.$$

Notice that $-1 = 1 + 2 \cdot 1 \in \mathcal{E}$ and so $-M(1 + 2(H + a)) = M(1 + 2(H + a + 1))$, i.e. $-C_a = C_{a+1}$. This means $R_a^t = R_{a+1}$ for $a \in K/H$. Therefore $\mathcal{X}_H$ is symmetric if and only if $1 \in H$. Furthermore notice that $<1>^{\perp}$, the orthogonal complement of the subspace spanned by 1, is the set of isotropic elements in K, since $(l, l) = S_{K/F}l^2 = S_{K/F}l = (1, l)$.

Theorem 8. *For a subgroup H of K, let $\mathcal{X}_H$ be the association scheme over $\mathcal{R}$ with association relation given by* (1). *Then $\mathcal{X}_H$ is symmetric and amorphous if and only if $H^{\perp}$ is totally isotropic subspace of K.*

Proof. See [6].

7. Characteristic Functions

Let D be a subset of K containing 2^{s-1} elements, not necessarily a subgroup. We give a necessary and sufficient condition that the union $\mathcal{D} = \cup_{a \in D} E_a = M(1 + 2D)$ becomes a generalized relative difference set associated with the amorphous association scheme over $\mathcal{R}$ in Theorem 8. So we can obtain PBIBDs over amorphous association schemes translating by cyclic automorphisms.

Lemma 9. *The characteristic function $f_a(\alpha)$ of E_a is given by*

$$f_a(\alpha) = 2^{-s} \sum_{l \in K} \chi_l(1 + 2a) \chi_l(\alpha).$$

From this Lemma, we obtain the characteristic function $F(\alpha)$ of $M(1 + 2D)$, a direct product of M and the set of principal units determined by a subset D of K, as

$$F(\alpha) = 2^{-s} \sum_{l \in K} \omega_l \chi_l(\alpha),$$

where $\omega_l = \sum_{a \in D} \chi_l(1 + 2a)$.

We define the group $\Omega = \{x^g, g \in \mathcal{R}\}$ isomorphic with $\mathcal{R}$ by the relation $x^g x^{g'} = x^{g+g'}$. Moreover we define the element $\mathcal{F}(x)$ of the group ring $\Omega \boldsymbol{Z}$ by

$$\mathcal{F}(x) = \sum_{\alpha \in \mathcal{R}} F(\alpha)x^{\alpha} = 2^{-s} \sum_{\alpha \in \mathcal{R}} \sum_{l \in K} \omega_l \chi_l(\alpha) x^{\alpha}.$$

8. Main Theorem

We have to verify

$$\mathcal{F}(x)\mathcal{F}(x^{-1}) = 2^{s-1}(2^s - 1) + \lambda_0 \sum_{\alpha \in \mathcal{P}^*} x^{\alpha} + \sum_{a \in K/H} \lambda_a \sum_{\alpha \in \mathcal{R}} x^{\alpha}.$$

We represent the left-hand side of the relation above by using Jacobi sums.

$$\begin{aligned}\mathcal{F}(x)\mathcal{F}(x^{-1}) &= 2^{-s} \sum_{\beta \in \mathcal{R}} \sum_{l \in K} \omega_l \chi_l(\beta) x^{\beta} \cdot 2^{-s} \sum_{\gamma \in \mathcal{R}} \sum_{m \in K} \omega_m \chi_m(\gamma) x^{-\gamma} \\ &= 2^{-2s} \sum_{l \in K} \sum_{m \in K} \omega_l \omega_m \sum_{\beta \in \mathcal{R}} \sum_{\gamma \in \mathcal{R}} \chi_l(\beta) \chi_m(\gamma) x^{\beta - \gamma}.\end{aligned}$$

Putting $\beta - \gamma = \alpha$, we have

$$\mathcal{F}(x)\mathcal{F}(x^{-1}) = 2^{-2s} \sum_{l \in K} \sum_{m \in K} \omega_l \omega_m \sum_{\alpha \in \mathcal{R}} \sum_{\beta \in \mathcal{R}} \chi_l(\beta) \chi_m(\beta - \alpha) x^{\alpha}.$$

Denote the multiplicative group of K by K^* and $\mathcal{P} - \{0\}$ by $\mathcal{P}^*$. From Lemma 7, we obtain

