TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 362, Number 6, June 2010, Pages 3203–3221
S 0002-9947(10)04864-6
Article electronically published on January 7, 2010

PRIMITIVE BICIRCULANT ASSOCIATION SCHEMES AND A GENERALIZATION OF WIELANDT'S THEOREM

I. KOVÁCS, D. MARUŠIČ, AND M. MUZYCHUK

Abstract. Bannai and Ito defined association scheme theory as doing "group theory without groups", thus raising a basic question as to which results about permutation groups are, in fact, results about association schemes. By considering transitive permutation groups in a wider setting of association schemes, it is shown in this paper that one such result is the classical theorem of Wielandt about primitive permutation groups of degree $2p$, p a prime, being of rank at most 3 (see *Math. Z.* **63** (1956), 478–485). More precisely, it is proved here that if $\mathfrak{X}$ is a primitive bicirculant association scheme of order $2p^e$, $p > 2$ is a prime, then $\mathfrak{X}$ is of class at most 2, and if it is of class exactly 2, then $2p^e = (2s+1)^2 + 1$ for some natural number s, with the valencies of $\mathfrak{X}$ being 1, $s(2s+1)$, $(s+1)(2s+1)$, and the multiplicities of $\mathfrak{X}$ being 1, p^e, $p^e - 1$. Consequently, translated into permutation group theory language, a primitive permutation group G of degree $2p^e$, p a prime and $e \geq 1$, containing a cyclic subgroup with two orbits of size p^e, is either doubly transitive or of rank 3, in which case $2p^e = (2s+1)^2+1$ for some natural number s, the sizes of suborbits of G are 1, $s(2s+1)$ and $(s+1)(2s+1)$, and the degrees of the irreducible constituents of G are 1, p^e and $p^e - 1$.

1. Introductory and historic remarks

Making essential use of the theory of representations and group characters, Wielandt [23] proved that a primitive permutation group G of degree $2p$, p a prime, is either doubly transitive or of rank 3. In the latter case, $2p = (2s+1)^2+1$ for some natural number s, the sizes of suborbits of G are 1, $s(2s+1)$ and $(s+1)(2s+1)$, and the degrees of the irreducible constituents of G are 1, p and $p-1$.

Despite the fact that, in the decades following Wielandt's result, considerable efforts had gone towards a more detailed description (and possible classification) of rank 3 groups of degree $2p$ (see [7, 8, 9, 18, 19]), the problem remained unresolved until the classification of simple groups was completed. It is now known that A_5 and S_5, in their simply transitive actions on unordered pairs of elements from a 5-element set, are the only rank 3 primitive groups of degree $2p$, p a prime. It would definitely be worthwhile to find a "classification of simple groups free" proof of this fact.

Wielandt's result is naturally linked to an old question of Burnside regarding B-groups. A group H is called a *B-group* if a primitive permutation group containing H as a regular subgroup is necessarily doubly transitive. As a generalization let us call H an *m-B-group* if a primitive permutation group containing H as a semiregular

Received by the editors May 22, 2007 and, in revised form, June 26, 2008.
2000 *Mathematics Subject Classification.* Primary 05E30.

subgroup with m orbits (of equal size) is necessarily doubly transitive. The following problem is then an obvious generalization of Burnside's question about B-groups: given a positive integer m, determine the class of m-B-groups. Of course, a 1-B-group is just a B-group. It is known for example that, by the classical results of Schur and Wielandt [22, Theorems 25.3 and 25.6], cyclic groups of composite order and dihedral groups are B-groups. As for 2-B-groups, for example, in view of the above comments, cyclic groups of prime order $p > 5$ are of this kind. In this context, determining which cyclic groups are 2-B-groups then seems like a natural question to pursue.

In this article we generalize Wielandt's theorem to primitive permutation groups of degree $2p^e$, p a prime and $e \geq 1$, which have a cyclic subgroup with two orbits of size p^e, thus making a first step towards a possible determination of cyclic 2-B-groups of prime power order. We do so by viewing transitive permutation groups as purely combinatorial objects within a wider setting of association schemes.

