

Nonsymmetric primitive translation schemes of prime power order

Tao Feng · Koji Momihara

Received: 19 May 2013 / Accepted: 5 April 2014 / Published online: 24 April 2014
© Springer Science+Business Media New York 2014

Abstract It is well-known that translation schemes of prime order are exactly the cyclotomic schemes. In this paper, we show that there do not exist any two-, three-, or four-class nonsymmetric primitive translation schemes of prime square order. On the other hand, we find new nonsymmetric four- and five-class association schemes from cyclotomy as fission schemes of certain symmetric three-class association schemes. Moreover, we provide an affirmative answer to the following question raised by Song (J Algebr Comb 5:47–55, 1996): are there any other two-class primitive association schemes that admit symmetrizable fission schemes besides the cyclotomic scheme of index 2 for $q \equiv 5 \pmod{8}$? To be more specific, we show that a certain two-class primitive association scheme in the finite field $\mathbb{F}_{3^{73}}$ constructed by Feng and Xiang (J Comb Theory Ser A 119:245–256, 2012) admits a four-class fission scheme. This fission scheme is realized as a fusion scheme of the cyclotomic scheme of index 28.

Keywords Nonsymmetric primitive translation scheme · Cyclotomic scheme · Gauss sum

1 Introduction

A translation scheme is an association scheme $(X, \{R_i\}_{i=0}^d)$ for which the underlying set X has naturally the structure of an abelian group, and for all relations $R_i \in \mathcal{R}$,

T. Feng
Department of Mathematics, Zhejiang University, Hangzhou, Zhejiang 310027, China
e-mail: tfeng@zju.edu.cn

K. Momihara (✉)
Faculty of Education, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan
e-mail: momihara@educ.kumamoto-u.ac.jp

$(x, y) \in R_i$ implies $(x + z, y + z) \in R_i$ for all $z \in X$. Each relation R_i in a translation scheme corresponds to a subset D_i of X such that $D_i = \{x - y : (x, y) \in R_i\}$. The Bose-Mesner algebra of the translation scheme is isomorphic to the subalgebra of the group algebra $\mathbb{C}[X]$ generated by D_0, \dots, D_d . This subalgebra is also known as a Schur ring. From now on, we shall call $(X, \{D_i\}_{i=0}^d)$ a translation scheme and the subsets D_i 's as relations for convenience. On p. 68 of the book [6], the following conjecture is raised:

Conjecture 1 *Let (X, \mathcal{R}) be a primitive translation scheme. Then one of the following holds: (1) X is elementary abelian, (2) (X, \mathcal{R}) is a Hamming scheme, (3) (X, \mathcal{R}) is of Latin square type or of negative Latin square type.*

An association scheme is of (negative) Latin square type if each of its nontrivial relations is a strongly regular graph of (negative) Latin square type. By A.V. Ivanov's classification, an amorphic association scheme with at least three classes must be of Latin square type or negative Latin square type, cf. [18, 35]. He also conjectured in [21] that if each nontrivial relation in an association scheme is strongly regular, then the association scheme must be amorphic. This conjecture turned out to be false, and all the known primitive counterexamples are constructed in finite fields using the union of cyclotomic classes; please refer to [15] and the references therein for more details. In view of Conjecture 1 and these facts, finite fields and cyclotomy play important roles in the study of primitive association schemes by yielding new association schemes which help us to understand their structures better.

By a well-known theorem due to Hanaki and Uno [19], all association schemes with a prime number of points must be pseudocyclic, which is the analog of the fact that finite groups of prime order must be cyclic. In the translation scheme case, we have the stronger result that a translation scheme with a prime number of points must be a cyclotomic scheme, which is a corollary of the following multiplier theorem of Schur and Wielandt.

Theorem 2 [6, Thm. 2.10.1] *Let (X, \mathcal{R}) be a translation scheme, and let s be an integer coprime to $|X|$. Then for any $R \in \mathcal{R}$, we have $R^{(s)} = \{sx \mid x \in R\} \in \mathcal{R}$.*

In [2, p. 58], the question of when a symmetric association scheme can be split into nonsymmetric commutative association scheme is posed. In [8], the authors considered nonsymmetric commutative association schemes with exactly one pair of nonsymmetric relations, and introduced a set of feasibility and realizability conditions. From each nonsymmetric association scheme with three classes, a symmetric association scheme with two classes can be obtained by merging the nonsymmetric relations, which is called the symmetrization of the original association scheme. Two-class skew-symmetric association schemes are regular tournaments, whose symmetrization is trivial. There are some papers on the feasibility conditions for the existence of such association schemes, cf. [3, 17, 33]. In [22], the author did a systematic investigation of such association schemes of order no more than 100. There are several such association schemes of order 36, see [10, 16, 20, 22]. There is an infinite family of such association schemes of order $4s^4$, where s is a power of 2, cf. [9, 25, 27]. In [23], the author found some more such association schemes of order 64. These are all the known

primitive three-class nonsymmetric association schemes so far. On the nonexistence side, in [17] the authors showed that there is no three-class nonsymmetric association scheme whose symmetrization is a Paley type strongly regular graph.

A skew-symmetric association scheme is an association scheme with no symmetric adjacency relations other than the diagonal one. A typical example is given by the cyclotomic scheme of index 4 in the finite field \mathbb{F}_q , where $q \equiv 5 \pmod{8}$. The study of four-class skew symmetric association schemes was initiated in [34]. In [3], Bannai and Song raised a question regarding the existence of four-class amorphous skew-symmetric association schemes, which was answered in the negative in [28]. In the same paper, Ma classified four-class skew-symmetric association schemes by their character tables, which fall into three types. In a subsequent paper [29], the authors determined their intersection matrices, and generated a list of feasible parameters with small orders. The aforementioned cyclotomic scheme of index 4 is the only known such association scheme which is primitive to our knowledge.

In the current paper, we are primarily concerned with primitive translation association schemes on prime power number of points. Let p be a prime. Symmetric two-class translation schemes of order p^2 are exactly the strongly regular graphs of Latin square type with \mathbb{Z}_p^* as multiplier group; see the survey [26] for details. Nonsymmetric two-class translation schemes correspond to skew Hadamard difference sets whose ambient groups must have order congruent to 3 modulo 4, so there are no such association schemes of order p^2 . We show that there are no three- or four-class primitive translation schemes of prime square order with at least one pair of nonsymmetric relations. On the other hand, we find new nonsymmetric four- and five-class association schemes from cyclotomy as fissions of certain symmetric three-class association schemes, which are primitive under certain conditions. Here, we say that an association scheme admits a fission scheme if a relation of the original association scheme is partitionable into at least two relations of a new association scheme. In particular, the obtained nonsymmetric four-class association schemes have exactly one pair of nonsymmetric relation, which give a lot of examples of association schemes studied in [8] by Chia and Kok. Moreover, we provide an affirmative answer to the following question raised by Song [34]:

Problem 3 *Are there any other two-class primitive association schemes that admit symmetrizable fission schemes besides the cyclotomic scheme of index 2 for $q \equiv 5 \pmod{8}$?*

2 Preliminaries

Let $(X, \{R_i\}_{i=0}^d)$ be a d -class association scheme, and A_i be the adjacency matrix of the relation R_i . Its Bose-Mesner algebra is defined as $\mathcal{A} = \langle A_0, A_1, \dots, A_d \rangle$. Throughout this paper, we will assume that $(X, \{R_i\}_{i=0}^d)$ is commutative, i.e., the algebra \mathcal{A} is commutative. Denote by $E_0 = (1/|X|)J, E_1, \dots, E_d$ the primitive idempotents of \mathcal{A} , where J is the $|X| \times |X|$ all one matrix. Both sets $\{A_0, A_1, \dots, A_d\}$ and $\{E_0, E_1, \dots, E_d\}$ are bases of the algebra \mathcal{A} , and we thus have

$$A_j = \sum_{i=0}^d p_j(i) E_i, \quad E_j = \frac{1}{|X|} \sum_{i=0}^d q_j(i) A_i,$$

for some constants $p_j(i)$ and $q_j(i)$. Let P and Q be the $(d+1) \times (d+1)$ matrix, whose (i, j) -th entry is $p_j(i)$ and $q_j(i)$, respectively. The matrices P and Q are called the *first eigenmatrix* (or the *character table*) and the *second eigenmatrix* of $(X, \{R_i\}_{i=0}^d)$, respectively. There exist numbers $p_{i,j}^k$ and $q_{i,j}^k$ such that

$$A_i A_j = \sum_{k=0}^d p_{i,j}^k A_k, \quad E_i \circ E_j = \sum_{k=0}^d q_{i,j}^k E_k,$$

where \circ stands for entrywise multiplication. The numbers $p_{i,j}^k$'s and $q_{i,j}^k$'s are called the *intersection numbers* and the *Krein parameters* of $(X, \{R_i\}_{i=0}^d)$, respectively. For each $0 \leq i \leq d$, the i -th intersection matrix B_i is defined as the $(d+1) \times (d+1)$ matrix whose (k, j) -th entry is $p_{i,j}^k$. Clearly, B_0 is the identity matrix.

