Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Combinatorial Theory, Series A 113 (2006) 1008–1018
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

Pseudocyclic association schemes arising from the actions of PGL(2, 2^m) and PΓL(2, 2^m)

Henk D.L. Hollmann [a], Qing Xiang [b]

[a] *Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands*
[b] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 24 March 2005

Available online 9 November 2005

In memory of Jack van Lint

Abstract

The action of PGL(2, 2^m) on the set of exterior lines to a nonsingular conic in PG(2, 2^m) affords an association scheme, which was shown to be pseudocyclic in [H.D.L. Hollmann, Association schemes, Master thesis, Eindhoven University of Technology, 1982]. It was further conjectured in [H.D.L. Hollmann, Association schemes, Master thesis, Eindhoven University of Technology, 1982] that the orbital scheme of PΓL(2, 2^m) on the set of exterior lines to a nonsingular conic in PG(2, 2^m) is also pseudocyclic if m is an odd prime. We confirm this conjecture in this paper. As a by-product, we obtain a class of Latin square type strongly regular graphs on nonprime-power number of points.
© 2005 Elsevier Inc. All rights reserved.

Keywords: Association scheme; Conic; Dickcon polynomial; Fusion scheme; Latin square type strongly regular graph; Permutation polynomial; Pseudocyclic association scheme; Strongly regular graph

1. Introduction

Let X be a finite set. A (symmetric) *association scheme* with d classes on X is a partition of $X \times X$ into sets $R_0, R_1, \ldots, R_d$ (called *associate classes* or *relations*) such that

(1) $R_0 = \{(x, x) \mid x \in X\}$ (the diagonal relation),
(2) R_i is symmetric for $i = 1, 2, \ldots, d$,

E-mail addresses: henk.d.l.hollmann@philips.com (H.D.L. Hollmann), xiang@math.udel.edu (Q. Xiang).

0097-3165/$ – see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2005.09.004

(3) for all i, j, k in $\{0, 1, 2, \ldots, d\}$ there is an integer p_{ij}^k such that, for all $(x, y) \in R_k$,

$$\left|\left\{z \in X \mid (x, z) \in R_i \text{ and } (z, y) \in R_j\right\}\right| = p_{ij}^k.$$

We denote such an association scheme by $(X, \{R_i\}_{0 \leqslant i \leqslant d})$. Elements x and y of X are called ith *associates* if $(x, y) \in R_i$. The numbers p_{ij}^k, $0 \leqslant k, i, j \leqslant d$, are called the *intersection parameters* of the scheme. That p_{ii}^0 exists means that there is a constant number of ith associates of any element of X, which is usually denoted by n_i. The numbers $n_0, n_1, \ldots, n_d$ are called the *valencies* (or *degrees*) of the scheme. We have

(1) $n_0 = 1$, $n_0 + n_1 + \cdots + n_d = |X|$,
(2) $p_{0j}^k = \delta_{j,k}$ (Kronecker delta), $p_{ij}^0 = \delta_{i,j} n_j$,
(3) $p_{ij}^k = p_{ji}^k$, $p_{ij}^k n_k = p_{ik}^j n_j$.

For $i \in \{0, 1, \ldots, d\}$, let A_i be the adjacency matrix of the relation R_i, that is, the rows and columns of A_i are both indexed by X and

$$(A_i)_{xy} := \begin{cases} 1, & \text{if } (x, y) \in R_i, \\ 0, & \text{if } (x, y) \notin R_i. \end{cases}$$

The matrices A_i are symmetric $(0, 1)$-matrices and

$$A_0 = I, \qquad A_0 + A_1 + \cdots + A_d = J,$$

where J is the all one matrix of size $|X|$ by $|X|$.

By the definition of an association scheme, we have

$$A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$$

for any $i, j \in \{0, 1, \ldots, d\}$. So $A_0, A_1, \ldots, A_d$ form a basis of the commutative algebra generated by $A_0, A_1, \ldots, A_d$ over the reals (which is called the *Bose–Mesner algebra* of the association scheme, see [2, p. 45]). Moreover this algebra has a unique basis $E_0, E_1, \ldots, E_d$ of primitive idempotents; one of the primitive idempotents is $\frac{1}{|X|} J$. So we may assume that $E_0 = \frac{1}{|X|} J$. Let $m_i = \operatorname{rank} E_i$. Then

$$m_0 = 1, \qquad m_0 + m_1 + \cdots + m_d = |X|.$$

The numbers $m_0, m_1, \ldots, m_d$ are called the *multiplicities* of the scheme. Since we have two bases of the Bose–Mesner algebra, we may consider the transition matrices between them. Define $P = (p_j(i))_{0 \leqslant i, j \leqslant d}$ (the *first eigenmatrix*) and $Q = (q_j(i))_{0 \leqslant i, j \leqslant d}$ (the *second eigenmatrix*) as the $(d + 1) \times (d + 1)$ matrices with rows and columns indexed by $0, 1, 2, \ldots, d$ such that

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

and

$$|X|(E_0, E_1, \ldots, E_d) = (A_0, A_1, \ldots, A_d) Q.$$

Of course, we have

$$P = |X| Q^{-1}, \qquad Q = |X| P^{-1}.$$

Note that $\{p_j(i) \mid 0 \leqslant i \leqslant d\}$ is the set of eigenvalues of A_j and the zeroth row and column of P and Q are as indicated below:

$$P = \begin{pmatrix} 1 & n_1 & \cdots & n_d \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & m_1 & \cdots & m_d \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix}.$$

Before we proceed further, we give some examples of association schemes.

