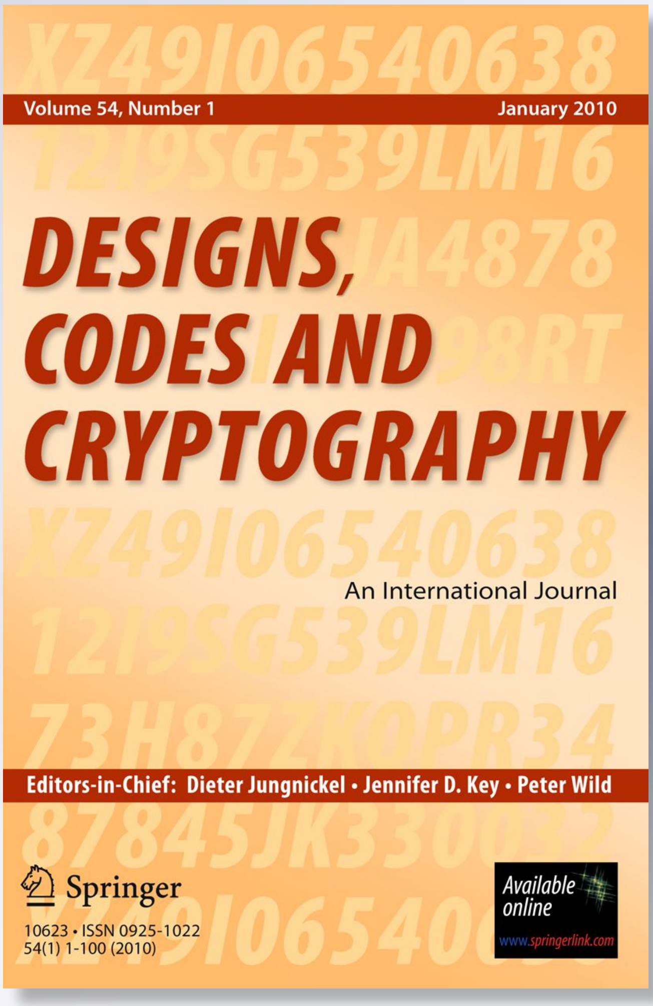

Des. Codes Cryptogr.
DOI 10.1007/s10623-011-9595-9

Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes

Tao Feng · Fan Wu · Qing Xiang

Received: 7 December 2010 / Revised: 3 October 2011 / Accepted: 30 November 2011

Abstract We construct twelve infinite families of pseudocyclic and non-amorphic association schemes, in which each nontrivial relation is a strongly regular graph. Three of the twelve families generalize the counterexamples to A. V. Ivanov's conjecture by Ikuta and Munemasa (Eur J Combin 31:1513–1519, 2010).

Keywords Amorphic association scheme · Cyclotomy · Gauss sum · Index 2 Gauss sum · Pseudocyclic association scheme · Strongly regular graph

Mathematics Subject Classification (2010) 05E30 · 11T22

1 Introduction

This note is a sequel to [12]. We assume that the reader is familiar with the basic theory of association schemes as can be found in [2,7]. For background in strongly regular graphs, we refer the reader to [8,13]. All association schemes considered in this paper are commutative and symmetric. Let $(X, \{R_i\}_{0\leq i\leq d})$ be an association scheme with d classes. For $i \in \{0, 1, \ldots, d\}$, let A_i be the adjacency matrix of the relation R_i, and let $E_0 = \frac{1}{|X|}J, E_1, \ldots, E_d$ be the primitive idempotents of the Bose-Mesner algebra of the scheme $(X, \{R_i\}_{0\leq i\leq d})$, where J is the all-one matrix of size $|X| \times |X|$. The basis transition matrix from $\{E_0, E_1, \ldots, E_d\}$ to

This is one of several papers published together in *Designs, Codes and Cryptography* on the special topic: "Combinatorics – A Special Issue Dedicated to the 65th Birthday of Richard Wilson".

T. Feng · F. Wu · Q. Xiang (✉)
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
e-mail: xiang@math.udel.edu

F. Wu
e-mail: wufan@math.udel.edu

Present Address:
T. Feng
Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China
e-mail: pku.tfeng@yahoo.com.cn

Published online: 27 December 2011

$\{A_0, A_1, \ldots, A_d\}$ is denoted by $P = \big(p_j(i)\big)_{0 \le i, j \le d}$, and usually called the *first eigenmatrix* (or *character table*) of the scheme. Explicitly P is the $(d+1) \times (d+1)$ matrix with rows and columns indexed by $0, 1, 2, \ldots, d$ such that

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d)P.$$

Let $k_i = p_i(0)$ and $m_i = \mathrm{rank}(E_i)$. The k_i's and m_i's are called *valencies* and *multiplicities* of the scheme, respectively. We say that the scheme $(X, \{R_i\}_{0 \le i \le d})$ is *pseudocyclic* if there exists an integer t such that $m_i = t$ for all $i \in \{1, \ldots, d\}$. A classical example of pseudocyclic association schemes is the cyclotomic association scheme over a finite field, which we define below.