Given two association schemes $\mathcal{X} = (X, \{R_i\}_{i=0}^d)$ and $\mathcal{X}' = (X, \{R'_j\}_{j=0}^e)$, if for each $0 \leq i \leq d$, $R_i \subseteq R'_j$ for some $0 \leq j \leq e$, then we say that \mathcal{X} is a *fusion scheme* of \mathcal{X}' , and \mathcal{X}' is a *fission scheme* of \mathcal{X} . We shall need the following well-known criterion due to Bannai [1] and Muzychuk [31], called the *Bannai-Muzychuk criterion*: Let P be the first eigenmatrix of an association scheme $(X, \{R_i\}_{0 \leq i \leq d})$, and $\Lambda_0 := \{0\}, \Lambda_1, \dots, \Lambda_{d'}$ be a partition of $\{0, 1, \dots, d\}$. Then $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq d'})$ forms an association scheme if and only if there exists a partition $\{\Delta_i\}_{0 \leq i \leq d'}$ of $\{0, 1, \dots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Δ_j) -block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i, Δ_j) -block is the (i, j) -th entry of the first eigenmatrix of the fusion scheme.

Assume that $(X, \{R_i\}_{i=0}^d)$ is a translation scheme. There is an equivalence relation defined on the character group \widehat{X} of X as follows: $\chi \sim \chi'$ if and only if $\chi(R_i) = \chi'(R_i)$ for each $0 \leq i \leq d$. Here $\chi(R) = \sum_{g \in R} \chi(g)$, for any $\chi \in \widehat{X}$, and $R \subseteq X$. Denote by D_0, D_1, \dots, D_d the equivalence classes, with D_0 consisting of only the principal character χ_0 . Then $(\widehat{X}, \{D_i\}_{i=0}^d)$ forms a translation scheme, called the *dual* of $(X, \{R_i\}_{i=0}^d)$. If $\{D_i\}_{i=0}^d$ is mapped to $\{R_i\}_{i=0}^d$ under an isomorphism between X and \widehat{X} , then the association scheme is called *self-dual*. In the case $X = (\mathbb{F}_{p^f}, +)$, we take the map $\tau : a \rightarrow \psi_a$ as the group isomorphism from X to \widehat{X} , where $\psi_a(x) = e^{\frac{2\pi i}{p} \text{Tr}(ax)}$, and Tr is the absolute trace. The first eigenmatrix of the dual association scheme is equal to the second eigenmatrix of the original association scheme. Please refer to [2] and [6] for more details.

An association scheme $(X, \{R_i\}_{i=0}^d)$ is called *primitive* if each of the undirected graphs defined by R_i , $1 \leq i \leq d$, is connected, and *imprimitive* otherwise. A nonsymmetric association scheme is primitive if and only if its symmetrization is primitive. If $(X, \{R_i\}_{i=0}^d)$ is a symmetric translation scheme, then it is well-known that $(X, \{R_i\}_{i=0}^d)$ is primitive if and only if each nontrivial relation R_i generates the whole group X , i.e., not contained in any proper subgroup of X ; see [2]. It is equivalent to the fact that for

each nontrivial relation R_i , $\chi(R_i) \neq |R_i|$ for all nonprincipal characters χ of X ; see [7].

A classical example of translation schemes is the cyclotomic scheme which we describe now. Let p be a prime and $q = p^f$ ($f \geq 1$) be a prime power, $N|q - 1$, and γ be a primitive root of the finite field \mathbb{F}_q . Define the multiplicative subgroup $C_0^{(N,q)} = \langle \gamma^N \rangle$. Its cosets $C_i^{(N,q)} = \gamma^i C_0^{(N,q)}$, $0 \leq i \leq N - 1$, are called the *cyclotomic classes* of order N of \mathbb{F}_q . Together with $\{0\}$, they form an N -class association scheme, which is called the *cyclotomic scheme* of index N . If $D = \bigcup_{i \in I} C_i^{(N,q)}$ for some subset $I \subseteq \mathbb{Z}_N$, then we say that D is defined by the index set I .

Now we introduce some notation that we shall use in the later sections. We define the *Gauss periods* of index N over \mathbb{F}_q as follows:

$$\eta_i = \sum_{x \in C_i^{(N,q)}} \psi(x), \quad 0 \leq i \leq N - 1,$$

where ψ is the canonical additive character of \mathbb{F}_q defined by $\psi(x) = e^{\frac{2\pi i}{p} \text{Tr}_{q/p}(x)}$, $x \in \mathbb{F}_q$. For each multiplicative character χ of \mathbb{F}_q^* , the multiplicative group of \mathbb{F}_q , we define the *Gauss sum*

$$G_q(\chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x).$$

The following relation will be repeatedly used in this paper (cf. [24, p. 195]):

$$\psi(x) = \frac{1}{q - 1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} G_q(\chi)\chi^{-1}(x), \quad \forall x \in \mathbb{F}_q^*,$$

where $\widehat{\mathbb{F}_q^*}$ is the character group of \mathbb{F}_q^* . The Gauss period can be expressed as a linear combination of Gauss sums as follows:

$$\begin{aligned} \eta_i &= \psi(\gamma^i C_0^{(N,q)}) = \frac{1}{q - 1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} G_q(\chi)\chi^{-1}(\gamma^i) \sum_{x \in C_0^{(N,q)}} \chi^{-1}(x) \\ &= \frac{1}{N} \sum_{i=0}^{N-1} G_q(\varphi^{-i})\varphi(\gamma^i), \end{aligned}$$

where φ is a multiplicative character of order N of \mathbb{F}_q^* .

We record some basic properties of Gauss sums here [24]:

- (i) $G_q(\chi)\overline{G_q(\chi)} = q$ if χ is nontrivial;
- (ii) $G_q(\chi^p) = G_q(\chi)$, where p is the characteristic of \mathbb{F}_q ;
- (iii) $G_q(\chi^{-1}) = \chi(-1)\overline{G_q(\chi)}$;
- (iv) $G_q(\chi) = -1$ if χ is trivial.

In general, explicit evaluations of Gauss sums are very difficult. There are only a few cases where the Gauss sums have been evaluated, see [4] for known results on Gauss sums. In Sect. 4, we will use the explicit evaluations of Gauss sums of the quadratic residue case and index 2 case.

Theorem 4 ([24]) *Let η be the quadratic character of $\mathbb{F}_q = \mathbb{F}_{p^f}$, and $p^* = (-1)^{\frac{p-1}{2}} p$. It holds that*

$$G_q(\eta) = (-1)^{f-1} \left(\sqrt{p^*} \right)^f.$$

Theorem 5 ([36, Case D; Theorem 4.12]) *Let $N = 2p_1^m$, where $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod{4}$, and m is a positive integer. Assume that p is a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a multiplicative character of order N of \mathbb{F}_q . For $0 \leq t \leq m-1$, we have*

$$G_q(\chi^{p_1^t}) = \begin{cases} (-1)^{\frac{p-1}{2}(m-1)} p^{\frac{f-1}{2}-hp_1^t} \sqrt{p^*} \left(\frac{b+c\sqrt{-p_1}}{2} \right)^{2p_1^t} & \text{if } p_1 \equiv 3 \pmod{8}, \\ (-1)^{\frac{p-1}{2}m} p^{\frac{f-1}{2}} \sqrt{p^*} & \text{if } p_1 \equiv 7 \pmod{8}; \end{cases}$$

$$G_q(\chi^{2p_1^t}) = p^{\frac{f-p_1^t}{2}} \left(\frac{b+c\sqrt{-p_1}}{2} \right)^{p_1^t};$$

$$G_q(\chi^{p_1^m}) = (-1)^{\frac{p-1}{2} \frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*},$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and b and c are integers determined by $4p^h = b^2 + p_1c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

We shall also need the following *Davenport-Hasse lifting formula* on Gauss sums.

Theorem 6 ([24, Theorem 5.14]) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let χ' be the lifted character of χ to the extension field $\mathbb{F}_{q^s} = \mathbb{F}_{p^{fs}}$, i.e., $\chi'(\alpha) := \chi(\text{Norm}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha))$ for any $\alpha \in \mathbb{F}_{q^s}$. It holds that*

$$G_{q^s}(\chi') = (-1)^{s-1} (G_q(\chi))^s.$$

3 Nonsymmetric primitive association schemes of prime square order

In this section, we show that there is no nonsymmetric primitive translation scheme with at most four classes of prime square order. As we mentioned in the introduction, there are no such association schemes with two classes of prime square order. As a consequence of the Wielandt-Schur multiplier theorem, such a translation scheme can only survive in the additive group $G = (\mathbb{F}_{p^2}, +)$, cf. [6, Theorem 2.10.5]. Let $(G, \{R_i\}_{i=0}^d)$ be such a translation scheme with $d = 3, 4$.