Example 1.1. Let X be a finite set and let G be a group acting transitively on X. We say that G acts *generously transitively* on X if the orbits of the induced action of G on $X \times X$ are all symmetric. (The orbits of G on $X \times X$ are usually called the *orbitals* of the action of G on X.) It is clear that if G acts generously transitively on X, then the orbitals of G on X can be taken as the relations of an association scheme, which will be called the *orbital scheme* of G on X. The next example arises in this way.

Example 1.2. We consider *cyclotomic schemes* defined as follows. Let q be a prime power and let $q - 1 = ef$ with $e > 1$. Let C_0 be the subgroup of the multiplicative group of $\mathbf{F}_q$ of index e, and let $C_0, C_1, \ldots, C_{e-1}$ be the cosets of C_0. We require $-1 \in C_0$. Define $R_0 = \{(x, x) \mid x \in \mathbf{F}_q\}$, and for $i \in \{1, 2, \ldots, e\}$, define $R_i = \{(x, y) \mid x, y \in \mathbf{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbf{F}_q, \{R_i\}_{0 \leqslant i \leqslant e})$ is an e-class symmetric association scheme (the R_i are the orbitals of the action of G on $\mathbf{F}_q$, where $G = \{x \mapsto ax + b \mid a \in C_0, b \in \mathbf{F}_q\}$). The intersection parameters of the cyclotomic scheme are related to the cyclotomic numbers [12, p. 25]. Namely, for $i, j, k \in \{1, 2, \ldots, e\}$, given $(x, y) \in R_k$,

$$p_{ij}^k = \big|\{z \in \mathbf{F}_q \mid x - z \in C_{i-1}, y - z \in C_{j-1}\}\big| = \big|\{z \in C_{i-k} \mid 1 + z \in C_{j-k}\}\big|. \tag{1}$$

The first eigenmatrix P of this scheme is the following $(e + 1)$ by $(e + 1)$ matrix (with the rows of P arranged in a certain way)

$$P = \begin{pmatrix} 1 & f & \cdots & f \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

with $P_0 = \sum_{i=1}^{e} \eta_i C^i$, where C is the e by e matrix:

$$C = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}$$

and $\eta_i = \sum_{\beta \in C_i} \psi(\beta)$, $1 \leqslant i \leqslant e$, for a fixed nontrivial additive character ψ of $\mathbf{F}_q$. See [1] for more details.

Next we introduce the notion of a pseudocyclic association scheme.

Definition 1.3. Let $(X, \{R_i\}_{0 \leqslant i \leqslant d})$ be an association scheme. We say that $(X, \{R_i\}_{0 \leqslant i \leqslant d})$ is *pseudocyclic* if there exists an integer t such that $m_i = t$ for all $i \in \{1, \ldots, d\}$.

The following theorem gives combinatorial characterizations for an association scheme to be pseudocyclic.

Theorem 1.4. *Let $(X, \{R_i\}_{0\leqslant i\leqslant d})$ be an association scheme, and for $x \in X$ and $1 \leqslant i \leqslant d$, let $R_i(x) = \{y \mid (x, y) \in R_i\}$. Then the following are equivalent*:

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

For a proof of this theorem, we refer the reader to [2, p. 48] and [6, p. 84]. Part (2) in the above theorem is very useful. For example, we may use it to prove that the cyclotomic scheme in Example 1.2 is pseudocyclic. The proof goes as follows. First, the nontrivial valencies of the cyclotomic scheme in Example 1.2 are all equal to f. Second, by (1) and noting that $-1 \in C_0$, we have

$$\sum_{k=1}^{e} p_{kj}^k = \sum_{k=1}^{e} \big|\{z \in C_0 \mid 1 + z \in C_{j-k}\}\big| = |C_0| - 1 = f - 1.$$

Pseudocyclic schemes can be used to construct strongly regular graphs and distance regular graphs of diameter 3 [3], [2, p. 388]. In view of this, it is of interest to construct pseudocyclic association schemes, as remarked by the authors of [2] (see [2, p. 389]). The cyclotomic schemes are examples of pseudocyclic association schemes on prime-power number of points. Very few examples of pseudocyclic association schemes on nonprime-power number of points are currently known (see [11], [2, p. 390] and [6]). One class of such examples comes from the action of $\mathrm{PGL}(2, 2^m)$ on the set of exterior lines to a nonsingular conic in $\mathrm{PG}(2, 2^m)$. We will give a quick review of this class of association schemes in Section 2, and also include a proof of the pseudocyclicity of these association schemes. In [6], it was further conjectured that the orbital scheme of $\mathrm{P\Gamma L}(2, 2^m)$ on the set of exterior lines to a nonsingular conic in $\mathrm{PG}(2, 2^m)$ is also pseudocyclic if m is an odd prime. We will confirm this conjecture in Section 3. As a by-product, we obtain a class of Latin square type strongly regular graphs on nonprime-power number of points.