(a)
$$\begin{aligned}&2^{-2s} \sum_{l \in K} \sum_{m \in K} \omega_l \omega_m \chi_m(-1) J_0(\chi_l, \chi_m) \\ &= 2^{-2s}\{\omega_0^2 \chi_0(-1) J_0(\chi_0, \chi_0) + \sum_{l \in K^*} \omega_l^2 \chi_l(-1) J_0(\chi_l, \chi_l)\} \\ &= 2^{-s}(2^s - 1)\{\omega_0^2 + \sum_{l \in K^*} \omega_l^2\} \\ &= 2^{s-1}(2^s - 1),\end{aligned}$$

(b)
$$\begin{aligned}&2^{-2s} \sum_{l \in K} \sum_{m \in K} \omega_l \omega_m \sum_{\alpha \in \mathcal{P}^*} \chi_l \chi_m \left[\frac{\alpha}{2}\right] \chi_m(-1) J_2(\chi_l, \chi_m) x^{\alpha} \\ &= 2^{-2s}\{\omega_0^2 \sum_{\alpha \in \mathcal{P}^*} \chi_0^2 \left[\frac{\alpha}{2}\right] \chi_0(-1) J_2(\chi_0, \chi_0) x^{\alpha} \\ &\quad + \sum_{l \in K^*} \omega_l^2 \sum_{\alpha \in \mathcal{P}^*} \chi_l^2 \left[\frac{\alpha}{2}\right] \chi_l(-1) J_2(\chi_l, \chi_l) x^{\alpha}\} \\ &= 2^{-2s}\{2^{2(s-1)} 2^s (2^s - 1) \sum_{\alpha \in \mathcal{P}^*} x^{\alpha} - 2^s \sum_{l \in K^*} \omega_l^2 \sum_{\alpha \in \mathcal{P}^*} x^{\alpha}\}\end{aligned}$$

$$= 2^{s-1}(2^{s-1}-1) \sum_{\alpha \in \mathcal{P}^*} x^{\alpha},$$

(c) $$2^{-2s} \sum_{l \in K} \sum_{m \in K} \omega_l \omega_m \sum_{\alpha \in \mathcal{R}^*} \chi_l \chi_m(\alpha) \chi_m(-1) J(\chi_l, \chi_m) x^{\alpha}$$

$$= 2^{-2s}\{\omega_0^2 \sum_{\alpha \in \mathcal{R}^*} \chi_0(\alpha)\chi_0(-1)J(\chi_0, \chi_0)x^{\alpha}$$

$$+ \sum_{l \in K^*} \sum_{\substack{m \in K^* \\ m \neq l}} \omega_l \omega_m \sum_{\alpha \in \mathcal{R}^*} \chi_l \chi_m(\alpha) \chi_m(-1) J(\chi_l, \chi_m) x^{\alpha}\}$$

$$= 2^{s-1}(2^{s-1}-1) \sum_{\alpha \in \mathcal{R}^*} x^{\alpha}$$

$$+ 2^{-s} \sum_{l \in K^*} \sum_{\substack{m \in K^* \\ m \neq l}} \omega_l \omega_m \sum_{\alpha \in \mathcal{R}^*} \chi_l \chi_m(\alpha) \chi_m(-1) \chi_{lm}(-1) x^{\alpha}.$$

Therefore,

$$\mathcal{F}(x)\mathcal{F}(x^{-1}) = 2^{s-1}(2^s-1) + 2^{s-1}(2^{s-1}-1) \sum_{\alpha \in \mathcal{P}^*} x^{\alpha} + 2^{s-1}(2^{s-1}-1) \sum_{\alpha \in \mathcal{R}^*} x^{\alpha} + 2^{-s}\Delta,$$

where $$\Delta = \sum_{l \in K^*} \sum_{\substack{m \in K^* \\ m \neq l}} \omega_l \omega_m \sum_{\alpha \in \mathcal{R}^*} \chi_l(\alpha) \chi_m(\alpha) \chi_m(-1) \chi_{lm}(-1) x^{\alpha}.$$

Denote the coefficient of x^{α}, $\alpha = \xi^m(1 + 2a)$, by Γ_a,

$$\Gamma_a = \sum_{l \in K^*} \sum_{\substack{m \in K^* \\ m \neq l}} \omega_l \omega_m \chi_l(\alpha) \chi_m(\alpha) \chi_m(-1) \chi_{lm}(-1)$$

$$= \sum_{l \in K^*} \sum_{\substack{m \in K^* \\ m \neq l}} \omega_l \omega_m (-1)^{S_{K/F} m(1+l)} (-1)^{S_{K/F}(l+m)a}. \qquad (2)$$

Lemma 10. $\Gamma_a = \Gamma_{a+1}$.