Lemma 7 *The translation scheme $(G, \{R_i\}_{i=0}^d)$ has the set S of nonzero squares of \mathbb{Z}_p^* as a multiplier group.*

Proof We will use the Wielandt-Schur theorem to prove this lemma. Let R be any nontrivial relation. Write γ for a fixed primitive root of \mathbb{F}_{p^2} , and $\gamma_0 = \gamma^{p+1} \in \mathbb{F}_p^*$. If $R^{(\gamma_0^2)} \neq R$, then $R, R^{(\gamma_0)}, R^{(\gamma_0^2)}$, and $R^{(\gamma_0^3)}$ are four distinct nontrivial relations of the association scheme, and thus $d = 4$. It follows that the association scheme has two pairs of nonsymmetric relations, and $R^{(-1)} = R^{(\gamma_0^2)}$. Its symmetrization is a two-class association scheme $(G, \{\{0\}, R \cup R^{(\gamma_0^2)}, R^{(\gamma_0)} \cup R^{(\gamma_0^3)}\})$, so $R \cup R^{(\gamma_0^2)}$ is a partial difference set in G which has \mathbb{Z}_p^* as a multiplier group, cf. [26]. This contradicts the fact that $R \cup R^{(\gamma_0^2)} \neq R^{(\gamma_0)} \cup R^{(\gamma_0^3)}$. □

Lemma 8 *A translation scheme $(G, \{R_i\}_{i=0}^d)$ is symmetric if and only if its first eigenmatrix has only real entries. Moreover, the dual of a symmetric translation scheme is also symmetric.*

Proof The first part follows from the simple fact that the eigenvalues of the transpose of an adjacency matrix A_i are the complex conjugates of those of A_i . The dual translation scheme has its first eigenmatrix equal to $Q = |G| \cdot P^{-1}$, which is real if P is. □

Corollary 9 *A translation scheme $(G, \{R_i\}_{i=0}^d)$ has the same number of nonsymmetric relations as its dual.*

Proof Let $(G, \{S_i\}_{i=0}^{d'})$ be the symmetrization of the translation scheme $(G, \{R_i\}_{i=0}^d)$. Then its dual translation scheme is symmetric by Lemma 8 and is a subscheme of the dual of $(G, \{R_i\}_{i=0}^d)$. Therefore, the symmetrization of the dual of $(G, \{R_i\}_{i=0}^d)$ has at least d' relations. Arguing in the opposite direction, we see that the symmetrization of the translation scheme $(G, \{R_i\}_{i=0}^d)$ and the symmetrization of its dual have the same number of relations. The claim immediately follows. □

Remark 10 As pointed out by the editor, Corollary 9 also follows from a general fact on commutative association schemes. For an arbitrary commutative association scheme, there are two permutations induced by the transpose map, on the set of adjacency matrices and on the set of primitive idempotents. These two involutions always have the same number of fixed points (and hence the same number of transposed pairs), because their permutation matrices are conjugate by the first eigenmatrix and thus have the same trace. Since the number of nonsymmetric relations in the dual of a translation scheme is the same as the number of nonsymmetric idempotents in the original scheme, the claim follows.

Throughout this section, we use the standard notation on group rings as in [32]. To make distinction, we use $[i]$ for the group ring element in $\mathbb{Z}[\mathbb{Z}_N]$ corresponding to $i \in \mathbb{Z}_N$.

One consequence of the above lemma is that -1 is a nonsquare in \mathbb{Z}_p , and so $p \equiv 3 \pmod{4}$. It is clear that $S = C_0^{(N, p^2)}$ with $N = 2(p + 1)$, the multiplicative subgroup of index $N = 2(p + 1)$ in \mathbb{F}_{p^2} . Let $C_i := \gamma^i S, 0 \leq i \leq N - 1$ be the cyclotomic classes of index N . If a set $D = \bigcup_{i \in I} C_i$, then we say that D is defined by the index set $I \subset \mathbb{Z}_N$. According to Lemma 7, we assume that the nontrivial relations in the association scheme $(G, \{R_i\}_{i=0}^d)$ are defined by the index sets I_1, \dots, I_d , and the nontrivial relations in the dual association scheme are defined by the index sets

J_1, \dots, J_d . Since $-1 \in C_{p+1}$, we have $J_i = \{i + p + 1 \bmod N \mid i \in J_i\}$, and $J_i([0] - [p + 1]) = 0$ in $\mathbb{Z}[\mathbb{Z}_N]$ if J_i defines a symmetric relation. The same conditions also hold for the I_i 's.

Let $L = \{x \in \mathbb{F}_{p^2}^* \mid \text{Tr}(x) = 1\}$ which has size p , where $\text{Tr} := \text{Tr}_{p^2/p}$. We observe that $T_s = \{i \bmod N \mid \gamma^i \in L\} \subset \mathbb{Z}_N$ is a relative difference set in \mathbb{Z}_N with respect to the order 2 subgroup $\langle N_0 \rangle$ (cf. [32]):

$$T_s T_s^{(-1)} = p + \frac{p-1}{2}(\mathbb{Z}_N - \langle N_0 \rangle).$$

Let ψ be the canonical additive character of \mathbb{F}_{p^2} such that $\psi(x) = \xi_p^{\text{Tr}(x)}$, where ξ_p is a primitive p -th root of unity. By direct computations, we have

$$\psi(C_i) = \sum_{j=0}^{M-1} \xi_p^{\text{Tr}(\gamma^{i+Nj})} = \sum_{j=0}^{M-1} \xi_p^{\gamma^{Nj} \text{Tr}(\gamma^i)} = \psi(\text{Tr}(\gamma^i)S).$$

We have a partition of \mathbb{Z}_N into three parts by $T_0 = \{\frac{p+1}{2}, \frac{3(p+1)}{2}\}$, T_s and $T_n := \{i + (q + 1) \bmod N \mid i \in T_s\}$. If $i \in T_0$, then $\text{Tr}(\gamma^i) = 0$, and $\psi(C_i) = |C_0|$. If $i \in T_s$, then $\text{Tr}(\gamma^i)$ is a nonzero square, and $\psi(C_i) = \frac{-1 + \sqrt{p}}{2}$ with a proper choice of ξ_p . If $i \in T_n$, then $\text{Tr}(\gamma^i)$ is a nonsquare, and $\psi(C_i) = \frac{-1 - \sqrt{p}}{2}$. Assume that the set D is defined by the index set $I \subset \mathbb{Z}_N$. Then we have

$$\begin{aligned} \psi(\gamma^a D) &= \sum_{i \in I} \psi(C_{i+a}) = M \cdot |I + a \cap T_0| + \frac{-1 + \sqrt{p}}{2} |I + a \cap T_s| \\ &\quad + \frac{-1 - \sqrt{p}}{2} |I + a \cap T_n| \\ &= \left[\left(\frac{p-1}{2} T_0 - \frac{1}{2} T_s - \frac{1}{2} T_n + \frac{\sqrt{p}}{2} (T_s - T_n) \right) I^{(-1)} \right]_a \\ &= \frac{\sqrt{p}}{2} \left[(\sqrt{p} \cdot T_0 + T_s - T_n) I^{(-1)} \right]_a - \frac{|I|}{2}. \end{aligned}$$

In the case where D is a relation in the association scheme $(G, \{R_i\}_{i=0}^d)$, the group ring element $(\sqrt{q} \cdot T_0 + T_s - T_n) I^{(-1)} = \sum_{i=1}^d c_i J_i$ for some algebraic integers c_i , $1 \leq i \leq d$. Multiplying both sides by $[0] - [p + 1]$, we have $T_s I^{(-1)}([0] - [p + 1]) = \sum_i c_i J_i([0] - [p + 1])$, where the summation is over such i that J_i defines a nonsymmetric relation.

Now assume that the association scheme $(G, \{R_i\}_{i=0}^d)$ has exactly one pair of nonsymmetric relations, defined by I_1 and I_2 , respectively. By Corollary 9, the dual translation scheme also has exactly one pair of nonsymmetric relations. The above argument yields that $T_s I_1^{(-1)}([0] - [p + 1]) = cJ([0] - [p + 1])$ where the J defines a nonsymmetric relation in the dual association scheme. Applying the same argument to the dual association scheme, we get $T_s J^{(-1)}([0] - [p + 1]) = dI_1([0] - [p + 1])$

for some $d \in \mathbb{Z}$. Multiplying both sides by $T_s^{(-1)}$ and taking involution, we get $T_s I_1^{(-1)}([0] - [p + 1]) = \frac{p}{d} J([0] - [p + 1])$. Therefore, $p = cd$. Without loss of generality, we assume that $c = \pm p$. Now $|T_s| = p$, so $T_s I_1^{(-1)}$ has all coefficients not exceeding p , and the coefficients $\pm p$ occur in $T_s I_1^{(-1)}([0] - [p + 1])$ only if $|I_1| = p$ in which case our association scheme is clearly imprimitive. Therefore, this case cannot occur.