2. The elliptic schemes

In the rest of this paper, we always assume that $q = 2^m$, where m is a positive integer. Let

$$\mathcal{O} = \big\{\big(\xi, \xi^2, 1\big) \mid \xi \in \mathbf{F}_q\big\} \cup \big\{(0, 1, 0)\big\}.$$

Then $\mathcal{O}$ is a nonsingular conic in $\mathrm{PG}(2, q)$. A line of $\mathrm{PG}(2, q)$ is called *exterior* (respectively *secant*) if it meets $\mathcal{O}$ in 0 (respectively 2) points. Let $\mathcal{E}$ (respectively $\mathcal{H}$) be the set of exterior (respectively secant) lines to $\mathcal{O}$. Then

$$|\mathcal{E}| = \frac{q(q-1)}{2} \quad \text{and} \quad |\mathcal{H}| = \frac{(q+1)q}{2}.$$

The subgroup of $\mathrm{PGL}(3, q)$ fixing $\mathcal{O}$ setwise is isomorphic to $\mathrm{PGL}(2, q)$ (cf. [5, p. 158]). Hence $\mathrm{PGL}(2, q)$ acts on $\mathcal{E}$ and $\mathcal{H}$, respectively. Moreover, it is shown in [8] that $\mathrm{PGL}(2, q)$ acts generously transitively on both $\mathcal{E}$ and $\mathcal{H}$. Therefore we obtain two association schemes, one on $\mathcal{E}$

and the other on $\mathcal{H}$. The association scheme on $\mathcal{E}$ will be called the *elliptic* scheme, and the association scheme on $\mathcal{H}$ is called the *hyperbolic* scheme.

Since the point $(1,0,0)$ is the nucleus of $\mathcal{O}$ (i.e., the point at which all tangent lines to $\mathcal{O}$ meet), we see that each line in $\mathcal{E}\cup\mathcal{H}$ can be written as $(1,x,y)^{\perp}=\{(a_0,a_1,a_2)\in\mathbf{F}_q^3 \mid a_0+a_1x+a_2y=0\}$ for some $x,y\in\mathbf{F}_q$. Let $\mathrm{Tr}:\mathbf{F}_q\to\mathbf{F}_2$ be the trace map. Also for $e\in\mathbf{F}_2$ we define

$$\mathbf{T}_e=\{x\in\mathbf{F}_q \mid \mathrm{Tr}(x)=e\},$$

and $\mathbf{T}_e^*=\mathbf{T}_e\setminus\{0\}$. Then $(1,x,y)^{\perp}$ is in $\mathcal{E}$ (respectively $\mathcal{H}$) if and only if $\mathrm{Tr}(xy)=1$ (respectively $\mathrm{Tr}(xy)=0$). Given two lines $\ell=(1,x,y)^{\perp}$ and $m=(1,z,u)^{\perp}$, we define

$$\hat{\rho}(\ell,m)=x^2u^2+y^2z^2+(x+z)(y+u).$$

We remark that the function $\hat{\rho}$ comes from the cross-ratio of four points on a projective line (see [8] for details). The following theorem in [8] gives a simple description of the orbitals of the action of $\mathrm{PGL}(2,q)$ on $\mathcal{E}$ by using the function $\hat{\rho}$.

Theorem 2.1. *The orbitals of the action of* $\mathrm{PGL}(2,q)$ *on* $\mathcal{E}$ *are* Γ_0 *(the diagonal class), and* $\Gamma_a=\{(\ell,m) \mid \hat{\rho}(\ell,m)=a\}$ *for all* $a\in\mathbf{T}_0^*$.

There is a similar description of the orbitals of $\mathrm{PGL}(2,q)$ on $\mathcal{H}$ in [8]. Since we are only concerned with the elliptic scheme in this paper, we omit that description.