Let $q = p^f$, where p is a prime and f a positive integer. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $N|(q-1)$ with $N > 1$. Let $C_0 = \langle \gamma^N \rangle$, and $C_i = \gamma^i C_0$ for $1 \le i \le N-1$. Assume that $-1 \in C_0$. Define $R_0 = \{(x, x) \mid x \in \mathbb{F}_q\}$, and for $i \in \{1, 2, \ldots, N\}$, define $R_i = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbb{F}_q, \{R_i\}_{0 \le i \le N})$ is an association scheme. We will call this scheme *the cyclotomic association scheme of class N over $\mathbb{F}_q$*. The first eigenmatrix P of the cyclotomic scheme of class N is the following $(N+1)$ by $(N+1)$ matrix (with the rows of P arranged in a certain way)

$$P = \begin{pmatrix} 1 & \frac{N-1}{q} & \frac{N-1}{q} & \frac{N-1}{q} & \ldots & \frac{N-1}{q} \\ 1 & \eta_{N-1} & \eta_0 & \eta_1 & \cdots & \eta_{N-2} \\ 1 & \eta_{N-2} & \eta_{N-1} & \eta_0 & \cdots & \eta_{N-3} \\ \vdots & & & & & \\ 1 & \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{N-1} \end{pmatrix} \tag{1.1}$$

where the η_i's are the cyclotomic periods (or Gauss periods) of order N defined by

$$\eta_i = \sum_{x \in C_i} \psi(x).$$

In the above defintion, ψ is the additive character of $\mathbb{F}_q$ defined by

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \xi_p^{\mathrm{Tr}(x)}, \tag{1.2}$$

where $\xi_p = e^{2\pi i/p}$ and Tr is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$.

The following theorem gives combinatorial characterizations of pseudocyclic association schemes.

Theorem 1.1 *Let $(X, \{R_i\}_{0 \le i \le d})$ be an association scheme, and for $x \in X$ and $1 \le i \le d$, let $R_i(x) = \{y \mid (x, y) \in R_i\}$. Then the following are equivalent.*

(1) $(X, \{R_i\}_{0 \le i \le d})$ *is pseudocyclic.*
(2) *For some constant k, we have $k_j = k$ and $\sum_{i=1}^{d} p_{ii}^{j} = k - 1$, for $1 \le j \le d$.*
(3) $(X, \mathcal{B})$ *is a $2 - (v, k, k-1)$ design, where $\mathcal{B} = \{R_i(x) \mid x \in X, 1 \le i \le d\}$.*

For a proof of this theorem, we refer the reader to [7, p. 48] and [14, p. 84]. Part 2 of the above theorem will be useful in Sect. 3.

Let $(X, \{R_i\}_{0 \le i \le d})$ be an association scheme. For a partition $\Lambda_0 := \{0\}, \Lambda_1, \ldots, \Lambda_{d'}$ of $\{0, 1, \ldots, d\}$, let $R_{\Lambda_i} = \cup_{k \in \Lambda_i} R_k$, for $0 \le i \le d'$. If $(X, \{R_{\Lambda_i}\}_{0 \le i \le d'})$ forms an association scheme, then we say that $(X, \{R_{\Lambda_i}\}_{0 \le i \le d'})$ is a *fusion scheme* of the original scheme. If $(X, \{R_{\Lambda_i}\}_{0 \le i \le d'})$ is an association scheme for every partition $\{\Lambda_i\}_{0 \le i \le d'}$ of $\{0, 1, 2, \ldots, d\}$ with $\Lambda_0 = \{0\}$, then we call the original scheme $(X, \{R_i\}_{0 \le i \le d})$ *amorphic*. For a recent survey on amorphic association schemes, we refer the reader to [11]. Given a partition $\{\Lambda_i\}_{0\le i\le d'}$ of $\{0, 1, 2, \ldots, d\}$ with $\Lambda_0 = \{0\}$, there is a simple criterion in terms of the first eigenmatrix P of $(X, \{R_i\}_{0\le i\le d})$ for deciding whether $(X, \{R_{\Lambda_i}\}_{0\le i\le d'})$ forms an association scheme or not. We state this criterion below.

The Bannai–Muzychuk Criterion. Let P be the first eigenmatrix of an association scheme $(X, \{R_i\}_{0\le i\le d})$. Let $\Lambda_0 := \{0\}, \Lambda_1, \ldots, \Lambda_{d'}$ be a partition of $\{0, 1, \ldots, d\}$. Then $(X, \{R_{\Lambda_i}\}_{0\le i\le d'})$ forms an association scheme if and only if there exists a partition $\{\Delta_i\}_{0\le i\le d'}$ of $\{0, 1, 2, \ldots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j)-block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i, Λ_j)-block is the (i, j) entry of the first eigenmatrix of the fusion scheme. (For a proof of this criterion we refer the reader to [1,21].)