Now assume that $d = 4$ and $(G, \{R_i\}_{i=0}^4)$ has two pair of nonsymmetric relations, defined by $I, I + (p + 1), J, J + (p + 1) \in \mathbb{Z}_N$, respectively. By Corollary 9, the dual translation scheme also has two pairs of nonsymmetric relations. Also assume that the nontrivial relations of the dual association scheme are defined by $I', I' + (p + 1), J', J' + (p + 1) \in \mathbb{Z}_N$. Now, we apply the same argument as above and get

$$\begin{aligned} T_s I^{(-1)}([0] - [p + 1]) &= aI'([0] - [p + 1]) + bJ'([0] - [p + 1]), \\ T_s J^{(-1)}([0] - [p + 1]) &= cI'([0] - [p + 1]) + dJ'([0] - [p + 1]). \end{aligned}$$

Multiplying both sides with $T_s^{(-1)}$ and taking involution, we have

$$\begin{aligned} pI([0] - [p + 1]) &= aT_s I'^{(-1)}([0] - [p + 1]) + bT_s J'^{(-1)}([0] - [p + 1]), \\ pJ([0] - [p + 1]) &= cT_s I'^{(-1)}([0] - [p + 1]) + dT_s J'^{(-1)}([0] - [p + 1]). \end{aligned}$$

The determinant $ad - bc \neq 0$, since the left hand side does not differ by a constant multiple. We may solve that

$$\begin{aligned} T_s I'^{(-1)}([0] - [p + 1]) &= \frac{p}{ad - bc} (dI - bJ)([0] - [p + 1]), \\ T_s J'^{(-1)}([0] - [p + 1]) &= \frac{p}{ad - bc} (-cI + aJ)([0] - [p + 1]). \end{aligned}$$

Therefore, $ad - bc$ divides $p \cdot \gcd(b, d, a, c)$. Since $\gcd(b, d, a, c)^2 | ad - bc$, we have $\gcd(b, d, a, c) | p$. It follows that $\gcd(b, d, a, c) = 1$ or p . It is easy to see that each of these four numbers are less than p , so we have $\gcd(b, d, a, c) = 1$, and $ad - bc \in \{\pm 1, \pm p\}$. By replacing the association scheme with its dual if necessary, we may assume that $ad - bc \in \{\pm 1\}$.

Now we solve that

$$\begin{aligned} I'^{(-1)}([0] - [p + 1]) &= \frac{1}{ad - bc} T_s^{(-1)}(dI - bJ)([0] - [p + 1]), \\ J'^{(-1)}([0] - [p + 1]) &= \frac{1}{ad - bc} T_s^{(-1)}(-cI + aJ)([0] - [p + 1]). \end{aligned}$$

Therefore, multiplying each equation by its involution, respectively, we get

$$\begin{aligned} I' I'^{(-1)}([0] - [p + 1]) &= p(dI - bJ)(dI - bJ)^{(-1)}([0] - [p + 1]), \\ J' J'^{(-1)}([0] - [p + 1]) &= p(-cI + aJ)(-cI + aJ)^{(-1)}([0] - [p + 1]). \end{aligned}$$

Assume without loss of generality that $1 < |I'| \leq \frac{p+1}{2}$ ($|I'| = 1$ would imply imprimitivity). Observe that $I'I'^{(-1)}$ has coefficients between 0 and $|I'|$, so $I'I'^{(-1)}([0] - [p + 1])$ has coefficient between $-|I'|$ and $|I'|$. Therefore, together with the fact that it is divisible by p , we have $I'I'^{(-1)}([0] - [p + 1]) = 0$. It follows that the coefficient of $p + 1$ in $I'I'^{(-1)}$ is the same as that of zero, namely $|I'|$. This means $I' = I' + (p + 1)$, which is a contradiction.

This leads us to deduce the following theorem.

Theorem 11 *There is no nonsymmetric primitive translation scheme of prime square order with at most four classes.*

4 Fission schemes of three-class association schemes based on index 2 Gauss sums

Throughout this section, we assume that we are in the same settings as in Theorem 5: p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3 \pmod{4}$; p is an odd prime such that $[\mathbb{Z}_{2p_1}^* : \langle p \rangle] = 2$ (that is, $f := \text{ord}_{2p_1}(p) = (p_1 - 1)/2$). Put $q = p^f$. In this case, the Gauss sums $G_q(\chi^j)$ were completely evaluated in [36] as described in Theorem 5, where χ is a multiplicative character of order $2p_1$ of \mathbb{F}_q . (We called this the *index 2 Gauss sum*.)

Consider the extension field \mathbb{F}_{q^s} for a positive integer s and put $G = (\mathbb{F}_{q^s}, +)$. Let γ be a primitive root of \mathbb{F}_{q^s} . Consider the automorphism group of G generated by multiplication by γ^{p_1} and the Frobenius automorphism which raises each element of \mathbb{F}_{q^s} to its p -th power. Its orbits on $(\mathbb{F}_{q^s}, +)$ consist of

$$R_0 = \{0\}, R_1 = \bigcup_{j \in \langle p \rangle \pmod{p_1}} C_j^{(p_1, q^s)}, R_2 = \bigcup_{j \in -\langle p \rangle \pmod{p_1}} C_j^{(p_1, q^s)}, R_3 = C_0^{(p_1, q^s)}.$$

This partition $(G, \{R_i\}_{i=0}^3)$ becomes a symmetric three-class association scheme. In particular, this is self-dual since J_i 's are also invariant under the multiplication of p modulo N by $\psi_a(C_0^{(N, q)}) = \psi_{ap}(C_0^{(N, q)})$ for any $a \in \mathbb{Z}_N$, where J_i are the index sets of the dual association scheme. This association scheme is primitive if and only if R_3 generates the whole group, namely $\mathbb{F}_p[\gamma^{p_1}] = \mathbb{F}_{q^s}$. This happens exactly when γ^{p_1} has a minimal polynomial of degree fs over \mathbb{F}_p , i.e., p has order fs modulo $\frac{q^s-1}{p_1}$.

We now consider a four-class fission scheme of this association scheme.

Theorem 12 *Take the conditions as above, and further assume that $p_1 \equiv 7 \pmod{8}$. Define*

$$S_0 = R_0, S_1 = R_1, S_2 = R_2, S_3 = C_0^{(2p_1, q^s)}, S_4 = C_{p_1}^{(2p_1, q^s)}.$$

Then $(G, \{S_i\}_{i=0}^4)$ becomes a four-class self-dual association scheme.

Proof In view of the Bannai-Muzychuk criterion, we need to compute the eigenvalues $\psi(\gamma^a S_i)$, $1 \leq i \leq 4$, and show that they are constant according to $\gamma^a \in S_j$, $1 \leq j \leq 4$.

Since we already know that $\psi(\gamma^a S_i)$, $i = 1, 2$, are constant according to $\gamma^a \in S_j$, $1 \leq j \leq 4$, we compute only the sum $\psi(\gamma^a S_3)$. (Note that $\psi(\gamma^a S_4) = \psi(\gamma^a R_3) - \psi(\gamma^a S_3)$.) By the expression of Gauss periods as linear combinations of Gauss sums as explained in the introduction, we have

$$\begin{aligned} \psi(\gamma^a S_3) &= \frac{1}{2p_1} \sum_{i=0}^{2p_1-1} G_{q^s}(\chi^i) \chi^{-i}(\gamma^a) \\ &= \frac{1}{2p_1} \sum_{0 \leq i \leq 2p_1-1: i \text{ odd}} G_{q^s}(\chi^i) \chi^{-i}(\gamma^a) \\ &\quad + \frac{1}{2p_1} \sum_{0 \leq i \leq 2p_1-1: i \text{ even}} G_{q^s}(\chi^i) \chi^{-i}(\gamma^a), \end{aligned} \tag{4.1}$$

where χ is a multiplicative character of order $2p_1$ of \mathbb{F}_{q^s} . On the other hand, we have

$$\psi(\gamma^a R_3) = \frac{1}{p_1} \sum_{i=0}^{p_1-1} G_{q^s}(\chi^{2i}) \chi^{-2i}(\gamma^a),$$

which implies that

$$(4.1) = \frac{1}{2p_1} \sum_{0 \leq i \leq 2p_1-1: i \text{ odd}} G_{q^s}(\chi^i) \chi^{-i}(\gamma^a) + \frac{1}{2} \psi(\gamma^a R_3).$$