Proof. Replacing a of the equation (2) by $a+1$, we can easily obtain the result.

The subset $\mathcal{D} = M(1 + 2D)$ becomes a generalized relative difference set associated with an amorphous association scheme over $\mathcal{R}$ if and only if $\Gamma_{a+h} = \Gamma_a$ for every $a \in K$ and for every $h \in H$.

When we put $k = l + m$, the equation (2) is equivalent to

$$\Gamma_a = \sum_{k\in K^*} \sum_{\substack{m\in K^* \\ m\neq k}} \omega_{k-m}\omega_m(-1)^{S_{K/F}k(m+a)}.$$

Extending this sum to contain the cases $k = 0$, $m = 0$ and $m = k$, we have

$$\sum_{k\in K}\sum_{m\in K} \omega_{k-m}\omega_m(-1)^{S_{K/F}k(m+a)} = \Gamma_a + 2^{s-1}\sum_{k\in K}(-1)^{S_{K/F}ka}\omega_k(1+\chi_k(-1)).$$

Furthermore we put $u_k = \sum_{m\in K}\omega_{k-m}\omega_m(-1)^{S_{K/F}km}$, we obtain

$$\Gamma_a = \sum_{k\in K}(-1)^{S_{K/F}ka}u_k - 2^s \sum_{\substack{k\in K \\ S_{K/F}k=0}}(-1)^{S_{K/F}ka}\omega_k.$$

Observe that $\sum_{\substack{k\in K \\ S_{K/F}k=1}}(-1)^{S_{K/F}ka}u_k = 0$, since $\Gamma_a = \Gamma_{a+1}$ from Lemma 10. Hence

$$\Gamma_a = \sum_{\substack{k\in K \\ S_{K/F}k=0}}(-1)^{S_{K/F}ka}(u_k - 2^s\omega_k) = \sum_{\substack{k\in K \\ S_{K/F}k=0}}(-1)^{S_{K/F}ka}V_k$$

where $V_k = u_k - 2^s\omega_k$.

Theorem 11. *Let D be a subset of K containing 2^{s-1} elements and H be a subgroup of K which satisfies the condition of Theorem 8. The subset $\mathcal{D} = M(1 + 2D)$ becomes a $R[2^{s-1}(2^s-1);\lambda_a,\lambda_b,\ldots;2^{2s}]$, $a, b \in K/H$, associated with $\mathcal{X}_H$ if and only if*

$$\sum_{\substack{b\in D \\ b\notin(D+k)}}(-1)^{S_{K/F}kb} = 0 \qquad \text{for all } k \text{ such that } k\in\langle 1\rangle^{\perp} \text{ and } k\notin H^{\perp}.$$

Then the multiplicity is given by

$$\lambda_a = 2^{s-1}(2^{s-1}-1) - \sum_{k\in H^{\perp}}(-1)^{S_{K/F}ka}\sum_{\substack{b\in D \\ b\notin(D+k)}}(-1)^{S_{K/F}kb}.$$

Proof. The subset $\mathscr{D} = M(1 + 2D)$ in $\mathscr{R}^*$ becomes $R[2^{s-1}(2^s - 1); \lambda_a, \lambda_b, \ldots; 2^{2s}]$ associated with $\mathscr{X}_H$ if and only if

$$\Gamma_{a+h} = \Gamma_a, \qquad \forall a \in K, \ \forall h \in H.$$

Let $\pi = \langle 1 \rangle^{\perp} = \{h \mid S_{K/F}h = 0\}$.

$$\begin{aligned}\Gamma_{a+h} - \Gamma_a &= \sum_{k\in\pi} (-1)^{S_{K/F}(a+h)k} V_k - \sum_{k\in\pi} (-1)^{S_{K/F}ka} V_k \\ &= \sum_{k\in\pi} (-1)^{S_{K/F}ka} (1 - (-1)^{S_{K/F}kh}) V_k.\end{aligned}$$