A. V. Ivanov conjectured in [16] 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. A counterexample was given by Van Dam [9] in the case where the association scheme is imprimitive. Later on, Van Dam [10] also gave a counterexample in the case where the association scheme is primitive. More counterexamples were given by Ikuta and Munemasa [15] in the primitive case. However, it should be noted that there are only a few known counterexamples to Ivanov's conjecture in the primitive case (cf. [15]).

The purpose of this note is to generalize the counterexamples to Ivanov's conjecture by Ikuta and Munemasa [15] into infinite families. Along the way, we obtain many more infinite families of counterexamples to Ivanov's conjecture in the primitive case. The counterexamples we came up with are all pseudocyclic fusion schemes of the cyclotomic schemes. One of the main tools that we use is the theory of Gauss sums, which we review in the next section.

2 Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. Let $\xi_p = e^{2\pi i/p}$ and let ψ be the additive character of $\mathbb{F}_q$ defined in (1.2). Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*$$

be a character of $\mathbb{F}_q^*$. We define the *Gauss sum* by

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

Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0) = -1$. We are usually concerned with nontrivial Gauss sums $g(\chi)$, i.e., those with $\chi \neq \chi_0$.

While it is easy to show that the absolute value of a nontrivial Gauss sum $g(\chi)$ is equal to $\sqrt{q}$, the explicit determination of Gauss sums is a difficult problem. However, there are a few cases where the Gauss sums $g(\chi)$ can be explicitly evaluated. The simplest case is the so-called *semi-primitive case*, where there exists an integer j such that $p^j \equiv -1 \pmod{N}$ (N is the order of χ in $\widehat{\mathbb{F}_q^*}$, the character group of $\mathbb{F}_q^*$). Some authors [5,6] also refer to this case as uniform cyclotomy, or pure Gauss sums. We refer the reader to [6, p. 364] for the precise evaluation of Gauss sums in this case.

The next interesting case is the index 2 case, where -1 is not in the subgroup $\langle p\rangle$, the cyclic group generated by p, and $\langle p\rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$ (again here N is the order of χ in $\widehat{\mathbb{F}_q^*}$). Many authors have investigated this case, including Baumert and Mykkeltveit [4], McEliece [19], Langevin [17], Mbodj [18], Meijer and Van de Vlugt [20], and Yang and Xia [22]. In the index 2 case, it can be shown that N has at most two odd prime divisors. Assume that N is odd, we have the following three possibilities in the index 2 case (see [22]): Below both p_1 and p_2 are primes.

(1) $N = p_1^m$, $p_1 \equiv 3 \pmod 4$;
(2) $N = p_1^m p_2^n$, $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$;
(3) $N = p_1^m p_2^n$, $p_1 \equiv 1, 3 \pmod 4$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $p_2 \equiv 3 \pmod 4$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)/2$.

We state below the results on evaluation of Gauss sums in Case (1) and (2) from the above list.

Theorem 2.1 *(Langevin [17]) Let $N = p_1^m$, where m is a positive integer, p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3 \pmod 4$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ (that is, $f := \mathrm{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0},$$

where

(1) $h_0 = \frac{f-h}{2}$,
(2) $b, c \not\equiv 0 \pmod p$,
(3) $b^2 + p_1c^2 = 4p^h$,
(4) $bp^{h_0} \equiv -2 \pmod{p_1}$.

Theorem 2.2 *(Mbodj [18]) Let $N = p_1^m p_2^n$, where m, n are positive integers, p_1 and p_2 are prime such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ (that is, $f := \mathrm{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0},$$

where

(1) $h_0 = \frac{f-h}{2}$,
(2) $b, c \not\equiv 0 \pmod p$,
(3) $b^2 + p_1p_2c^2 = 4p^h$,
(4) $b \equiv 2p^{h/2} \pmod{\ell}$, *here $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.*

3 Pseudocyclic fusion schemes of the cyclotomic schemes

Let p be a prime, f be a positive integer and $q = p^f$. Let γ be a fixed primitive element of $\mathbb{F}_q$, and $N > 1$ be an integer such that $N|(q-1)$. As we did in Section 1, let $C_0 = \langle\gamma^N\rangle$ and $C_i = \gamma^i C_0$ for $1 \le i \le N-1$. Assume that $-1 \in C_0$. Define $R_0 = \{(x, x) \mid x \in \mathbb{F}_q\}$, and for $i \in \{1, 2, \ldots, N\}$, define $R_i = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbb{F}_q, \{R_i\}_{0\le i\le N})$ is the cyclotomic association scheme of class N on $\mathbb{F}_q$. It was proven by Baumert, Mills and Ward [5] that $(\mathbb{F}_q, \{R_i\}_{0\le i\le N})$ is amorphic if and only if -1 is congruent to a power of p

modulo N (i.e., the so-called semi-primitive condition holds). See also [3] for a proof of this fact. Below we will show that even though in the index 2 case the cyclotomic association scheme $(\mathbb{F}_q, \{R_i\}_{0\le i\le N})$ is not amorphic, we can still have interesting fusion schemes of $(\mathbb{F}_q, \{R_i\}_{0\le i\le N})$.