We now briefly review some basic concepts about association schemes. (A more detailed discussion with all the definitions is given in the Preliminaries.) For a collection $\mathcal{R}$ of relations on a finite set X, the pair $\mathfrak{X} = (X, \mathcal{R})$ is called an *association scheme* (or a *scheme*) on X if the following properties hold:

(AS1) the diagonal relation $\Delta_X := \{(x, x) \mid x \in X\}$ is in $\mathcal{R}$;
(AS2) $\mathcal{R}$ is a partition of $X^2 = X \times X$;
(AS3) if $R \in \mathcal{R}$, then also its transpose R^t is in $\mathcal{R}$, where $R^t := \{(y, x) \mid (x, y) \in R\}$;
(AS4) for every triple $R, S, T \in \mathcal{R}$ and for $(x, y) \in R$, the number, denoted by p^R_{ST}, of elements $z \in X$ such that $(x, z) \in S$ and $(z, y) \in T$ does not depend on the choice of the pair $(x, y) \in R$.

The cardinality of X is called the *order* of the scheme $\mathfrak{X}$. The relations $R \in \mathcal{R}$ are called *basic relations*, and the digraphs (X, R) *basic digraphs* of $\mathfrak{X}$. It follows from axiom (AS4) that every basic digraph (X, R) is regular. The *degree* of R is the degree of (X, R) and will be denoted by $\deg(R)$. We denote by $\mathcal{R}^\#$ the set of all nondiagonal relations of $\mathcal{R}$. The cardinality $|\mathcal{R}^\#|$ is called the *class* of the scheme.

The scheme with basic relations Δ_X and $X^2 \setminus \Delta_X$ is called the *trivial scheme* on X. More generally, given a permutation group $G \leq \mathsf{Sym}(X)$ acting transitively on X, the set $\mathsf{Orb}_2(G)$ of 2-orbits (sometimes also referred to as *orbitals* of G), that is, the set of orbits in its natural action on X^2, gives rise to the association scheme $\mathfrak{X} = (X, \mathsf{Orb}_2(G))$; every scheme of this kind is called *Schurian*. In particular, the trivial scheme above is Schurian and it corresponds to the case when G is doubly transitive. (Of course, not every scheme arises in this way.)

In analogy with primitive permutation groups which are characterized by strongly connected orbital digraphs, we call a scheme $\mathfrak{X} = (X, \mathcal{R})$ *primitive* if each basic digraph (X, R), $R \in \mathcal{R} \setminus \{\Delta_X\}$, is strongly connected [1, page 79], and we call it *imprimitive* otherwise. The automorphism group $\mathsf{Aut}(\mathfrak{X})$ of a scheme $\mathfrak{X} = (X, \mathcal{R})$ is the subgroup of $\mathsf{Sym}(X)$ defined as follows:

$$\mathsf{Aut}(\mathfrak{X}) := \bigcap_{R \in \mathcal{R}} \mathsf{Aut}((X, R));$$

see [5]. Further, a scheme $\mathfrak{X} = (X, \mathcal{R})$ is called a *Cayley* (or a *translation* [3]) *scheme* if there is a subgroup $G \leq \mathsf{Aut}(\mathfrak{X})$ which acts regularly on X. Cayley

schemes are equivalent to the objects called Schur rings, and primitive Schur rings have been studied extensively [21, 22], and also in the context of B-groups.