The pair $(\mathcal{E},\{\Gamma_a\})$ is an association scheme on $\mathcal{E}$ with $\frac{(q-2)}{2}$ classes. The intersection parameters of this scheme are computed in [8]. For $a,b,c\in\mathbf{T}_0^*$, given $(\ell,m)\in\Gamma_c$, we use $p_{a,b}^c$ to denote $|\{k\in\mathcal{E} \mid (\ell,k)\in\Gamma_a \text{ and } (k,m)\in\Gamma_c\}|$. We have:

Theorem 2.2. *Let* $a,b,c\in\mathbf{T}_0^*$. *Then for any* $v\in\mathbf{T}_1$,

$$p_{a,b}^c=\begin{cases}1+2\delta_{\mathrm{Tr}(ac),1}, & \text{if } a+b+c=0;\\ \sum_{\tau}|\{z\in\mathbf{F}_q \mid z^2+z=v+ac/\tau^2\}|, & \text{otherwise},\end{cases}\tag{2}$$

where the last sum is over the two elements $\tau\in\mathbf{F}_q$ *satisfying* $\tau^2+\tau=a+b+c$. *Also for all* $a\in\mathbf{T}_0^*$, *the valency* $n_a=q+1$.

The association scheme $(\mathcal{E},\{\Gamma_a\})$ is pseudocyclic. This is already known in [6]. For convenience of the reader, we include a proof here.

Theorem 2.3. *The association scheme* $(\mathcal{E},\{\Gamma_a\})$ *is pseudocyclic.*

Proof. By Theorem 2.2, the nontrivial valencies of the association scheme $(\mathcal{E},\{\Gamma_a\})$ are all equal to $q+1$. By part (2) of Theorem 1.4, it suffices to prove that $\sum_{a\in\mathbf{T}_0^*}p_{a,b}^a=q$ for all $b\in\mathbf{T}_0^*$.

By Theorem 2.2, for $a,b\in\mathbf{T}_0^*$, we have

$$p_{a,b}^a=\sum_{\tau^2+\tau=b}\left(1-(-1)^{\mathrm{Tr}(a/\tau)}\right).$$

Fixing $\tau\in\mathbf{F}_q\setminus\{0,1\}$ with $\tau^2+\tau=b$, we have

$$\sum_{a\in\mathbf{T}_0^*}p_{a,b}^a=\sum_{a\in\mathbf{T}_0^*}\left(1-(-1)^{\mathrm{Tr}(a/\tau)}+1-(-1)^{\mathrm{Tr}(a/(\tau+1))}\right)$$

$$= 2(q/2-1) - \sum_{a\in\mathbf{T}_0^*} \left((-1)^{\mathrm{Tr}(a/\tau)} + (-1)^{\mathrm{Tr}(a/(\tau+1))}\right)$$
$$= 2(q/2-1) - (-1-1) = q.$$

This completes the proof. □

3. Pseudocyclic fusion schemes of the elliptic schemes

As we have seen in the last section, the elliptic scheme $(\mathcal{E}, \{\Gamma_a\})$ is pseudocyclic. In this section, we will consider the fusion scheme of $(\mathcal{E}, \{\Gamma_a\})$ obtained by merging the classes Γ_a via the Frobenius automorphism $x \mapsto x^2$ of $\mathbf{F}_q$. Specifically, for $a \in \mathbf{T}_0^*$, define

$$\Delta_a = \bigcup_{i\in C_a} \Gamma_i,$$

where $C_a := \{a, a^2, a^4, \ldots, a^{2^{m-1}}\}$. Let $\mathcal{R}$ be a set of orbit representatives of $\mathbf{T}_0^*$ under the action of the Frobenius automorphism. Then $\Delta_0 := \Gamma_0$, and Δ_a, $a \in \mathcal{R}$ are the orbitals of $\mathrm{P\Gamma L}(2, q)$ on $\mathcal{E}$. Therefore $(\mathcal{E}, \{\Delta_a\})$ is also an association scheme. The (nontrivial) intersection parameters of this fusion scheme will be denoted by $P_{a,b}^c$, where $a, b, c \in \mathcal{R}$. We have for $a, b, c \in \mathcal{R}$,

$$P_{a,b}^c = \sum_{e\in C_a} \sum_{f\in C_b} p_{e,f}^g,$$

where $g \in C_c$. (This is independent of the choice of $g \in C_c$.)

Now, if m is prime, then each C_a, $a \in \mathcal{R}$, has size m, so the nontrivial valencies of the fusion scheme $(\mathcal{E}, \{\Delta_a\})$ are all equal to $m(q+1)$. Hollmann [6, p. 133] made the following conjecture.

Conjecture 3.1. *If m is an odd prime, then $(\mathcal{E}, \{\Delta_a\})$ is pseudocyclic.*

As far as we know, there is no published proof of this conjecture. There is one sentence in [2, p. 390] stating the above conjecture as a fact. But this was not backed up by a proof.