3.1 The index 2 case with $N = p_1^m p_2$

In this subsection, we assume that $N = p_1^m p_2\,(m \ge 1), p_1, p_2$ are primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, p is a prime such that $\gcd(p, N) = 1, \mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $\mathrm{ord}_{p_2}(p) = \phi(p_2)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$. Note that here we have $-C_i = C_i$ for all $0 \le i \le N-1$ since either $2N|(q-1)$ or q is even. For convenience, we define $d := p_1 p_2$. For $0 \le k \le d-1$, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} C_{ip_2 + kp_1^{m-1}} \tag{3.1}$$

Note that $D_k = \gamma^{kp_1^{m-1}} D_0$ and $\{0\}, D_0, D_1, \ldots, D_{d-1}$ form a partition of $\mathbb{F}_q$. Now define $R'_0 = R_0$ and

$$R'_k = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}. \tag{3.2}$$

We will show that $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is a fusion scheme of $(\mathbb{F}_q, \{R_i\}_{0\le i\le N})$. The proof depends on the following evaluation of Gauss sums in the index 2 case, and results from [12].

Let χ_1 be the multiplicative character of order p_1^m of $\mathbb{F}_q$ defined by $\chi_1(\gamma) = \exp(\frac{2\pi i}{p_1^m})$, and let χ_2 be the multiplicative character of order p_2 of $\mathbb{F}_q$ defined by $\chi_2(\gamma) = \exp(\frac{2\pi i}{p_2})$. By Theorem 2.2, we have

$$g(\bar{\chi}_1\bar{\chi}_2) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0}, \tag{3.3}$$

where $h_0 = \frac{f-h}{2}$ (h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$), $b, c \not\equiv 0 \pmod p$, $b^2 + p_1p_2c^2 = 4p^h$, and $b \equiv 2p^{h/2} \pmod \ell$, here $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.

Theorem 3.1 *With the definition of R'_k given in (3.2), $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is a pseudocyclic association scheme.*

Proof We will first prove that $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is an association scheme by using the Bannai–Muzychuk criterion discussed in Sect. 1.

For each $a, 0 \le a \le N-1$, there exists a unique $i_a \in \{0, 1, \ldots, p_1^{m-1} - 1\}$ such that $p_1^{m-1} \mid (a + p_2 i_a)$. It follows that there is a unique $j_a, 0 \le j_a \le p_1p_2 - 1$, such that $a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod N$. It is now easy to check that $-ip_2 + jp_1^{m-1}, 0 \le i \le p_1^{m-1} - 1$ and $0 \le j \le p_1p_2 - 1$, form a complete set of residues modulo N.

The group of additive characters of $\mathbb{F}_q$ consists of ψ_0 and $\psi_{\gamma^a}, 0 \le a \le q-2$, where ψ_0 is the trivial character and ψ_{γ^a} is defined by

$$\psi_{\gamma^a} : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi_{\gamma^a}(x) = \xi_p^{\mathrm{Tr}(\gamma^a x)}. \tag{3.4}$$

We usually write ψ_1 simply as ψ. The character values of D_0 were computed in the proof of Theorem 5.1 [12]. Since D_k is a (multiplicative) translate of D_0, we know the character values of D_k as well. Explicitly, for each $a, 0 \le a \le N-1$, write

$$a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod{N},$$

with $0 \le i_a \le p_1^{m-1} - 1$ and $0 \le j_a \le p_1 p_2 - 1$. For convenience we introduce the Kronecker delta δ_{a,p_1}, which equals 1 if $p_1 | a$, 0 otherwise. Also we define δ_{a,p_2} by setting it equal to 1 if $p_2 | a$, 0 otherwise. By the results in [12], we have

$$\psi_{\gamma^a}(D_k) = \psi(\gamma^{a+p_1^{m-1}k} D_0) = \frac{1}{N} T_{a+p_1^{m-1}k},$$

where

$$\begin{aligned} T_{a+p_1^{m-1}k} &= -p_1^{m-1} - (-1)^{\frac{p_1-1}{2}} p_1^{m-1} p_2 \sqrt{q}\,\delta_{a+p_1^{m-1}k,p_2} - (-1)^{\frac{p_2-1}{2}} p_1^m \sqrt{q}\,\delta_{j_a+k,p_1} \\ &\quad + \frac{b}{2} p^{h_0} p_1^{m-1} (p_1 \delta_{j_a+k,p_1} - 1)(p_2 \delta_{a+p_1^{m-1}k,p_2} - 1) \\ &\quad - \left(\frac{a+p_1^{m-1}k}{p_2}\right)\left(\frac{j_a+k}{p_1}\right) \frac{c}{2} p^{h_0} p_1^m p_2 \end{aligned}$$

In the above formula, b, c are given by (3.3), $(\frac{\cdot}{p_2})$ and $(\frac{\cdot}{p_1})$ are Legendre symbols. Observe that $a + p_1^{m-1}k \equiv -p_2 i_a + p_1^{m-1}(j_a + k) \pmod{N}$. So $\delta_{a+p_1^{m-1}k,p_2} = \delta_{j_a+k,p_2}$, and $\left(\frac{a+p_1^{m-1}k}{p_2}\right) = \left(\frac{p_1}{p_2}\right)^{m-1}\left(\frac{j_a+k}{p_2}\right)$. Therefore, $\psi_{\gamma^a}(D_k)$ is independent of i_a.