Going a step further, as a natural generalization of transitive permutation groups containing a semiregular subgroup with two orbits, a scheme $\mathfrak{X}$ is called a *bi-Cayley scheme* if there is a subgroup $G \leq \mathsf{Aut}(X)$ acting semiregularly on X with two orbits. In particular, $\mathfrak{X}$ is said to be a (*biabelian/bicirculant scheme*) if G is an abelian/cyclic group. In contrast with Cayley schemes, much less is known about primitive bi-Cayley schemes. Note that there are examples of strongly regular bicirculants which do not arise from groups of rank 3 (see [14]), and consequently there are primitive bicirculant non-Schurian schemes of order $2n$ for $n \in \{8, 13, 25, 41, 61\}$, but even the classification of all primitive bicirculant schemes of order $2p$, p a prime, seems to be presently beyond our reach.

In the context of bi-Cayley schemes, the above-mentioned theorem of Wielandt, rephrased in the language of schemes, claims that a primitive bicirculant Schurian scheme on $2p$ points, p a prime, is of class at most 2, and that further, if the class is exactly 2, then the degrees of its basic digraphs are 1, $s(2s+1)$, $(s+1)(2s+1)$, and the degrees of its irreducible representations are 1, p, $p-1$. The main purpose of this paper is to prove the following generalization of Wielandt's result.

Theorem 1.1. *Let $\mathfrak{X}$ be a primitive bicirculant scheme on $2p^e$ points, $p > 2$ a prime. Then*

(A) $\mathfrak{X}$ is of class at most two; and
(B) if the class is exactly 2, then $2p^e = (2s+1)^2 + 1$ for some natural number s, and the degrees of basic digraphs of $\mathfrak{X}$ are 1, $s(2s+1)$, $(s+1)(2s+1)$, and the multiplicities of the irreducible representations of $\mathfrak{X}$ in its standard module are 1, p^e, $p^e - 1$.

As an immediate corollary we will then have the following result about primitive permutation groups.

Corollary 1.2. *Let G be a primitive permutation group of degree $2p^e$ points, $p > 2$ a prime. Assume that G contains a permutation with two cycles of length p^e. Then*

(A) G is either doubly transitive; or
(B) the rank of G is 3, and there exist a positive integer s such that $2p^e = (2s+1)^2+1$, and the sizes of subdegrees of G are 1, $s(2s+1)$, $(s+1)(2s+1)$, and the degrees of the irreducible representations of G are 1, p^e, $p^e - 1$.

As a consequence, in view of Corollary 1.2, a possible determination of which cyclic groups of prime power orders are 2-B-groups, depends on a detailed analysis of rank 3 groups containing semiregular cyclic subgroups with two orbits. Since all rank 3 groups were classified in [13] using the classification of finite simple groups, it's not difficult to check which groups from the list have degree $2p^e$ and contain a semiregular cyclic subgroup of order p^e. A direct inspection of the list of rank 3 groups shows that the only cyclic 2-B-group of odd prime power order is the cyclic group of order 5.

Notice that using the CFSG one can obtain much stronger results about permutation groups mentioned in Corollary 1.2, and, more generally, about primitive permutation groups containing a *bicycle* (a bicycle is a permutation which has two cycles not necessarily of the same length). P. Müller [16] classified all primitive permutation groups which contain a bicycle. He found that every such group is of

rank at most 3. In the same paper, Müller noticed that it would be very interesting to find a direct proof of this fact independent of the classification of finite simple groups. We consider Corollary 1.2 as a first step towards such a proof.

We would like to pose the following conjecture about a possible generalization of the above-mentioned results of Müller.

Conjecture 1.3. *A primitive bicirculant association scheme of any order contains at most two nontrivial classes.*

R. Guralnick pointed out [6] that using the CFSG, all primitive permutation groups of degree $2p^e$, p an odd prime, may be classified.

The article is organized as follows. In the next section we collect different concepts which are needed later on in the paper. In Section 3 various techniques which are needed to deal with biabelian association schemes are developed. In Section 4 we show that the splitting field of the Bose-Mesner algebra of a bicirculant association scheme is the p^e-th cyclotomic field $\mathbb{Q}(\xi_{p^e})$, p an odd prime. We also derive some properties of the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_{p^e})\colon \mathbb{Q})$ on the set of irreducible representations of the Bose-Mesner algebra. Sections 5 and 6 are devoted to the proof of the main result. Unfortunately we were unable to find a uniform proof; hence we had to split it into two parts: the first one deals with the case $e = 1$ and is done in Section 5, whereas the second one dealing with the case $e > 1$ is presented in Section 6.