Note that the nontrivial valencies of $(\mathcal{E}, \{\Delta_a\})$ are all equal to $m(q+1)$ when m is prime. So in order to prove Conjecture 3.1, by part (2) of Theorem 1.4, we need to show that

$$\sum_{c\in\mathcal{R}} P_{c,c}^b = m(q+1) - 1, \tag{3}$$

for all $b \in \mathcal{R}$. (Here we implicitly used the fact that $P_{c,c}^b = P_{c,b}^c$ since all nontrivial valencies are equal when m is prime.) Simplifying the left-hand side of (3), we see that (3) is equivalent to

$$\sum_{k=0}^{m-1} \sum_{c\in\mathbf{T}_0^*} p_{c,c^{2^k}}^b = m(q+1) - 1. \tag{4}$$

Now, the $k = 0$ term of the left-hand side of (4) is equal to q as seen in the proof of Theorem 2.3. So in order to prove (4), we have to show that

$$\sum_{k=1}^{m-1} \sum_{c\in\mathbf{T}_0^*} p_{c,c^{2^k}}^b = (m-1)(q+1), \tag{5}$$

for all $b \in \mathbf{T}_0^*$.

We will prove a stronger result:

Theorem 3.2. *Let m be an odd integer, and let k be any integer in $\{1, 2, \ldots, m-1\}$ satisfying $\gcd(k, m) = 1$. Write $\sigma = 2^k$. Then*

$$\sum_{c \in \mathbf{T}_0^*} p_{c,c^\sigma}^b = q + 1, \quad \text{for all } b \in \mathbf{T}_0^*. \tag{6}$$

The most important ingredient in our proof of Theorem 3.2 is a family of polynomials $H_{\alpha,\gamma}(X)$ introduced in [7]. In fact we discovered these polynomials while working on a proof of Theorem 3.2. We now define the polynomials $H_{\alpha,\gamma}(X)$ and quote the main theorem from [7].

Let $m \geqslant 1$ be an integer, let k be any integer in $\{1, \ldots, m-1\}$ with $\gcd(k, m) = 1$, and let $r \in \{1, \ldots, m-1\}$ be such that $kr \equiv 1 \pmod m$. Write $\sigma = 2^k$ and use $\mathrm{Tr}(X)$ to denote the following polynomial in $\mathbf{F}_2[X]$:

$$\mathrm{Tr}(X) := X + X^2 + \cdots + X^{2^{m-1}}.$$

For α, γ in $\{0, 1\}$, we define the polynomial

$$H_{\alpha,\gamma}(X) := \gamma \,\mathrm{Tr}(X) + \frac{(\alpha \,\mathrm{Tr}(X) + \sum_{i=0}^{r-1} X^{\sigma^i})^{\sigma+1}}{X^2}.$$

(Note that $H_{\alpha,\gamma}(X)$ is indeed a polynomial in X with coefficients in $\mathbf{F}_2$ and $H_{\alpha,\gamma}(0) = 0$. Also see [7] for connections between $H_{\alpha,\gamma}(X)$ and the Dickson polynomials.)

The following is the main theorem from [7].

Theorem 3.3. *Let m, k be positive integers with $\gcd(k, m) = 1$, let $r \in \{1, \ldots, m-1\}$ be such that $kr \equiv 1 \pmod m$, and let $\alpha, \gamma \in \{0, 1\}$. Then the mapping $H_{\alpha,\gamma} : x \mapsto H_{\alpha,\gamma}(x)$, $x \in \mathbf{F}_q$, maps $\mathbf{T}_0$ bijectively to $\mathbf{T}_0$, and maps $\mathbf{T}_1$ bijectively to $\mathbf{T}_{r+(\alpha+\gamma)m}$. In particular, the polynomial $H_{\alpha,\gamma}(X)$ is a permutation polynomial of $\mathbf{F}_q$ if and only if $r + (\alpha + \gamma)m \equiv 1 \pmod 2$.*

We are now ready to give the proof of Theorem 3.2.

Proof of Theorem 3.2. Recall that from Theorem 2.2, for $b, c \in \mathbf{T}_0^*$,

$$p_{c,c^\sigma}^b = \begin{cases} 1 + 2\delta_{\mathrm{Tr}(bc),1}, & \text{if } c^\sigma + c + b = 0; \\ \sum_{\tau^2+\tau=c^\sigma+c+b} |\{z \in \mathbf{F}_q \mid z^2 + z = v + bc/\tau^2\}|, & \text{if } c^\sigma + c + b \neq 0, \end{cases}$$

where v is any element with $\mathrm{Tr}(v) = 1$. Since $b \in \mathbf{T}_0^*$ and m is odd, we can find a unique $c_0 \in \mathbf{T}_0^*$ such that $c_0^\sigma + c_0 = b$. So

$$\begin{aligned} \sum_{c \in \mathbf{T}_0^*} p_{c,c^\sigma}^b &= 1 + 2\delta_{\mathrm{Tr}(bc_0),1} + 2 \sum_{c \in \mathbf{T}_0^*,\, c^\sigma+c+b \neq 0} \sum_{\tau^2+\tau=c^\sigma+c+b} \delta_{\mathrm{Tr}(bc/\tau^2),1} \\ &= 1 + 2\big|\big\{(c, \tau) \in \mathbf{F}_q^* \times \mathbf{F}_q^* \mid \tau^2 + \tau = c^\sigma + c + b,\ \mathrm{Tr}(c) = 0, \mathrm{Tr}\big(bc/\tau^2\big) = 1\big\}\big|. \end{aligned}$$

For convenience, we define

$$N_k(b) := \big|\big\{(c, \tau) \in \mathbf{F}_q^* \times \mathbf{F}_q^* \mid \tau^2 + \tau = c^\sigma + c + b,\ \mathrm{Tr}(c) = 0,\ \mathrm{Tr}\big(bc/\tau^2\big) = 1\big\}\big|.$$

Our goal is to prove that $N_k(b) = q/2$ for all $b \in \mathbf{T}_0^*$.