By Theorem 5 and the Davenport-Hasse lifting formula,

$$G_{q^s}(\chi^i) = (-1)^{s-1} (-1)^{\frac{p-1}{2}s} p^{\frac{f-1}{2}s} \sqrt{p^*}^s$$

for all odd i , where we used the facts that $\chi^i(-1)\sqrt{p^*} = \sqrt{p^*}$ and $\frac{p-1}{2} \equiv \frac{p-1}{2} \frac{f-1}{2} \pmod{2}$. We now compute that

$$\begin{aligned} \sum_{0 \leq i \leq p_1-1: i \text{ odd}} G_{q^s}(\chi^i) \chi^{-i}(\gamma^a) &= (-1)^{s-1} (-1)^{\frac{p-1}{2}s} p^{\frac{f-1}{2}s} \sqrt{p^*}^s \chi^{-1}(\gamma^a) \sum_{i=0}^{p_1-1} \chi^{-2i}(\gamma^a) \\ &= (-1)^{s-1} (-1)^{\frac{p-1}{2}s} p^{\frac{f-1}{2}s} \sqrt{p^*}^s \cdot \begin{cases} (-1)^a & \text{if } a \equiv 0 \pmod{p_1}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

This implies that $\psi(\gamma^a S_3)$ is constant according to $\gamma^a \in S_i$, $1 \leq i \leq 4$, since we already know that $\psi(\gamma^a R_3)$ is constant according to $\gamma^a \in R_i$, $1 \leq i \leq 3$. This completes the proof. \square

Remark 13 (1) If s is odd and $p \equiv 3 \pmod{4}$, then the resulting association schemes of Theorem 12 are nonsymmetric four-class association scheme with exactly one pair of nonsymmetric relations. This result gives a lot of examples of nonsymmetric association schemes studied in [8] by Chia and Kok.

(2) We investigate the primitivity of the resulting nonsymmetric association schemes in the case $s = 1$ in detail: As described in Sect. 2, the nonsymmetric association scheme $(G, \{S_i\}_{i=0}^4)$ is primitive if and only if $\psi(\gamma^a(S_i \cup -S_i)) \neq |S_i \cup -S_i|$ for $1 \leq i \leq 4$. Noting that $S_3 \cup -S_3 = R_3$, it is enough to see that $\psi(\gamma^a R_3) \neq |R_3|$. (Note that if the graph corresponding to R_3 is connected, then so are the others.) In [13], the sum $\psi(\gamma^a R_3)$ was computed as follows:

$$\psi(\gamma^a R_3) = \frac{1}{p_1} \left(p^{(f-h)/2} \left(\frac{-b \pm p_1 c}{2} \right) - 1 \right) \text{ or } \frac{1}{p_1} \left(p^{(f-h)/2} \left(\frac{p_1 - 1}{2} \right) - 1 \right).$$

Therefore, $(G, \{S_i\}_{i=0}^4)$ is primitive if and only if $-b \pm p_1 c \neq 2p^{\frac{f+h}{2}}$ and $p_1 - 1 \neq 2p^{\frac{f+h}{2}}$. Noting that $b^2 + p_1 c^2 = 4p^h$, for each $x \in \{-b \pm p_1 c, p_1 - 1\}$ we have $x \leq b^2 + c^2 p_1 = 4p^h < 2p^{(f+h)/2}$ if $p_1 > 2h + 1$ and $c \neq 0$. Thus, the nonsymmetric association scheme $(G, \{S_i\}_{i=0}^4)$ is primitive if $p_1 > 2h + 1$ and $c \neq 0$.

Next we describe an infinite family of nonsymmetric five-class association schemes with exactly two pairs of nonsymmetric relations in the case $p_1 \equiv 3 \pmod{8}$. Again, we assume that we are in the same settings as in Theorem 5 with $p_1 \equiv 3 \pmod{8}$. Let $f = (p_1 - 1)/2$, $q = p^f$, and $G = (\mathbb{F}_q, +)$. Define

$$R_0 = \{0\}, R_1 = \bigcup_{j \in (p) \pmod{p_1}} C_j^{(p_1, q)}, R_2 = \bigcup_{j \in -(p) \pmod{p_1}} C_j^{(p_1, q)}, R_3 = C_0^{(p_1, q)}.$$

Then, $(G, \{R_i\}_{i=0}^3)$ is a three-class self-dual association scheme. This association scheme is primitive if and only if R_3 generates the whole group, namely $\mathbb{F}_p[\gamma^{p_1}] = \mathbb{F}_q$. This happens exactly when γ^{p_1} has a minimal polynomial of degree f over \mathbb{F}_p , i.e., p has order f modulo $\frac{q-1}{p_1}$.

Suppose it holds that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Let $\xi_{q-1} = e^{\frac{2\pi i}{q-1}}$ and \mathfrak{P} be a prime ideal in $\mathbb{Z}[\xi_{q-1}]$ lying over p . Then, $\mathbb{Z}[\xi_{q-1}]/\mathfrak{P}$ is the finite field of order q and

$$\mathbb{Z}[\xi_{q-1}]/\mathfrak{P} = \{\bar{\xi}_{q-1}^i \mid 0 \leq i \leq q - 2\} \cup \{\bar{0}\},$$

where $\bar{\xi}_{q-1} = \xi_{q-1} + \mathfrak{P}$. Hence, $\gamma := \bar{\xi}_{q-1}$ is a primitive root of $\mathbb{F}_q = \mathbb{Z}[\xi_{q-1}]/\mathfrak{P}$.

Let $\omega_{\mathfrak{P}}$ be the Teichmüller character of \mathbb{F}_q^* such that $\omega_{\mathfrak{P}}(\gamma) = \xi_{q-1}$. Put $\chi := \omega_{\mathfrak{P}}^{\frac{q-1}{2p_1}}$. Then χ is a multiplicative character of order $2p_1$ of \mathbb{F}_q^* .

By Theorem 5, we have

$$G_q(\chi) = p^{\frac{f-1}{2}-h} \sqrt{p^*} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^2, \tag{4.2}$$

where $b, c \not\equiv 0 \pmod{p}$, $b^2 + c^2 p_1 = 4p^h$, and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$. Since $1 + p_1 = 4p^h$, we have $b, c \in \{-1, 1\}$, where the sign of c depends on the choice of \mathfrak{P} . It was shown in [12] that $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$. On the other hand, $1 + p_1 = 4p^h$ implies that $(1 + \sqrt{-p_1})(1 - \sqrt{-p_1}) \in \mathfrak{P}$, so either $1 + \sqrt{-p_1} \in \mathfrak{P}$ or $1 - \sqrt{-p_1} \in \mathfrak{P}$. We choose a prime ideal \mathfrak{P} such that $1 + \sqrt{-p_1} \in \mathfrak{P}$. Then $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$ yields that $bc = 1$. From now on, we fix this choice of \mathfrak{P} and the corresponding character χ .

Theorem 14 *Take the conditions as above. Define*

$$S_0 = R_0, S_1 = R_1, S_2 = \bigcup_{j \in -\langle p \rangle \pmod{2p_1}} C_j^{(2p_1, q)},$$

$$S_3 = \bigcup_{j \in -\langle p \rangle \pmod{2p_1}} C_{j+p_1}^{(2p_1, q)}, S_4 = C_0^{(2p_1, q)}, S_5 = C_{p_1}^{(2p_1, q)}.$$

Then $(G, \{S_i\}_{i=0}^5)$ becomes a five-class self-dual association scheme.

Proof Note that $S_2 \cup S_3 = R_2$ and $S_4 \cup S_5 = R_3$. By the Bannai-Muzychuk criterion, it is enough to show that the sums $\psi(\gamma^a S_2)$ and $\psi(\gamma^a S_4)$ are constant according to $\gamma^a \in S_i, 1 \leq i \leq 5$.

First, we compute the sum $\psi(\gamma^a S_4)$. By the same argument as that in the proof of Theorem 12, we have

$$\begin{aligned} \psi(\gamma^a S_4) &= \frac{1}{2p_1} \sum_{\ell=0}^{2p_1-1} G_q(\chi^\ell) \chi^{-\ell}(\gamma^a) \\ &= \frac{1}{2p_1} \sum_{0 \leq \ell \leq 2p_1-1: \ell \text{ odd}} G_q(\chi^\ell) \chi^{-\ell}(\gamma^a) + \frac{1}{2} \psi(\gamma^a R_3), \end{aligned}$$

where χ is as defined above. Since $\psi(\gamma^a R_3)$ is constant according to $\gamma^a \in R_i, 1 \leq i \leq 3$, we only need to consider the sum

$$\sum_{0 \leq \ell \leq 2p_1-1: \ell \text{ odd}} G_q(\chi^\ell) \chi^{-\ell}(\gamma^a). \tag{4.3}$$