It implies

$$\sum_{\substack{k\in\pi \\ k\notin H^{\perp}}} (-1)^{S_{K/F}ka} V_k = 0.$$

From the orthogonality relations of characters, we have

$$V_k = 0.$$

for all k such that $k \in \pi$ and $k \notin H^{\perp}$. Hence

$$\Gamma_a = \sum_{k\in H^{\perp}} (-1)^{S_{K/F}ka} V_k.$$

We transform u_k to a simpler form.

$$\begin{aligned}u_k &= \sum_{m\in K} \omega_m \omega_{k-m} (-1)^{S_{K/F}km} \\ &= \sum_{m\in K} \sum_{b\in D} (-1)^{S_{K/F}mb} \sum_{c\in D} (-1)^{S_{K/F}(k-m)c} (-1)^{S_{K/F}km} \\ &= \sum_{b\in D} \sum_{c\in D} (-1)^{S_{K/F}kc} \sum_{m\in K} (-1)^{S_{K/F}m(b-c+k)}.\end{aligned}$$

The sum $\sum_{m\in K} (-1)^{S_{K/F}m(b-c+k)} = 2^s$ only if $c = b + k$, and it is equal to 0 otherwise. Hence

$$u_k = 2^s (-1)^{S_{K/F}k} \sum_{b\in D\cap(D+k)} (-1)^{S_{K/F}bk}.$$

Substituting this to $V_k = u_k - 2^s \omega_k$, we have

$$V_k = 2^s \sum_{b\in D\cap(D+k)} (-1)^{S_{K/F}bk} - 2^s \sum_{b\in D} (-1)^{S_{K/F}kb}$$
$$= 2^s \sum_{\substack{b\in D \\ b\notin(D+k)}} (-1)^{S_{K/F}bk}.$$

Thus

$$\Gamma_a = 2^s \sum_{k\in H^{\perp}} (-1)^{S_{K/F}ak} \sum_{\substack{b\in D \\ b\notin(D+k)}} (-1)^{S_{k/F}bk}$$

This leads to the multiplicity.

Corollary 12. *The subset* $\mathscr{D}$ *is a* $(2^{2s}, 2^{s-1}(2^s - 1), 2^{s-1}(2^{s-1} - 1))$ *difference set if and only if*

$$\mathcal{V}_k = \sum_{\substack{b\in D \\ b\notin(D+k)}} (-1)^{S_{K/F}bk} = 0$$

for all $k\in\pi$.

Proof. Assume that $\mathcal{V}_k = 0$, that is $V_k = 0$. Then it can be easily proved that $\mathscr{D}$ becomes a $(2^{2s}, 2^{s-1}(2^s - 1), 2^{s-1}(2^{s-1} - 1))$ difference set from Theorem 11. Now we assume $\mathscr{D}$ is a $(2^{2s}, 2^{s-1}(2^s - 1), 2^{s-1}(2^{s-1} - 1))$ difference set. Then for all $a\in K$,

$$\Gamma_a = \sum_{k\in H^{\perp}} (-1)^{S_{K/F}ka} V_k = 0$$

must be satisfied. From the orthogonality relation of characters, $V_k = 0$ for all $k\in H^{\perp}$. The assumption implies that $V_k = 0$ for all k such that $k\in\pi$, and $k\notin H^{\perp}$. So we get the result.

Hadamard matrices can be constructed from these difference sets over $\mathscr{R}$.

10. Generalized Relative Difference Sets Associated with Amorphous Association Schemes of Class 3 over $\mathscr{R}$

amorphous association scheme $\mathcal{X} = (\mathcal{R}, \{0\}, \mathcal{P}^*, R_0, R_a)$ of class 3 for the cases $s = 3$ and $s = 4$. We have only to verify that either $\Gamma_a = \Gamma_0$ or $\Gamma_a = -\Gamma_0$ is satisfied for all $a \in K$ and for the subset D which satisfies a necessary and sufficient condition of Theorem 11. It is equivalent to verify that either

$$\sum_{\substack{k \in H^\perp \\ S_{K/F}ka = 1}} v_k = \sum_{\substack{k \in H^\perp \\ S_{K/F}ka = 1}} \sum_{\substack{b \in D \\ b \notin (D+k)}} (-1)^{S_{K/F}bk} = 0$$

or

$$\sum_{\substack{k \in H^\perp \\ S_{K/F}ka = 0}} v_k = \sum_{\substack{k \in H^\perp \\ S_{K/F}ka = 0}} \sum_{\substack{b \in D \\ b \notin (D+k)}} (-1)^{S_{K/F}bk} = 0$$

must be satisfied for every $a \in K$, where H is a subgroup of K of index 2 which satifies the condition of Theorem 8.