For later use, we define the polynomial

$$f(X) := \sum_{i=0}^{r-1} X^{\sigma^i} \in \mathbf{F}_2[X],$$

where r is an integer satisfying $kr \equiv 1 \pmod m$.

Since $b \in \mathbf{T}_0^*$ and m is odd, we can write $b = \beta + \beta^2$ with $\beta \in \mathbf{T}_0^*$. Then the equation $\tau^2 + \tau = c^\sigma + c + b$ involved in the definition of $N_k(b)$ becomes

$$c^\sigma + c = (\beta + \tau) + (\beta + \tau)^2. \tag{7}$$

Noting that m is odd, we see that for any $\tau \in \mathbf{F}_q$, there is a unique solution $c \in \mathbf{T}_0$ of (7), namely

$$c = f(\tau + \beta) + r\,\mathrm{Tr}(\tau + \beta) = f(\tau + \beta) + r\,\mathrm{Tr}(\tau),$$

where in the last equality we used the fact that $\beta \in \mathbf{T}_0$. Therefore we have

$$N_k(b) = \begin{cases} |\{\tau \in \mathbf{F}_q^* \mid \frac{b(f(\tau+\beta)+\mathrm{Tr}(\tau))}{\tau^2} \in \mathbf{T}_1\}|, & \text{if } r \text{ is odd;} \\ |\{\tau \in \mathbf{F}_q^* \mid \frac{bf(\tau+\beta)}{\tau^2} \in \mathbf{T}_1\}|, & \text{if } r \text{ is even.} \end{cases}$$

We will consider the r odd case and the r even case separately.

Case 1. r is odd. Let $x = b/\tau^2$, where $b = \beta + \beta^2 \in \mathbf{T}_0^*$ and $\tau \in \mathbf{F}_q^*$. Then

$$\begin{aligned} \mathrm{Tr}\left(\frac{b(f(\tau+\beta)+\mathrm{Tr}(\tau))}{\tau^2}\right) &= \mathrm{Tr}\left(x\sum_{i=0}^{r-1}\big(\beta + \sqrt{b/x}\big)^{\sigma^i} + x\,\mathrm{Tr}(b/x)\right) \\ &= \mathrm{Tr}\left(\sum_{i=0}^{r-1} x^2\big(\beta^2 + b/x\big)^{\sigma^i}\right) + \mathrm{Tr}(x)\,\mathrm{Tr}(b/x) \\ &= \mathrm{Tr}\left(\sum_{i=0}^{r-1} x^{\sigma^{r-i}}\big(\beta^2 + b/x\big)\right) + \mathrm{Tr}(x)\,\mathrm{Tr}(b/x) \\ &= \mathrm{Tr}\big(\big(\beta^2 + b/x\big)\big(f(x) + x^2 + x\big)\big) + \mathrm{Tr}(x)\,\mathrm{Tr}(b/x) \\ &= \mathrm{Tr}\left(\beta^2\left(f(x) + \frac{f(x)}{x} + \frac{f(x)^2}{x^2}\right)\right) + \mathrm{Tr}(x)\,\mathrm{Tr}(b/x), \end{aligned}$$

where in the last step, we used $b = \beta + \beta^2$. Now noting that for $x \in \mathbf{F}_q^*$,

$$H_{0,0}(x) = f(x) + \frac{f(x)}{x} + \frac{f(x)^2}{x^2}.$$

(One can prove this directly, or see [7, Lemma 3.1].) Therefore, in this case, we have

$$N_k(b) = \big|\big\{x \in \mathbf{T}_0^* \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| + \big|\big\{x \in \mathbf{T}_1 \mid \beta^2 H_{0,0}(x) + b/x \in \mathbf{T}_1\big\}\big|. \tag{8}$$

For the first summand in (8), noting that $H_{0,0}(0) = 0$ and $H_{0,0}$ maps $\mathbf{T}_0$ to $\mathbf{T}_0$ bijectively (Theorem 3.3), we have

$$\big|\big\{x \in \mathbf{T}_0^* \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| = \big|\beta^2\mathbf{T}_0^* \cap \mathbf{T}_1\big| = (q/2 - 1) - \big|\beta^2\mathbf{T}_0^* \cap \mathbf{T}_0^*\big|.$$