By Theorem 5, we have

$$G_q(\chi^\ell) = A \left(\frac{b + c\sqrt{-p_1}}{2} \right)^2$$

for all $\ell \in \langle p \rangle$, where b, c are the same as in the evaluation (4.2) of $G_q(\chi)$ and $A = p^{\frac{f-1}{2}-h} \sqrt{p^*}$. By the choice of \mathfrak{P} , it is expanded as

$$G_q(\chi^\ell) = A \left(\frac{1 - p_1 + 2\sqrt{-p_1}}{4} \right).$$

Since $G_q(\chi^{p_1}) = p^{\frac{f-1}{2}} \sqrt{p^*}$ by Theorem 5 and $\chi^\ell(-1)\sqrt{p^*} = \sqrt{p^*}$ for any odd ℓ , the sum in Eqn. (4.3) is reformulated as

$$A \left(\left(\frac{1 - p_1 + 2\sqrt{-p_1}}{4} \right) \sum_{\ell \in \langle p \rangle \pmod{2p_1}} \chi^{-\ell}(\gamma^a) + \left(\frac{1 - p_1 - 2\sqrt{-p_1}}{4} \right) \sum_{\ell \in -\langle p \rangle \pmod{2p_1}} \chi^{-\ell}(\gamma^a) + p^h(-1)^a \right). \tag{4.4}$$

Let η be the quadratic character of \mathbb{F}_{p_1} and ψ_{p_1} be the canonical additive character of \mathbb{F}_{p_1} . Noting that 2 is a nonsquare in \mathbb{F}_{p_1} , it holds that

$$\begin{aligned} \sum_{\ell \in \langle p \rangle \pmod{2p_1}} \chi^{-\ell}(\gamma^a) &= \sum_{\ell \in \langle p \rangle \pmod{2p_1}} \chi^{-p_1 \ell}(\gamma^a) \chi^{2\frac{p_1-1}{2} \ell}(\gamma^a) \\ &= (-1)^a \frac{1}{2} \sum_{\ell \in \mathbb{F}_{p_1}^*} (1 + \eta(\ell)) \psi_{p_1}(-2^{-1} a \ell) \\ &= (-1)^a \frac{-1 + \eta(-2^{-1} a) G_{p_1}(\eta)}{2} = (-1)^a \frac{-1 + \eta(a) \sqrt{-p_1}}{2}. \end{aligned}$$

Hence, by using $1 + p_1 = 4p^h$, we have

$$(4.4) = A(-1)^a \cdot \begin{cases} 0 & \text{if } a \in \langle p \rangle \pmod{p_1}, \\ \frac{1}{4}(-1 + 3p_1) + p^h & \text{if } a \in -\langle p \rangle \pmod{p_1}, \\ -\frac{(p_1-1)^2}{4} + p^h & \text{if } a \equiv 0 \pmod{p_1}. \end{cases}$$

This shows that $\psi(\gamma^a S_4)$ is constant according to $\gamma^a \in S_i, 1 \leq i \leq 5$.

Next, we consider the sum $\psi(\gamma^a S_2)$. In the same way, we get

$$\begin{aligned} \psi(\gamma^a S_2) &= \frac{1}{2p_1} \sum_{\ell=0}^{2p_1-1} \sum_{i \in -\langle p \rangle \pmod{2p_1}} G_q(\chi^\ell) \chi^{-\ell}(\gamma^{a+i}) \\ &= \frac{1}{2p_1} \sum_{0 \leq \ell \leq 2p_1-1: \ell \text{ odd}} \sum_{i \in -\langle p \rangle \pmod{2p_1}} G_q(\chi^\ell) \chi^{-\ell}(\gamma^{a+i}) + \frac{1}{2} \psi(\gamma^a R_2). \end{aligned}$$

If $a \not\equiv 0 \pmod{p_1}$, then

$$\begin{aligned} &\sum_{0 \leq \ell \leq 2p_1-1: \ell \text{ odd}} \sum_{i \in -\langle p \rangle \pmod{2p_1}} G_q(\chi^\ell) \chi^{-\ell}(\gamma^{a+i}) \\ &= A \left(\left(\frac{1 - p_1 + 2\sqrt{-p_1}}{4} \right) \sum_{i \in -\langle p \rangle \pmod{2p_1}} \sum_{\ell \in \langle p \rangle \pmod{2p_1}} \chi^{-\ell}(\gamma^{a+i}) \right) \end{aligned}$$

$$\begin{aligned}
 & + \left(\frac{1-p_1-2\sqrt{-p_1}}{4} \right) \sum_{i \in -\langle p \rangle \pmod{2p_1}} \sum_{\ell \in -\langle p \rangle \pmod{2p_1}} \chi^{-\ell} (\gamma^{a+i}) - \frac{p_1-1}{2} p^h (-1)^a \Big) \\
 = & A(-1)^a \left(\left(\frac{1-p_1+2\sqrt{-p_1}}{4} \right) \left(\frac{-1+\eta(a)\sqrt{-p_1}}{2} \right) \sum_{i \in \langle p \rangle \pmod{2p_1}} \chi^i (\gamma) \right. \\
 & \left. + \left(\frac{1-p_1-2\sqrt{-p_1}}{4} \right) \left(\frac{-1-\eta(a)\sqrt{-p_1}}{2} \right) \sum_{i \in -\langle p \rangle \pmod{2p_1}} \chi^i (\gamma) - \frac{p_1-1}{2} p^h \right) \\
 = & A(-1)^a \left(- \left(\frac{1-p_1+2\sqrt{-p_1}}{4} \right) \left(\frac{-1+\eta(a)\sqrt{-p_1}}{2} \right) \left(\frac{-1-\sqrt{-p_1}}{2} \right) \right. \\
 & \left. - \left(- \frac{1-p_1-2\sqrt{-p_1}}{4} \right) \left(\frac{-1-\eta(a)\sqrt{-p_1}}{2} \right) \left(\frac{-1+\sqrt{-p_1}}{2} \right) - \frac{p_1-1}{2} p^h \right) \\
 = & A(-1)^a \cdot \begin{cases} 0 & \text{if } a \in \langle p \rangle \pmod{p_1}, \\ -\frac{p_1^2-6p_1+1}{8} - \frac{p_1-1}{2} p^h & \text{if } a \in -\langle p \rangle \pmod{p_1}. \end{cases}
 \end{aligned}$$

This shows that $\psi(\gamma^a S_2)$ is constant according to $\gamma^a \in S_i, 1 \leq i \leq 5$. Thus, we have the assertion of the theorem. □

Remark 15 (i) We find that $(G, \{S_i\}_{i=0}^5)$ becomes a five-class association scheme in the following cases:

$$(p, p_1, h) = (3, 11, 1), (5, 19, 1), (17, 67, 1), (3, 107, 3), (41, 163, 1), (5, 499, 3).$$

We checked by using Magma [5] for all $p_1 < 5000$. (Note that p and h are determined by $1+p_1 = 4p^h$.) The association schemes for $(p, p_1) = (3, 11), (3, 107)$ are nonsymmetric with exactly two pairs of nonsymmetric relations, where $-S_3 = S_2$ and $-S_5 = S_4$, and the others are symmetric.

(ii) We obtain infinite families of five-class association schemes by using the ‘‘recursive’’ technique applied in [13, 14, 30]: Let p and p_1 be primes such that $[\mathbb{Z}_{2p_1}^* : \langle p \rangle] = 2$ for all $m \geq 1$, and let $q = p^{\frac{p_1-1}{2}} p_1^{m-1}$. Define

$$\begin{aligned}
 R_0 = \{0\}, \quad R_1 &= \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in \langle p \rangle \pmod{p_1}} C_{2i+p_1^{m-1}j}^{(p_1^m, q)}, \\
 R_2 &= \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in -\langle p \rangle \pmod{p_1}} C_{2i+p_1^{m-1}j}^{(p_1^m, q)}, \quad R_3 = \bigcup_{i=0}^{p_1^{m-1}-1} C_{2i}^{(p_1^m, q)},
 \end{aligned}$$

and

$$S_0 = R_0, \quad S_1 = R_1, \quad S_2 = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in -\langle p \rangle \pmod{2p_1}} C_{2i+p_1^{m-1}j}^{(2p_1^m, q)},$$

$$S_3 = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in -\langle p \rangle \pmod{2p_1}} C_{2i+p_1^{m-1}j+p_1^m}^{(2p_1^m, q)},$$

$$S_4 = \bigcup_{i=0}^{p_1^{m-1}-1} C_{2i}^{(2p_1^m, q)}, \quad S_5 = \bigcup_{i=0}^{p_1^{m-1}-1} C_{2i+p_1^m}^{(2p_1^m, q)}.$$

Write $G' = (\mathbb{F}_q, +)$. Then, the partition $(G', \{R_i\}_{i=0}^3)$ becomes a three-class association scheme and the partition $(G', \{S_i\}_{i=0}^5)$ forms a five-class fission scheme of $(G', \{R_i\}_{i=0}^3)$. The proof is done by the quite similar argument as [14, Theorem 3.6], that is, reducing the proof to the case $m = 1$, i.e., the proof of Theorem 14. So we omit the proof.