In order to apply the Bannai–Muzychuk criterion, we define the following partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each j, $0 \le j \le d-1$, define

$$\Delta_{j+1} = \{\psi_{\gamma^{-p_2 i + p_1^{m-1} j}} \mid 0 \le i \le p_1^{m-1} - 1\},$$

and $\Delta_0 = \{\psi_0\}$. Clearly $\Delta_0, \Delta_1, \ldots, \Delta_d$ form a partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each $0 \le k \le d-1$, since $\psi_{\gamma^a}(D_k)$ is independent of i_a (here $a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod{N}$), we see that $\psi_{\gamma^a}(D_k)$ is a constant for those a in the same subset of the above partition. By the Bannai–Muzychuk criterion (with $\Lambda_0 = \{0\}$, $\Lambda_{j+1} = \{1 + ip_2 + p_1^{m-1} j \mid 0 \le i \le p_1^{m-1} - 1\}$, $0 \le j \le d-1$), we see that $(\mathbb{F}_q, \{R'_0, R'_1, \ldots, R'_d\})$ is an association scheme.

Next we show that the association scheme $(\mathbb{F}_q, \{R'_k\}_{0 \le k \le d})$ is pseudocyclic. To this end, we show that the following group ring equation holds in $\mathbb{Z}[(\mathbb{F}_q, +)]$.

Claim: $\sum_{k=0}^{d-1} D_k^2 = (q-1) \cdot 0_{\mathbb{F}_q} + \left(\frac{q-1}{p_1 p_2} - 1\right)(\mathbb{F}_q - 0_{\mathbb{F}_q})$, where $0_{\mathbb{F}_q}$ is the zero element in $\mathbb{F}_q$.

For any a, $0 \le a \le N-1$, we write $a \equiv -i_a p_2 + j_a p_1^{m-1} \pmod{N}$ with $i_a \in \{0, 1, \ldots, p_1^{m-1} - 1\}$ and $j_a \in \{0, 1, 2, \ldots, d-1\}$. Since $\psi_{\gamma^a}(D_k)$ is independent of i_a, we may assume that $i_a = 0$. We now compute

$$\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2 = \frac{1}{N^2} \sum_{k=0}^{d-1} T^2_{p_1^{m-1}(j_a+k)} = \frac{1}{N^2} \sum_{k=0}^{d-1} T^2_{kp_1^{m-1}}$$

Since the last expression above is independent of a, we see that $\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2$ are equal to the same constant for all $0 \le a \le N-1$. Since each D_k is a union of some N-th cyclotomic classes, it follows that $\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2$ are equal to the same constant for all $0 \le a \le q-2$. Therefore, by the inversion formula, we have

$$\sum_{k=0}^{d-1} D_k^2 = (n - \lambda) \cdot 0_{\mathbb{F}_q} + \lambda \mathbb{F}_q,$$

for some integers n, λ. Now applying the principal character to both sides, and computing the coefficients of $0_{\mathbb{F}_q}$ on both sides, we have

$$n = p_1 p_2 \cdot \frac{q-1}{p_1 p_2},$$
$$n + (q-1)\lambda = d \cdot \left(\frac{q-1}{p_1 p_2}\right)^2.$$

It follows that $n = q - 1$, and $\lambda = \frac{q-1}{p_1 p_2} - 1$. The claim is now established. A direct consequence is that $\sum_{i=0}^{d-1} p_{i,i}^j = \frac{q-1}{N} - 1$, for all j, where $p_{i,i}^j$ are the intersection parameters given by $D_i^2 = \sum_{j=0}^{d-1} p_{i,i}^j D_j + p_{i,i}^0 \cdot 0_{\mathbb{F}_q}$. By Part (2) of Theorem 1.1, the association scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le d})$ is pseudocyclic. The proof is complete. □

In order to obtain counterexamples to Ivanov's conjecture, we need to have each $R_k'(1 \le k \le d)$ in Theorem 3.1 to be strongly regular. Note that R_k' is just the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D_{k-1})$, and $\mathrm{Cay}(\mathbb{F}_q, D_{k-1}) \cong \mathrm{Cay}(\mathbb{F}_q, D_0)$ for all $1 \le k \le d$ since $D_{k-1} = \gamma^{(k-1)p_1^{m-1}} D_0$. It follows that if $\mathrm{Cay}(\mathbb{F}_q, D_0)$ is strongly regular, then all R_k', $1 \le k \le d$, are strongly regular. In [12], we obtained necessary and sufficient conditions for $\mathrm{Cay}(\mathbb{F}_q, D_0)$ to be strongly regular, which we quote below.