2. Preliminaries

In this section we collect all definitions and facts which will be needed throughout the rest of this paper.

2.1. **More on association schemes.** In this subsection we follow notation from [1] and [24].

Let $\mathbb{C}^X$ denote the vector space of all complex-valued functions on X, and let $M_X(\mathbb{C})$ denote the algebra of all X-by-X matrices with entries in $\mathbb{C}$. The usual product of two matrices $A, B \in M_X(\mathbb{C})$ is written as AB (or $A \cdot B$). The *Schur-Hadamard* (entrywise) product is denoted by $A \circ B$. The identity and the all-one matrices are denoted as I_X and J_X, respectively.

If R is a relation on X, then its adjacency matrix $A(R)$ is the element in $M_X(\mathbb{C})$ with

$$A(R)(x,y) = \begin{cases} 1, & \text{if } (x,y) \in R, \\ 0, & \text{otherwise.} \end{cases}$$

Given a scheme $\mathfrak{X} = (X, \mathcal{R})$, the linear span of all matrices $A(R)$, $R \in \mathcal{R}$, is a subalgebra of $M_X(\mathbb{C})$. This is called the *adjacency algebra* (or *Bose-Mesner algebra*, or for short *BM-algebra*) of $\mathfrak{X}$, and will be denoted by $\mathbb{C}[\mathcal{R}]$. The vector space $\mathbb{C}^X$ is a (left) $\mathbb{C}[\mathcal{R}]$-module by letting $A \in \mathbb{C}[\mathcal{R}]$ act as $(Af)(x) = \sum_{y \in X} A(x,y)f(y)$, $f \in \mathbb{C}^X$. Since $\mathbb{C}[\mathcal{R}]$ is a semisimple algebra [24], the vector space $\mathbb{C}^X$ admits a decomposition into a direct sum of irreducible $\mathbb{C}[\mathcal{R}]$-submodules. These are called the *irreducible representations* of $\mathfrak{X}$. Recall that irreducible representations of a semisimple algebra are in one-to-one correspondence with central primitive idempotents. So, if ρ is an irreducible representation of an adjacency algebra $\mathbb{C}[R]$, then E_ρ will stand for the corresponding idempotent.

If $\mathfrak{X}$ is a Schurian scheme, that is, $\mathcal{R} = \mathsf{Orb}_2(G)$ for some $G \leq \mathsf{Sym}(X)$, then the adjacency algebra $\mathbb{C}[\mathcal{R}]$ is also known as the *centralizer ring (algebra)* of G [22], and

will be denoted by $\mathcal{V}(G)$. The irreducible representations of $\mathfrak{X}$ are in one-to-one correspondence with the *irreducible constituents* of the permutation group G.

A scheme $(X, \mathcal{S})$ is called a *fusion* of a scheme $(X, \mathcal{R})$ if each relation of $\mathcal{S}$ is a union of some relations from $\mathcal{R}$. An equivalent definition may be formulated via adjacency algebra: a scheme $(X, \mathcal{S})$ is a fusion of $(X, \mathcal{R})$ iff $\mathbb{C}[\mathcal{S}] \subseteq \mathbb{C}[\mathcal{R}]$. All possible fusions of $\mathfrak{X}$ may be described via their adjacency algebras.