When reduced by the equivalence relation based on translations, we obtain the following generalized relative difference sets over $\mathcal{R}$. Denote a primitive element of K by g. The primitive polynomial is given by $x^3 = x^2 + 1$ for $s = 3$ and $x^4 = x + 1$ for $s = 4$.

The case $s = 3$.

A subgroup which gives rise to an amorphous association scheme of class 3:	Generalized relative difference sets:
$0, 1, g^2, g^3$	$\{0, 1, g, g^4\}$ $\{0, g, g^3, g^5\}$
$0, 1, g, g^5$	$\{0, 1, g^2, g^4\}$ $\{0, g^2, g^3, g^5\}$
$0, 1, g^4, g^6$	$\{0, 1, g, g^2\}$ $\{0, g, g^5, g^6\}$

The case $s = 4$.

A subgroup which gives rise to an association scheme of class 3	
Generalized relative difference sets	
$0, 1, g, g^2, g^4, g^5, g^8, g^{10}$	
$0, 1, g, g^3, g^4, g^6, g^7, g^{12}$	$0, g^2\ g^3, g^4, g^7, g^9, g^{10}, g^{14}$
$0, 1, g, g^3, g^4, g^6, g^9, g^{11}$	$0, g, g^2, g^3, g^5, g^7, g^9, g^{14}$
$0, 1, g, g^3, g^4, g^7, g^{11}, g^{13}$	$0, g^4\ g^5, g^6, g^8, g^{11}, g^{12}, g^{13}$
$0, 1, g, g^3, g^4, g^9, g^{12}, g^{13}$	$0, g, g^3, g^7, g^8, g^9, g^{10}, g^{14}$
$0, 1, g^2, g^3, g^6, g^7, g^8, g^{12}$	$0, g^2\ g^3, g^4, g^6, g^{10}, g^{13}, g^{14}$
$0, 1, g^2, g^3, g^6, g^8, g^9, g^{11}$	$0, g, g^2, g^3, g^5, g^6, g^{13}, g^{14}$
$0, 1, g^2, g^3, g^7, g^8, g^{11}, g^{13}$	$0, g^3, g^4, g^5, g^6, g^8, g^{13}, g^{14}$
$0, 1, g^2, g^3, g^8, g^9, g^{12}, g^{13}$	$0, g, g^3, g^6, g^8, g^{10}, g^{13}, g^{14}$
$0, 1, g^3, g^5, g^6, g^7, g^{10}, g^{12}$	$0, g^2, g^3, g^4, g^{10}, g^{11}, g^{12}, g^{14}$
$0, 1, g^3, g^5, g^6, g^9, g^{10}, g^{11}$	$0, g, g^2, g^3, g^5, g^{11}, g^{12}, g^{14}$
$0, 1, g^3, g^5, g^7, g^{10}, g^{11}, g^{13}$	$0, g^3, g^4, g^5, g^8, g^{11}, g^{12}, g^{14}$
$0, 1, g^3, g^5, g^9, g^{10}, g^{12}, g^{13}$	$0, g, g^3, g^8, g^{10}, g^{11}, g^{12}, g^{14}$

$s = 4$ (continued).