Theorem 3.2 (Corollary 5.2 in [12]) *With b, c, h given in (3.3),* $\mathrm{Cay}(\mathbb{F}_q, D_0)$ *is a strongly regular graph if and only if $b, c \in \{1, -1\}$, h is even and $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}} b$, $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}} b$.*

In [12], we used a computer to search for p, p_1, p_2 satisfying the conditions in Theorem 3.2. We found six infinite families of strongly regular graphs in this way. By the discussion preceding Theorem 3.2, and since the parameters of each of the six examples of srg are neither Latin square type nor negative Latin square type, each of the six families of srg gives rise to an infinite class of counterexamples to Ivanov's conjecture. Below we list the parameters of these examples. For the detailed reasons why we have strongly regular graphs, we refer the reader to [12].

Example 3.3 Let $p = 2, q = 2^{4 \cdot 3^{m-1}}$, $p_1 = 3$, $p_2 = 5$, $N = 3^m \cdot 5$, with $m \ge 1$. Then we have a 15-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le 15})$ in which each relation R_k', $1 \le k \le 15$, is strongly regular.

We remark that when $m = 2$, Example 3.3 is the same as Example 1 in [15].

Example 3.4 Let $p = 2, q = 2^{4 \cdot 5^{m-1}}$, $p_1 = 5$, $p_2 = 3$, $N = 5^m \cdot 3$, with $m \ge 1$. Then we have a 15-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le 15})$ in which each relation R_k', $1 \le k \le 15$, is strongly regular.

We remark that when $m = 2$, Example 3.4 is the same as Example 2 in [15].

Example 3.5 Let $p = 3, q = 3^{12 \cdot 5^{m-1}}$, $p_1 = 5$, $p_2 = 7$, $N = 5^m \cdot 7$, with $m \ge 1$. Then we have a 35-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le 35})$ in which each relation R_k', $1 \le k \le 35$, is strongly regular.

Example 3.6 Let $p = 3, q = 3^{12 \cdot 5^{m-1}}$, $p_1 = 7$, $p_2 = 5$, $N = 7^m \cdot 5$, with $m \ge 1$. Then we have a 35-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le 35})$ in which each relation R_k', $1 \le k \le 35$, is strongly regular.

Example 3.7 Let $p = 3, q = 3^{144\cdot 17^{m-1}}, p_1 = 17, p_2 = 19, N = 17^m \cdot 19$, with $m \geq 1$. Then we have a 323-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 323})$ in which each relation R'_k, $1 \leq k \leq 323$, is strongly regular.

Example 3.8 Let $p = 3, q = 3^{144\cdot 19^{m-1}}, p_1 = 19, p_2 = 17, N = 19^m \cdot 17$, with $m \geq 1$. Then we have a 323-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 323})$ in which each relation R'_k, $1 \leq k \leq 323$, is strongly regular.

We remark that by using Corollary 3.2 in [15], one can further obtain 3-class fusion schemes of the above pseudocyclic association schemes, in which two relations are strongly regular graphs, while the third relation is not (see the character table of these 3-class fusion schemes in the statement of Corollary 3.2 of [15]).

3.2 The index 2 case with $N = p_1^m$

In this subsection, we assume that $N = p_1^m$ (here $m \geq 1$, $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$), p is a prime such that $\gcd(N, p) = 1$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$. Note that $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N|(q-1)$ or q is even. For $0 \leq k \leq p_1 - 1$, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} C_{i+kp_1^{m-1}} \tag{3.5}$$

Note that $D_k = \gamma^{kp_1^{m-1}} D_0$ and $\{0\}, D_0, D_1, \ldots, D_{p_1-1}$ form a partition of $\mathbb{F}_q$. Now define $R'_0 = R_0$ and

$$R'_k = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}. \tag{3.6}$$

We will show that $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq p_1})$ is a fusion scheme of $(\mathbb{F}_q, \{R_i\}_{0\leq i\leq N})$. The proof depends on the following evaluation of Gauss sums in the index 2 case, and results from [12].

Let χ be the multiplicative character of $\mathbb{F}_q$ defined by $\chi(\gamma) = \exp(\frac{2\pi i}{N})$. By Theorem 2.1, we have

$$g(\bar{\chi}) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0}, \quad b, c \not\equiv 0 \pmod{p}, \tag{3.7}$$

where $h_0 = \frac{f-h}{2}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $b^2 + p_1c^2 = 4p^h$, and $bp^{h_0} \equiv -2 \pmod{p_1}$.