Since $\mathbf{T}_0^*$ is a $(q-1, q/2-1, q/4-1)$ Singer difference set in the cyclic group $\mathbf{F}_q^*$ (see [9, p. 378]), and $\beta \neq 0, 1$, we see that $|\beta^2\mathbf{T}_0^* \cap \mathbf{T}_0^*| = q/4 - 1$. Hence

$$\big|\big\{x \in \mathbf{T}_0^* \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| = (q/2 - 1) - (q/4 - 1) = q/4.$$

For the second summand in (8), using $b = \beta + \beta^2$, we see that

$$\mathrm{Tr}\big(\beta^2 H_{0,0}(x) + b/x\big) = \mathrm{Tr}\big(\beta^2\big(H_{0,0}(x) + 1/x + 1/x^2\big)\big).$$

For any $x \in \mathbf{T}_1$, we have

$$\begin{aligned} H_{1,0}(x) &= \frac{(1+f(x))^{\sigma+1}}{x^2} = 1 + f(x) + \big(1+f(x)\big)/x + \big(1+f(x)\big)^2/x^2 \\ &= 1 + 1/x + 1/x^2 + H_{0,0}(x). \end{aligned}$$

Also by Theorem 3.3, $H_{1,0}$ maps $\mathbf{T}_1$ bijectively to $\mathbf{T}_{r+m} = \mathbf{T}_0$. Hence

$$\begin{aligned} \big|\big\{x \in \mathbf{T}_1 \mid \beta^2 H_{0,0}(x) + b/x \in \mathbf{T}_1\big\}\big| &= \big|\big\{x \in \mathbf{T}_1 \mid \beta^2\big(H_{0,0}(x) + 1/x + 1/x^2\big) \in \mathbf{T}_1\big\}\big| \\ &= \big|\beta^2 \mathbf{T}_1 \cap \mathbf{T}_1\big| = q/4. \end{aligned}$$

Therefore we have $N_k(b) = q/4 + q/4 = q/2$.

Case 2. r is even. This case is similar to Case 1 and actually easier. Let $x = b/\tau^2$. By the same computations as those in the r odd case, we find that

$$\mathrm{Tr}\left(\frac{bf(\tau+\beta)}{\tau^2}\right) = \mathrm{Tr}\big(\beta^2 H_{0,0}(x)\big).$$

By Theorem 3.3, $H_{0,0}$ maps $\mathbf{T}_0^*$ bijectively to $\mathbf{T}_0^*$, and maps $\mathbf{T}_1$ bijectively to $\mathbf{T}_r = \mathbf{T}_0$. Therefore,

$$\begin{aligned} &\left|\left\{\tau \in \mathbf{F}_q^* \;\middle|\; \frac{bf(\tau+\beta)}{\tau^2} \in \mathbf{T}_1\right\}\right| \\ &\quad = \big|\big\{x \in \mathbf{F}_q^* \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| \\ &\quad = \big|\big\{x \in \mathbf{T}_0^* \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| + \big|\big\{x \in \mathbf{T}_1 \mid \beta^2 H_{0,0}(x) \in \mathbf{T}_1\big\}\big| \\ &\quad = \big|\beta^2 \mathbf{T}_0^* \cap \mathbf{T}_1\big| + \big|\beta^2 \mathbf{T}_0 \cap \mathbf{T}_1\big| = 2\big|\beta^2 \mathbf{T}_0^* \cap \mathbf{T}_1\big| = q/2. \end{aligned}$$

In summary, in both cases, we have shown that $N_k(b) = q/2$ for all $b \in \mathbf{T}_0^*$. The proof is complete. □

Remark 3.4. More general results can be proved in the same fashion as above. Let $e, f \in \mathbf{F}_2$. Define

$$N_{k,e,f}(b) := \big|\big\{(c,\tau) \in \mathbf{F}_q^* \times \mathbf{F}_q^* \mid \tau^2 + \tau = c^\sigma + c + b,\ \mathrm{Tr}(c) = e,\ \mathrm{Tr}\big(bc/\tau^2\big) = f\big\}\big|.$$

Then using the same arguments as those in the proof of Theorem 3.2, we find that

$$N_{k,0,0}(b) = q/2 - 3, \qquad N_{k,1,0}(b) = q/2 - 1, \quad \text{and} \quad N_{k,1,1}(b) = q/2,$$

for all $b \in \mathbf{T}_0^*$.

Now we can finish the proof of Conjecture 3.1.