$0, 1, g^2, g^3, g^6, g^8, g^{13}, g^{14}$	
$0, 1, g, g^2, g^7, g^8, g^{10}, g^{11}$	$0, g, g^4, g^5, g^6, g^8, g^{10}, g^{14}$
$0, 1, g, g^2, g^8, g^9, g^{10}, g^{12}$	$0, g, g^3, g^4, g^5, g^8, g^{10}, g^{13}$
$0, g, g^2, g^3, g^4, g^6, g^7, g^9$	$0, 1, g, g^3, g^5, g^9, g^{11}, g^{14}$
$0, g, g^2, g^3, g^4, g^6, g^{11}, g^{12}$	$0, 1, g, g^5, g^6, g^9, g^{11}, g^{13}$
$0, g, g^2, g^4, g^7, g^9, g^{13}, g^{14}$	$0, 1, g, g^3, g^5, g^7, g^{12}, g^{14}$
$0, g, g^2, g^4, g^{11}, g^{12}, g^{13}, g^{14}$	$0, 1, g, g^5, g^6, g^7, g^{12}, g^{13}$
$0, 1, g^2, g^7, g^8, g^9\ g^{11}, g^{12}$	
$0, 1, g, g^2, g^3, g^5, g^6, g^8$	$0, g, g^2, g^4, g^5, g^9, g^{10}, g^{11}$
$0, 1, g, g^2, g^5, g^8, g^{13}, g^{14}$	$0, g, g^2, g^4, g^5, g^7, g^{10}, g^{12}$
$0, g, g^3, g^4, g^7, g^8, g^{11}, g^{14}$	$0, 1, g, g^6, g^7, g^9, g^{10}, g^{14}$
$0, g, g^3, g^4, g^8, g^9, g^{12}, g^{14}$	$0, 1, g, g^3, g^7, g^9, g^{10}, g^{13}$
$0, g, g^4, g^6, g^7, g^8, g^{11}, g^{13}$	$0, 1, g, g^6, g^{10}, g^{11}, g^{12}, g^{14}$
$0, g, g^4, g^6, g^8, g^9, g^{12}, g^{13}$	$0, 1, g, g^3, g^{10}, g^{11}, g^{12}, g^{13}$
$0, 1, g^3, g^5, g^{10}, g^{11}, g^{12}, g^{14}$	
$0, 1, g, g^2, g^3, g^6, g^9, g^{14}$	$0, g, g^3, g^4, g^5, g^7, g^9, g^{11}$
$0, g, g^2, g^4, g^8, g^{10}, g^{11}, g^{14}$	$0, 1, g, g^5, g^6, g^7, g^8, g^{10}$
$0, 1, g^3, g^4, g^6, g^8, g^9, g^{14}$	$0, g, g^4, g^5, g^7, g^9, g^{12}, g^{14}$
$0, 1, g, g^2, g^6, g^9, g^{11}, g^{12}$	$0, g, g^3, g^4, g^5, g^6, g^{11}, g^{13}$
$0, 1, g, g^2, g^7, g^{11}, g^{12}, g^{13}$	$0, g, g^4, g^5, g^6, g^{12}, g^{13}, g^{14}$
$0, g, g^2, g^3, g^4, g^8, g^{10}, g^{12}$	$0, 1, g, g^5, g^8, g^9, g^{10}, g^{13}$

$s = 4$ (continued).