Since the pairs

$$(p, p_1) = (5, 19), (17, 67), (3, 107), (41, 163), (5, 499)$$

as listed in Remark 15 (i) satisfy that $[\mathbb{Z}_{2p_1^m}^* : \langle p \rangle] = 2$ for all $m \geq 1$, we obtain five infinite families of five-class association schemes. Since $[\mathbb{Z}_{2p_1^m}^* : \langle p \rangle] \neq 2$ for $m \geq 2$ in the case $(p, p_1) = (3, 11)$, it cannot be generalized in this way.

- (iii) We show that the five infinite families of association schemes of Remark 15 (ii) are primitive similar to the argument in Remark 13: if $(p, p_1) = (3, 107)$, i.e., the association schemes are nonsymmetric, by using the computation of $\psi(\gamma^a R_3)$ given in [13] we have

$$\begin{aligned} \psi(\gamma^a(S_4 \cup -S_5)) &= \psi(\gamma^a R_3) \\ &= \frac{1}{p_1} \left(p^{(f-h)/2} \left(\frac{-b \pm p_1 c}{2} \right) - 1 \right) \text{ or} \\ &\quad \frac{1}{p_1} \left(p^{(f-h)/2} \left(\frac{p_1 - 1}{2} \right) - 1 \right) \\ &= \frac{3^{\frac{f-1}{2}} \cdot 53 - 1}{107} \text{ or } \frac{-3^{\frac{f-1}{2}} \cdot 54 - 1}{107} \neq \frac{3^f - 1}{107}. \end{aligned}$$

Next consider the case $(p, p_1) \neq (3, 107)$, i.e., the association schemes are symmetric. By [30, Theorem 3.2], if $p \equiv 1 \pmod{4}$, it holds that for any $I \subseteq \mathbb{Z}_{2p_1}$

$$\begin{aligned} \sum_{i=0}^{p_1^m-1} \sum_{j \in I} \psi \left(\gamma^a C_{2i+p_1^m j}^{(2p_1^{m+1}, p^{\frac{p_1-1}{2} p_1^m})} \right) &= p^{\frac{(p_1-1)^2 p_1^{m-1}}{4}} \\ \sum_{i=0}^{p_1^{m-1}-1} \sum_{j \in I} \psi' \left(\omega^a C_{2i+p_1^{m-1} j}^{(2p_1^m, p^{\frac{p_1-1}{2} p_1^{m-1}})} \right) &+ \frac{p^{\frac{(p_1-1)^2 p_1^{m-1}}{4}} - 1}{p_1}, \quad (4.5) \end{aligned}$$

where ψ and ψ' are canonical additive characters of $\mathbb{F}_p^{\frac{p_1-1}{2}p_1^m}$ and $\mathbb{F}_p^{\frac{p_1-1}{2}p_1^{m-1}}$, and γ and ω are primitive roots of $\mathbb{F}_p^{\frac{p_1-1}{2}p_1^m}$ and $\mathbb{F}_p^{\frac{p_1-1}{2}p_1^{m-1}}$, respectively. Then, by the computation of $\psi(\gamma^a S_4)$ for $m = 1$ in Theorem 14, we have that for general m

$$\begin{aligned} \psi(\gamma^a S_4) &= \frac{1}{2p_1} \left(p^{(f-h)/2} \left(\frac{-b - p_1c}{2} \right) - 1 \right), \\ &\quad \frac{1}{2p_1} \left(p^{(f-h)/2} \left(\frac{-b + p_1c}{2} \right) - 1 \right) \pm \frac{p^{\frac{f}{2}-h}}{2p_1} \left(p^h + \frac{3p_1 - 1}{4} \right), \\ &\quad \frac{1}{2p_1} \left(p^{(f-h)/2} \left(\frac{p_1 - 1}{2} \right) - 1 \right) \pm \frac{p^{\frac{f}{2}-h}}{2p_1} \left(p^h - \frac{(p_1 - 1)^2}{4} \right), \end{aligned}$$

which are not equal to $\frac{p^f-1}{2p_1}$ for any $(p, p_1) = (5, 19), (17, 67), (41, 163), (5, 499)$.

5 A nonsymmetric four-class fission scheme of a conference graph

First we recall the construction of two-class translation schemes in [12]. A more common way to describe two-class translation schemes is to use the language of partial difference sets, but we don't introduce this definition here and refer to [26] for details. Let p_1 be an odd prime. We assume the following specific index 2 case: $N_0 = 2p_1$, $p_1 > 3$ is a prime, and $p_1 \equiv 3 \pmod{4}$; p is an odd prime such that $[\mathbb{Z}_{N_0}^* : \langle p \rangle] = 2$ (that is, $f := \text{ord}_{N_0}(p) = \phi(N_0)/2$). Assume that $p_1 \equiv 7 \pmod{8}$. Let $C_i = C_i^{(N_0, q)}$ for $1 \leq i \leq N_0 - 1$.

Theorem 16 *Assume that we are in the index 2 case specified as above. Let $p_1 \equiv 7 \pmod{8}$, $f = (p_1 - 1)/2$, and $q = p^f$, and write $G = (\mathbb{F}_q, +)$. Let I_0 be any subset of \mathbb{Z}_{N_0} such that $\{i \pmod{p_1} \mid i \in I_0\} = \mathbb{Z}_{p_1}$, and let $D_0 = \bigcup_{i \in I_0} C_i^{(N_0, q)}$, $D_1 = \mathbb{F}_q^* \setminus D_0$. Then $(G, \{\{0\}, D_0, D_1\})$ is a two-class translation scheme if $p \equiv 1 \pmod{4}$.*

The Cayley graph of D_0 in Theorem 16 is a conference graph, namely, it is a strongly regular graph with parameters of the form $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$. By using Magma [5], we find that for $p = 37$, $q = p^3$, and $N = 2N_0 = 28$, the sets $R_i = \bigcup_{i \in I_i} C_i^{(N, q)}$ with the index sets

$$I_1 = \{0, 1, 4, 12, 16, 20, 24\} \subset \mathbb{Z}_{28}, \quad I_2 = I_1 + 7, \quad I_3 = I_1 + 14, \quad I_4 = I_1 + 21$$

define a four-class skew-symmetric association scheme whose symmetrization is covered by Theorem 16. The dual association scheme is defined by

$$J_1 = \{0, 4, 8, 12, 13, 16, 24\} \subset \mathbb{Z}_{28}, \quad J_2 = J_1 + 7, \quad J_3 = J_1 + 14, \quad J_4 = J_1 + 21.$$

We have $q = 37^3 = 107^2 + 4 \cdot 99^2 = 37^2 + 4 \cdot 111^2$. By Ma and Wang's results [29], a skew-symmetric fission scheme with four classes of a conference graph exists

only if $q \equiv 5 \pmod{8}$ and there exist integers g, h such that $q = g^2 + 4h^2$ with $g \equiv 1 \pmod{4}$, and the first eigenmatrix P is of the form

$$P = \begin{pmatrix} 1 & f & f & f & f \\ 1 & \rho & \tau & \bar{\rho} & \bar{\tau} \\ 1 & \tau & \bar{\rho} & \bar{\tau} & \rho \\ 1 & \bar{\rho} & \bar{\tau} & \rho & \tau \\ 1 & \bar{\tau} & \rho & \tau & \bar{\rho} \end{pmatrix}$$

where $f = \frac{q-1}{4}$, $\rho = \frac{1}{4}(-1 + \sqrt{q} + \sqrt{-2q + 2g\sqrt{q}})$, $\tau = \frac{1}{4}(-1 - \sqrt{q} + \sqrt{-2q - 2g\sqrt{q}})$. However, Ma and Wang did not give new constructions besides the cyclotomic schemes. It turns out that our example happens with $g = 37$. For the corresponding cyclotomic scheme of order 4 over \mathbb{F}_{37^3} , we have $g = -107$. This implies that the two association schemes have different first eigenmatrices, so the resulting association schemes are non-isomorphic.

The intersection matrices of our association scheme are given below:

$$B_1 = \begin{pmatrix} 0 & 0 & 0 & 12663 & 0 \\ 1 & 3170 & 3161 & 3170 & 3161 \\ 0 & 3115 & 3161 & 3161 & 3226 \\ 0 & 3152 & 3226 & 3170 & 3115 \\ 0 & 3226 & 3115 & 3161 & 3161 \end{pmatrix} \quad B_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 12663 \\ 0 & 3161 & 3226 & 3115 & 3161 \\ 1 & 3161 & 3170 & 3161 & 3170 \\ 0 & 3226 & 3115 & 3161 & 3161 \\ 0 & 3115 & 3152 & 3226 & 3170 \end{pmatrix}$$

$$B_3 = \begin{pmatrix} 0 & 12663 & 0 & 0 & 0 \\ 0 & 3170 & 3115 & 3152 & 3226 \\ 0 & 3161 & 3161 & 3226 & 3115 \\ 1 & 3170 & 3161 & 3170 & 3161 \\ 0 & 3161 & 3226 & 3115 & 3161 \end{pmatrix} \quad B_4 = \begin{pmatrix} 0 & 0 & 12663 & 0 & 0 \\ 0 & 3161 & 3161 & 3226 & 3115 \\ 0 & 3226 & 3170 & 3115 & 3152 \\ 0 & 3115 & 3161 & 3161 & 3226 \\ 1 & 3161 & 3170 & 3161 & 3170 \end{pmatrix}$$

Remark 17 The cyclotomic field $\mathbb{Q}(\xi_{37})$ has a cyclic Galois group so has only one subfield of extension degree 4 over \mathbb{Q} , whose algebraic integer ring has a basis given by the Gauss periods of index 4 over \mathbb{F}_{37} , denoted by η_0, \dots, η_3 as usual. We can express the ρ in terms of the linear combinations of these η_i 's over \mathbb{Z} as follows: with $g = 37$, we have $\rho = 9 + 37\eta_0$; with $g = -107$, we have $\rho = 8 + 35\eta_0 + 5\eta_1 - 7\eta_3$. In both cases, τ is a conjugate of ρ .