Theorem 2.1. *A subalgebra $\mathcal{B}$ of $\mathcal{A} = \mathbb{C}[\mathcal{R}]$ is an adjacency algebra of a certain fusion scheme of $\mathcal{R}$ if and only if $\mathcal{B}$ contains I_X, J_X and is closed with respect to the operations ^{t} and $\circ$.*

2.2. **Representation theory.** For the sake of simplicity, we will write irrep for an irreducible representation. Let $\mathcal{A}$ be a finite-dimensional semisimple $\mathbb{F}$-algebra, where $\mathbb{F}$ is an arbitrary field. We denote the set of its irreps by $\mathsf{Irr}(\mathcal{A})$. If $\rho \in \mathsf{Irr}(\mathcal{A})$, then let e_ρ denote the corresponding central idempotent in $\mathcal{A}$. If $\mathcal{B}$ is a subalgebra of $\mathcal{A}$ and ρ is an irrep of $\mathcal{A}$, then $\rho_{\mathcal{B}}$ denotes the restriction of ρ on $\mathcal{B}$.

If $\mathcal{B}$ is semisimple, then $\rho_{\mathcal{B}}$ is isomorphic to a direct sum of irreps of $\mathcal{B}$. If σ is an irrep of $\mathcal{B}$, then we let $m_{\rho\sigma}$ denote the multiplicity of σ in the decomposition of $\rho_{\mathcal{B}}$.

Proposition 2.2. *Let $\mathcal{B}$ be a semisimple subalgebra of a finite-dimensional semisimple $\mathbb{F}$-algebra $\mathcal{A}$ and let $\rho \in \mathsf{Irr}(\mathcal{A}), \sigma \in \mathsf{Irr}(\mathcal{B})$. Then*

(a) $e_\sigma e_\rho \neq 0 \iff m_{\rho\sigma} \neq 0$;
(b) if $\dim(\rho) = \dim(\sigma)$, then either $e_\rho e_\sigma = 0$ or $e_\rho e_\sigma = e_\rho$.

Proof. (a) We have that $e_\rho e_\sigma = 0 \iff e_\sigma = (1 - e_\rho)e_\sigma \iff e_\sigma \in (1 - e_\rho)\mathcal{A}$. Since $(1 - e_\rho)\mathcal{A}$ is the kernel of ρ, we obtain $e_\rho e_\sigma = 0$ if and only if $\rho(e_\sigma) = 0$. The latter equality is equivalent to saying that σ does not appear in the decomposition of $\rho_{\mathcal{B}}$.

(b) Assume that $e_\rho e_\sigma \neq 0$. Then σ appears in the decomposition of $\rho_{\mathcal{B}}$. Comparing the dimensions we obtain that $\rho_{\mathcal{B}} = \sigma$. Let us denote their common dimension as n. Then

$$\rho(e_\rho e_\sigma) = \rho(e_\sigma) = \rho_{\mathcal{B}}(e_\sigma) = \sigma(e_\sigma) = I_n = \rho(e_\rho)$$

implying

$$\rho(e_\rho e_\sigma - e_\rho) = 0 \implies e_\rho e_\sigma - e_\rho \in \ker(\rho) = (1 - e_\rho)\mathcal{A} \implies e_\rho e_\sigma - e_\rho = 0.$$

□

As a consequence we obtain the following.

Corollary 2.3. *Let $\mathcal{B}$ be a semisimple subalgebra of a finite-dimensional semisimple $\mathbb{F}$-algebra $\mathcal{A}$. Denote by k the maximal dimension of irreps of $\mathcal{A}$. Then for each irrep σ of $\mathcal{B}$ with $\dim(\sigma) = k$ we have that $e_\sigma = e_{\rho_1} + ... + e_{\rho_\ell} \in Z(\mathcal{A})$, where $\rho_1, ..., \rho_\ell$ is the complete set of irreps of $\mathcal{A}$ which satisfy the property $\rho_i|_{\mathcal{B}} = \sigma$.*

2.3. **Group algebras.** All groups considered in the paper are finite and written multiplicatively. If H is a group, then 1_H denotes its identity element. The complex group algebra is denoted as $\mathbb{C}[H]$, and its elements are written as formal sums $\sum_{h \in H} \alpha_h h$. If $\alpha = \sum_{h \in H} \alpha_h h, \beta = \sum_{h \in H} \beta_h h \in \mathbb{C}[H]$, then

$$\alpha\beta := \sum_{h,f \in H} \alpha_h \beta_f hf$$

and

$$\alpha \circ \beta := \sum_{h \in H} \alpha_h \beta_h h.$$

The latter operation is called a *Schur-Hadamard* product. Given a subset $S \subseteq H$, we write $\underline{S}$ for $\sum_{h \in S} h$.