Theorem 3.9 *With the definition of R'_k given in (3.6), $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq p_1})$ is a pseudocyclic association scheme.*

Proof The proof is similar to that of Theorem 3.1. For each a, $0 \leq a \leq N-1$, there is a unique $i_a \in \{0, 1, \ldots, p_1^{m-1} - 1\}$, such that $p_1^{m-1}|(a + i_a)$. It follows that there is a unique j_a, $0 \leq j_a \leq p_1 - 1$, such that $a \equiv -i_a + p_1^{m-1} j_a \pmod{N}$. It is now easy to check that $-i + jp_1^{m-1}$, $0 \leq i \leq p_1^{m-1} - 1$ and $0 \leq j \leq p_1 - 1$, form a complete set of residues modulo N.

The group of additive characters of $\mathbb{F}_q$ consists of ψ_0 and ψ_{γ^a}, $0 \leq a \leq q-2$. The character values of D_0 were computed in the proof of Theorem 4.1 [12]. Since D_k is a (multiplicative) translate of D_0, we know the character values of D_k as well. Explicitly, for each a, $0 \leq a \leq N-1$, write

$$a \equiv -i_a + p_1^{m-1} j_a \pmod{N},$$

with $0 \leq i_a \leq p_1^{m-1} - 1$ and $0 \leq j_a \leq p_1 - 1$. For convenience, we also introduce the Kronecker delta δ_{j_a}, which equals 1 if $p_1 | j_a$, and 0 otherwise. By the results in [12], we have

$$\psi_{\gamma^a}(D_k) = \psi(\gamma^{a+kp_1^{m-1}} D_0) = \frac{1}{N} T_{a+kp_1^{m-1}},$$

where

$$T_{a+kp_1^{m-1}} = -p_1^{m-1} + \frac{p^{h_0} p_1^{m-1} b}{2}(p_1 \delta_{j_a+k} - 1) - \frac{p^{h_0} p_1^m c}{2}\left(\frac{j_a + k}{p_1}\right).$$

In the above formula, b, c are given in (3.7), and $(\frac{\cdot}{p_1})$ is the Legendre symbol. It is important to note that $\psi_{\gamma^a}(D_k)$ is independent of i_a.

We define the following partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each j, $0 \leq j \leq p_1 - 1$, we define

$$\Delta_{j+1} = \{\psi_{\gamma^{-i+p_1^{m-1} j}} \mid 0 \leq i \leq p_1^{m-1} - 1\},$$

and $\Delta_0 = \{\psi_0\}$. Then clearly $\Delta_0, \Delta_1, \ldots, \Delta_{p_1}$ form a partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each $0 \leq k \leq p_1 - 1$, since $\psi_{\gamma^a}(D_k)$ is independent of i_a (here $a \equiv -i_a + p_1^{m-1} j_a \pmod{N}$), we see that $\psi_{\gamma^a}(D_k)$ is a constant for those a in the same subset of the above partition. By the Bannai–Muzychuk criterion (with $\Lambda_0 = \{0\}$, $\Lambda_{j+1} = \{1 + i + p_1^{m-1} j \mid 0 \leq i \leq p_1^{m-1} - 1\}$, $0 \leq j \leq p_1 - 1$), we see that $(\mathbb{F}_q, \{R'_0, R'_1 \ldots, R'_{p_1}\})$ is an association scheme.

Similarly we can show that the following group ring equation holds in $\mathbb{Z}[(\mathbb{F}_q, +)]$:

$$\sum_{k=0}^{p_1-1} D_k^2 = (q-1) \cdot 0_{\mathbb{F}_q} + \left(\frac{q-1}{p_1} - 1\right)(\mathbb{F}_q - 0_{\mathbb{F}_q}),$$

from which the pseudocyclicity of the scheme $(\mathbb{F}_q, \{R'_0, R'_1, \ldots, R'_{p_1}\})$ follows. We omit the details of the proof of the above group ring equation. The proof is now complete. □

In order to obtain counterexamples to Ivanov's conjecture, we need to have each $R'_k (1 \leq k \leq p_1)$ in Theorem 3.9 to be strongly regular. Note that R'_k is just the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D_{k-1})$, and $\mathrm{Cay}(\mathbb{F}_q, D_{k-1}) \cong \mathrm{Cay}(\mathbb{F}_q, D_0)$ for all $1 \leq k \leq p_1$ since $D_{k-1} = \gamma^{(k-1)p_1^{m-1}} D_0$. Again it follows that if $\mathrm{Cay}(\mathbb{F}_q, D_0)$ is strongly regular, then all R'_k, $1 \leq k \leq p_1$, are strongly regular. In [12], we obtained necessary and sufficient conditions for $\mathrm{Cay}(\mathbb{F}_q, D_0)$ to be strongly regular, which we quote below.

Theorem 3.10 (Corollary 4.2 in [12]) *With b, c given in (3.7),* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a strongly regular graph if and only if $b, c \in \{1, -1\}$.*

In [12], we used a computer to search for p, p_1 satisfying the conditions in Theorem 3.10. We found six infinite families of strongly regular graphs in this way. By the discussion preceding Theorem 3.10, each of the six examples of srg gives rise to a class of infinitely many counterexamples to Ivanov's conjecture. Below we list the parameters of these examples. For the detailed reasons why we have strongly regular graphs, we refer the reader to [12].