6 Concluding remarks

In this paper, we showed that there do not exist any two-, three- or four-class non-symmetric primitive translation schemes of prime square order. On the other hand, we found new nonsymmetric four- and five-class association schemes from cyclotomy as fission schemes of certain symmetric three-class association schemes. Moreover, we provided one example of skew-symmetric four-class association schemes as a fission scheme of a conference graph other than the cyclotomic scheme of index 2, which gives an affirmative answer to a question raised in [34].

We close this paper by giving some interesting problems for future work.

1. Generalize Theorem 11 for general $d \geq 5$, or find examples of nonsymmetric primitive translation schemes of prime square order with more than four classes.
2. Find analogies of Theorems 12 and 14 in index more than 2 cases. In particular, in index 4 case, the Gauss sums with characters of order $N = p_1$, where p_1 is a prime, have already been evaluated in [11].
3. Generalize the skew-symmetric four-class association scheme in Sect. 5 into an infinite family. For an odd prime p , the finite field \mathbb{F}_{p^3} already has a very rich structure. It will be interesting to construct more translation schemes in this field.

Acknowledgments The authors thank the referees and the editor for very detailed suggestions and comments that helped to improve the presentation of the paper. T. Feng was supported by Fundamental Research Fund for the Central Universities of China, Zhejiang Provincial Natural Science Foundation under Grant LQ12A01019, the National Natural Science Foundation of China under Grant 11201418, and the Research Fund for Doctoral Programs from the Ministry of Education of China under Grant 20120101120089. The work of K. Momihara was supported by JSPS under Grant-in-Aid for Young Scientists (B) 25800093 and Scientific Research (C) 24540013

References

1. Bannai, E.: Subschemes of some association schemes. *J. Algebra* **144**, 167–188 (1991)
2. Bannai, E., Ito, T.: *Algebraic Combinatorics I. Association Schemes*, Benjamin/Cumming, California (1984)
3. Bannai, E., Song, S.-Y.: Character tables of fission schemes and fusion schemes. *Eur. J. Comb.* **14**, 385–396 (1993)
4. Berndt, B., Evans, R., Williams, K.S.: *Gauss and Jacobi Sums*. Wiley, Toronto (1997)
5. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. *J. Symb. Comput.* **24**, 235–265 (1997)
6. Brouwer, A.E., Cohen, A.M., Neumaier, A.: *Distance-Regular Graphs*, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, 18. Springer, Berlin (1989)
7. Brouwer, A.E., Haemers, W.H.: *Spectra of Graphs*. Springer, New York (2012)
8. Chia, G.L., Kok, W.K.: On nonsymmetric commutative association schemes with exactly one pair of nonsymmetric relations. *Discr. Math.* **306**, 3189–3222 (2006)
9. Enomoto, H., Mena, R.A.: Distance-regular digraphs of girth 4. *J. Comb. Theory. Ser. B* **43**, 293–302 (1987)
10. Faradžev, I.A., Klin, M.H., Muzichuk, M.E.: Cellular rings and groups of automorphisms of graphs. In: Faradžev, I.A., Ivanov, A.A., Klin, M.H., Woldar, A.J. (eds.) *Investigations in Algebraic Theory of Combinatorial Objects*, pp. 1–152. Kluwer, Dordrecht (1994)
11. Feng, K., Yang, J., Luo, S.: Gauss sum of index 4: (1) cyclic case. *Acta. Math. Sin. (Engl. Ser.)* **21**, 1425–1434 (2005)
12. Feng, T., Xiang, Q.: Cyclotomic constructions of skew Hadamard difference sets. *J. Comb. Theory. Ser. A* **119**, 245–256 (2012)
13. Feng, T., Xiang, Q.: Strongly regular graphs from union of cyclotomic classes. *J. Comb. Theory. Ser. B* **102**, 982–995 (2012)
14. Feng, T., Momihara, K., Xiang, Q.: Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. [arXiv:1201.0701](https://arxiv.org/abs/1201.0701)
15. Feng, T., Wu, F., Xiang, Q.: Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes. *Des. Codes Cryptogr.* **65**, 247–257 (2012)
16. Goldbach, R.W., Claassen, H.L.: A primitive nonsymmetric 3-class association scheme on 36 elements with $p_{11}^1 = 0$ exists and is unique. *Eur. J. Comb.* **15**, 519–524 (1994)
17. Goldbach, R.W., Claassen, H.L.: Feasibility conditions for nonsymmetric 3-class association schemes. *Discr. Math.* **159**, 111–118 (1996)

18. Gol'fand, Ja.Ju., Ivanov, A.V., Klin, M.H.: Amorphic cellular rings. In: Faradžev, I.A., Ivanov, A.A., Klin, M.H., Woldar, A.J. (eds.) *Investigations in Algebraic Theory of Combinatorial Objects*, pp. 167–184. Kluwer, Dordrecht (1994)
19. Hanaki, A., Uno, K.: Algebraic structure of association schemes of prime order. *J. Algebr. Comb.* **23**, 189–195 (2006)
20. Ivanov, A.A., Klin, M.H., Faradžev, I.A.: *The Primitive Representations of the Non-Abelian Simple Groups of Order Less Than 106: Part 2 (Russian)*. Preprint, Institute for System Studies, Moscow (1984)
21. Ivanov, A.A., Praeger, C.E.: Problem session at ALCOM-91. *Euro. J. Comb.* **15**, 105–112 (1994)
22. Jørgensen, L.K.: Algorithmic approach to nonsymmetric 3-class association schemes. In: Klin, M.H., Jones, G.A., Jurisic, A., Muzychuk, M., Ponomarenko, I. (eds.) *Algorithmic Algebraic Combinatorics and Gröbner Bases*, pp. 251–268. Springer, Berlin (2009)
23. Jørgensen, L.K.: Schur rings and nonsymmetric association schemes on 64 vertices. *Discr. Math* **310**, 3259–3266 (2010)
24. Lidl, R., Niederreiter, H.: *Finite Fields*. Cambridge Univ. Press, Cambridge (1997)
25. Liebler, R.A., Mena, R.A.: Certain Distance regular digraphs and related rings of characteristic 4. *J. Comb. Theory. Ser. B* **47**, 111–123 (1988)
26. Ma, S.L.: A survey of partial difference sets. *Des. Codes Cryptogr.* **4**, 221–261 (1994)
27. Ma, J.: Three-class association schemes on Galois rings in characteristic 4. *Graphs Comb.* **23**, 73–86 (2007)
28. Ma, J.: The nonexistence of certain skew-symmetric amorphous association schemes. *Eur. J. Comb.* **31**, 1671–1679 (2010)
29. Ma, J., Wang, K.: Four-class skew-symmetric association schemes. *J. Comb. Theory. Ser. A* **118**, 1381–1391 (2011)
30. Momihara, K.: Cyclotomic strongly regular graphs, skew Hadamard difference sets, and rationality of relative Gauss sums. *Eur. J. Comb.* **34**, 706–723 (2013)
31. Muzychuk, M.E.: *V-rings of permutation groups with invariant metric*. Ph.D. thesis, Kiev State University (1987)
32. Pott, A.: *Finite Geometries and Character Theory*. Lecture Notes in Mathematics 1601. Springer, Berlin (1995)
33. Song, S.-Y.: Class 3 association schemes whose symmetrization have two classes. *J. Comb. Theory. Ser. A* **70**, 1–29 (1995)
34. Song, S.-Y.: Commutative association schemes whose symmetrizations have two classes. *J. Algebr Comb.* **5**, 47–55 (1996)
35. van Dam, E.R., Muzychuk, M.: Some implications on amorphic association schemes. *J. Comb. Theory. Ser. A* **117**, 111–127 (2010)
36. Yang, J., Xia, L.: Complete solving of explicit evaluation of Gauss sums in the index 2 case. *Sci. China Ser. A* **53**, 2525–2542 (2010)