Theorem 3.5. *If m is an odd prime, then $(\mathcal{E}, \{\Delta_a\})$ is pseudocyclic.*

Proof. Since m is prime, the nontrivial valencies of the scheme are all equal to $m(q+1)$. To finish the proof, we need to prove (3) for all $b \in \mathcal{R}$. As we have seen in the analysis before the statement of Theorem 3.2, (3) is equivalent to (5). Since m is an odd prime, any integer $k \in \{1, 2, \ldots, m-1\}$ is relatively prime to m. So we can apply Theorem 3.2 to obtain

$$\sum_{c\in\mathbf{T}_0^*} p_{c,c^\sigma}^b = q+1,$$

for all $b \in \mathbf{T}_0^*$. Now (5) follows. This completes the proof. □

4. Latin square type strongly regular graphs

A *strongly regular graph srg* (v,k,λ,μ) is a graph with v vertices that is regular of valency k and that has the following properties:

(1) For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.
(2) For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

It is well known [9, p. 407] that strongly regular graphs are equivalent to two-class association schemes. An srg (v,k,λ,μ) is said to be of *Latin square type* if

$$(v,k,\lambda,\mu) = \big(n^2, t(n-1), n+t^2-3t, t^2-t\big),$$

where $1 \leqslant t \leqslant n+1$. Any Latin square of order n gives rise to a Latin square type srg (actually called Latin square graph in this case) with parameters $(n^2, 3(n-1), n-2, 6)$ (see [9, p. 273]). Many examples of Latin square type srg on prime-power number of points are known [10]. In contrast, not too many examples of Latin square type srg on nonprime-power number of points are known.

In [3], it was shown that pseudocyclic association schemes can give rise to Latin square type srg. We quote the following theorem from [3]. A proof can be found in [4].

Theorem 4.1. *Let $(X, \{R_i\}_{0\leqslant i\leqslant d})$ be a pseudocyclic association scheme on $dt+1$ points. Then the graph G whose vertex set is $X\times X$, and where two distinct vertices (x,y) and (x',y') are adjacent if and only if $(x,x') \in R_i$ and $(y,y') \in R_i$ for some $i \neq 0$, is a Latin square type srg with parameters*

$$\big(|X|^2, t\big(|X|-1\big), |X|+t^2-3t, t^2-t\big).$$

Using Theorem 4.1, one can obtain Latin square type srg from the pseudocyclic association scheme $(\mathcal{E}, \{\Gamma_a\})$ (the elliptic scheme). These srg have parameters

$$\left(\frac{1}{4}q^2(q-1)^2, \frac{1}{2}(q-2)(q+1)^2, \frac{1}{2}\big(3q^2-3q-4\big), q(q+1)\right).$$

We note that the Latin square type srg arising from $(\mathcal{E}, \{\Gamma_a\})$ were mentioned in [4], in which another construction of these srg was given.

Now since we have shown that the fusion scheme $(\mathcal{E}, \{\Delta_a\})$ of the elliptic scheme $(\mathcal{E}, \{\Gamma_a\})$ is also pseudocyclic when m is an odd prime. We obtain more Latin square type srg via Theorem 4.1.

Theorem 4.2. *Let $q = 2^m$, where m is an odd prime. Then there exists a Latin square type srg with parameters*

$$\left(\frac{1}{4}q^2(q-1)^2, \frac{1}{2}m(q-2)(q+1)^2, \lambda, \mu\right),$$

where $\lambda = \frac{q(q-1)}{2} + m^2(q+1)^2 - 3m(q+1)$ and $\mu = m^2(q+1)^2 - m(q+1)$.

Proof. Straightforward. □

Acknowledgments

The second author thanks Philips Research Eindhoven, the Netherlands, where part of this work was carried out. The research of the second author is supported in part by NSF grant DMS 0400411.

References

[1] E. Bannai, A. Munemasa, Davenport–Hasse theorem and cyclotomic schemes, unpublished notes.
[2] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance Regular Graphs, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 18, Springer, Berlin, 1989.
[3] A.E. Brouwer, R. Mathon, unpublised notes.
[4] T. Fujisaki, A four-class association scheme derived from a hyperbolic quadric in PG$(3, q)$, Adv. Geom. 4 (2004) 105–117.
[5] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second ed., Oxford Math. Monogr., Clarendon Press/Oxford Univ. Press, New York, 1998.
[6] H.D.L. Hollmann, Association schemes, Master thesis, Eindhoven University of Technology, 1982.
[7] H.D.L. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbf{F}_{2^m}$ related to Dickson polynomials, Finite Fields Appl. 11 (2005) 111–122.
[8] H.D.L. Hollmann, Q. Xiang, Association schemes arising from the action of PGL$(2, q)$ fixing a nonsingular conic in PG$(2, q)$, J. Algebraic Combin., in press.
[9] J. van Lint, R.M. Wilson, A Course in Combinatorics, second ed., Cambridge Univ. Press, Cambridge, 2001.
[10] S.L. Ma, A survey of partial difference sets, Des. Codes Cryptogr. 4 (1994) 221–261.
[11] R. Mathon, 3-class association schemes, in: Proceedings of the Conference on Algebraic Aspects of Combinatorics, Univ. Toronto, Toronto, ON, 1975, in: Congr. Numer., vol. XIII, Utilitas Math., Winnipeg, MB, 1975, pp. 123–155.
[12] T. Storer, Cyclotomy and Difference Sets, Lectures in Adv. Math., vol. 2, Markham Publishing, Chicago, IL, 1967.