Example 3.11 Let $p = 2$, $q = 2^{3 \cdot 7^{m-1}}$, $p_1 = 7$, $N = p_1^m$, $m \geq 1$ is an integer. Then we have a 7-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0 \leq k \leq 7})$ in which each relation R'_k, $1 \leq k \leq 7$, is strongly regular.

We remark that when $m = 2$, Example 3.11 is the same as Example 3 of [15].

Example 3.12 Let $p = 3, q = 3^{53\cdot 107^{m-1}}, p_1 = 107, N = p_1^m, m \geq 1$ is an integer. Then we have a 107-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 107})$ in which each relation $R'_k, 1 \leq k \leq 107$, is strongly regular.

Example 3.13 Let $p = 5, q = 5^{9\cdot 19^{m-1}}, p_1 = 19, N = p_1^m, m \geq 1$ is an integer. Then we have a 19-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 19})$ in which each relation $R'_k, 1 \leq k \leq 19$, is strongly regular.

Example 3.14 Let $p = 5, q = 5^{249\cdot 499^{m-1}}, p_1 = 499, N = p_1^m, m \geq 1$ is an integer. Then we have a 499-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 499})$ in which each relation $R'_k, 1 \leq k \leq 499$, is strongly regular.

Example 3.15 Let $p = 17, q = 17^{33\cdot 67^{m-1}}, p_1 = 67, N = p_1^m, m \geq 1$ is an integer. Then we have a 67-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 67})$ in which each relation $R'_k, 1 \leq k \leq 67$, is strongly regular.

Example 3.16 Let $p = 41, q = 41^{81\cdot 163^{m-1}}, p_1 = 163, N = p_1^m, m \geq 1$ is an integer. Then we have a 163-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 163})$ in which each relation $R'_k, 1 \leq k \leq 163$, is strongly regular.

Again we remark that by using Corollary 3.2 in [15], one can further obtain 3-class fusion schemes of the above pseudocyclic association schemes, in which two relations are strongly regular graphs, while the third relation is not.

Acknowledgments Tao Feng was supported in part by the Fundamental Research Funds for the central universities. Qing Xiang was supported in part by NSF Grant DMS 1001557, by the Overseas Cooperation Fund (Grant 10928101) of China, and by Y. C. Tang disciplinary development fund, Zhejiang University.

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/Cummings, Menlo Park (1984).
3. Bannai E., Munemasa A.: Davenport-Hasse theorem and cyclotomic association schemes. In: Proc. Algebraic Combinatorics, Hirosaki University, Hirosaki (1990).
4. Baumert L.D., Mykkeltveit J.: Weight distributions of some irreducible cyclic codes. DSN Progr. Rep. **16**, 128–131 (1973).
5. Baumert L.D., Mills M.H., Ward R.L.: Uniform cyclotomy. J. Number Theory **14**, 67–82 (1982).
6. Berndt B.C., Evans R.J., Williams K.S.: Gauss and Jacobi sums. A Wiley-Interscience Publication, New York, (1998).
7. 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-Verlag, Berlin (1989).
8. Brouwer A.E., Haemers W.H.: Spectra of graphs, course notes, available at http://homepages.cwi.nl/~aeb/math/ipm.pdf.
9. van Dam E.R.: A characterization of association schemes from affine spaces. Des. Codes Cryptogr. **21**, 83–86 (2000).
10. van Dam E.R.: Strongly regular decompositions of the complete graph. J. Algebraic Combin. **17**, 181–201 (2003).
11. van Dam E., Muzychuk M.: Some implications on amorphic association schemes. J. Combin. Theory (A) **117**, 111–127 (2010).
12. Feng T., Xiang Q.: Strongly regular graphs from union of cyclotomic classes. J. Combin. Theory (B) (in press).
13. Godsil C., Royle G.: Algebraic graph theory, GTM 207, Springer-Verlag, Berlin (2001).

14. Hollmann Henk D.L.: Association schemes, Master Thesis, Eindhoven University of Technology, The Netherlands (1982).
15. Ikuta T., Munemasa A.: Pseudocyclic association schemes and strongly regular graphs. Eur. J. Combin. **31**, 1513–1519 (2010).
16. Ivanov A.A., Praeger C.E.: Problem session at ALCOM-91. Eur. J. Combin **15**, 105–112 (1994).
17. Langevin P.: Calculs de certaines sommes de Gauss. J. Number Theory **63**, 59–64 (1997).
18. Mbodj O.D.: Quadratic Gauss sums. Finite Fields Appl. **4**, 347–361.
19. McEliece R.J.: Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory, pp. 179–196. Math. Centre Tracts, No. 55, Math. Centrum, Amsterdam.
20. Meijer P., van der Vlugt M.: The evaluation of Gauss sums for characters of 2-power order. J. Number Theory **100**, 381–395 (2003).
21. Muzychuk M.E.: V-rings of permutation groups with invariant metric, Ph.D. thesis, Kiev State University (1987).
22. 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).