$0, 1, g^5, g^6, g^7, g^9, g^{10}, g^{13}$	
$0, 1, g, g^2, g^3, g^5, g^{10}, g^{11}$	$0, g, g^2, g^4, g^5, g^6, g^8, g^9$
$0, g, g^4, g^9, g^{10}, g^{11}, g^{12}, g^{13}$	$0, 1, g, g^3, g^6, g^8, g^{12}, g^{13}$
$0, g, g^3, g^4, g^9, g^{10}, g^{13}, g^{14}$	$0, 1, g, g^3, g^7, g^8, g^9, g^{12}$
$0, g, g^4, g^6, g^7, g^{10}, g^{11}, g^{12}$	$0, 1, g, g^6, g^8, g^{11}, g^{13}, g^{14}$
$0, g, g^3, g^4, g^6, g^{7,} g^{10}, g^{14}$	$0, 1, g, g^7, g^8, g^9, g^{11}, g^{14}$
$0, 1, g, g^2, g^5, g^{10}, g^{12}, g^{14}$	$0, g, g^2, g^4, g^5, g^7, g^8, g^{13}$
$0, 1, g, g^3, g^4, g^7, g^9, g^{14}$	
$0, 1, g, g^2, g^4, g^6, g^{10}, g^{12}$	$0, g^2, g^3, g^4, g^5, g^7, g^8, g^{10}$
$0, 1, g, g^2, g^4, g^{10}, g^{11}, g^{13}$	$0, g^2, g^4, g^5, g^8, g^9, g^{10}, g^{14}$
$0, g, g^2, g^3, g^6, g^8, g^9, g^{13}$	$0, 1, g^2, g^3, g^5, g^6, g^{11}, g^{14}$
$0, g, g^2, g^3, g^8, g^9, g^{11}, g^{12}$	$0, 1, g^2, g^5, g^6, g^7, g^9, g^{11}$
$0, g, g^2, g^6, g^7, g^8, g^{13}, g^{14}$	$0, 1, g^2, g^3, g^5, g^{12}, g^{13}, g^{14}$
$0, g, g^2, g^7, g^8, g^{11}, g^{12}, g^{14}$	$0, 1, g^2, g^5, g^7, g^9, g^{12}, g^{13}$
$0, 1, g, g^4, g^6, g^{11}, g^{12}, g^{13}$	
$0, 1, g, g^2, g^3, g^4, g^5, g^9$	$0, g, g^2, g^5, g^6, g^8, g^{10}, g^{11}$
$0, 1, g\ g^2, g^4, g^5, g^7, g^{14}$	$0, g, g^2, g^5, g^8, g^{10}, g^{12}, g^{13}$
$0, g^2, g^3, g^4, g^6, g^8, g^{12}, g^{14}$	$0, 1, g^2, g^3, g^6, g^7, g^{10}, g^{13}$
$0, g^2, g^3, g^4, g^8, g^{11}, g^{13}, g^{14}$	$0, 1, g^2, g^6, g^9, g^{10}, g^{13}, g^{14}$
$0, g^2, g^4, g^6, g^7, g^8, g^9, g^{12}$	$0, 1, g^2, g^3, g^7, g^{10}, g^{11}, g^{12}$
$0, g^2, g^4, g^7, g^8, g^9, g^{11}, g^{13}$	$0, 1, g^2, g^9, g^{10}, g^{11}, g^{12}, g^{14}$

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I : Association schemes*, Benjamin/Cummings, 1984.

[2] R.D. Bose and K.R. Nair, *Partially balanced incompete block designs*, Sankhya **4** (1939), 337–372.

[3] A.T. Butson, *Relations among generalized Hadamard matrices, relative difference sets and maximal length sequences*, Canad. J. Math **15** (1963),42–48.

[4] J.E. Elliott and A.T. Butson, *Relative difference sets*, Illinois J. Math. **10** (1966), 517–531

[5] J.M. Goethals and J.J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math. **12** (1970), 597–614.

[6] T. Ito, A. Munemasa and M. Yamada, *Amorphous association schemes over the Galois rings of characteristic* 4, to appear in European J. Combinatorics.

[7] A.A. Ivanov and I.V. Chubaeva, *Action of the group* M_{12} *on Hadamard matrices*, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for System Science (1985), 159–169 (in Russian).

[8] A.V. Ivanov, *Amorphous cellular rings II*, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for System Science (1985), 104–111 (in Russian).

[9] C. Koukouvinos, S. Kounias and J. Seberry, *Supplementary difference sets and optimal designs*, Discrete Mathematics **88** (1991), 49–58.

[10] R.A. Liebler and R.A. Mena, *Certain distance-regular digraphs and related rings of characteristic* 4, J. Combinatorial Theory (A) **47** (1988), 111–123.

[11] B.R. McDonald, *Finite Rings with Identity*, Dekker, 1974.

[12] E. Spence, *Hadamard matrices from relative difference sets*, J.

combinatorial Theory (A) **19** (1975), 287-300.

[13] E. Spence, *Skew-Hadamard matrices of order* $2(q+1)$, Discrete Mathematics **18** (1977), 79-85.

[14] E. Spence, *Skew-Hadamard matrices of the Goethals-Seidel type*, Canad J. Math. **27** (1975), 555-560.

[15] A.P. Street and D.J. Street, *Combinatorics of Experimental Design*, Oxford Science Publ. 1987.

[16] W.D. Wallis, A.P. Street and J.S. Wallis, *Combinatorics : Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Math. **292** Springer, 1972.

[17] M. Yamada, *Distance-regular digraphs of girth 4 over an extension ring of* $Z/4Z$, Graphs and Combinatorics **6** (1990), 381-394.

[18] K. Yamamoto and M. Yamada, *Hadamard difference sets over an extension of* $Z/4Z$, Utilitas Math. **34** (1988), 169-178.

The author's current address : Department of Mathematics, Kyushu University, Hakozaki, Higashi-ku, Fukuoka 812, Japan