Given a number $m \in \mathbb{Z}$ and $\alpha = \sum_{h \in H} \alpha_h h$, we set $\alpha^{(m)} := \sum_{h \in H} \alpha_h h^m$. If H is abelian, then the mapping $\alpha \mapsto \alpha^{(m)}$ is an endomorphism of the group algebra $\mathbb{C}[H]$. If m is coprime to $|H|$, then $^{(m)}$ is an automorphism of $\mathbb{C}[H]$. The set of all irreps of H will be denoted as $\mathsf{Irr}(H)$. If H is abelian, then the irreps of H are one-dimensional and coincide with irreducible characters of H. In this case we refer to the elements of $\mathsf{Irr}(H)$ as irreducible characters. Recall that the primitive central idempotent of $\mathbb{C}[H]$ corresponding to a character $\chi \in \mathsf{Irr}(H)$ has the form

$$e_\chi = \frac{1}{|H|} \sum_{h \in H} \overline{\chi(h)} h. \tag{2.1}$$

Now let H denote a cyclic group of order n generated by $h \in H$. For a divisor d of n, let H_d denote the subgroup of H of order d. We also will write $[m], m \in \mathbb{N}$ for the set $\{x \in \mathbb{Z} \,|\, 0 \le x \le m\}$.

It is well known that $\mathsf{Aut}(H) \cong \mathbb{Z}_n^*$. In what follows we identify $\mathsf{Aut}(H)$ with $\mathbb{Z}_n^*$. Recall that the automorphism $k \in \mathbb{Z}_n^*$ maps $h \in H$ to the power h^k.

Fix ξ_n as a primitive complex n-th root of unity, and for $i \in [n-1]$, let χ_i be the character of $H = \langle h \rangle$ defined as

$$\chi_i(h^j) = \xi_n^{ij}, \quad j \in [n-1].$$

It is well known that the Galois group of the field $\mathbb{Q}(\xi_n)$ is isomorphic to $\mathbb{Z}_n^*$. In what follows we denote the action of $k \in \mathbb{Z}_n^*$ on $\mathbb{Q}(\xi_n)$ as $^{(k)}$. Note that $(\xi_n^j)^{(k)} = \xi_n^{kj}$. The action of $\mathbb{Z}_n^*$ on $\mathbb{Q}(\xi_n)$ induces an action of $\mathbb{Z}_n^*$ on $\mathsf{Irr}(H)$: $(\chi_i)^{(k)} = \chi_{ik}$, where the multiplication is done modulo n. For each $\alpha \in \mathbb{Q}[H]$ and $\chi_i \in \mathsf{Irr}(H)$ we have that

$$\chi_i(\alpha^{(k)}) = \chi_i(\alpha)^{(k)} = \chi_{ik}(\alpha).$$

2.4. **Strongly regular bicirculant graphs.** Let $R \subset X^2 \setminus \Delta_X$ such that $R = R^t$, where X is a finite set. The graph (X, R) is called *bi-Cayley* (*semi-Cayley* in [17]) if there is a subgroup $G \le \mathsf{Aut}((X, R))$ acting semi-regularly on X with two orbits. If G is cyclic, then (X, R) is also called a *bicirculant graph*.

A nonempty and noncomplete graph (X, R) is called *strongly regular* if the relations Δ_X, R, R^c, where $R^c := X^2 \setminus (R \cup \Delta_X)$, form an association scheme on X. The numbers $v := |X|, k := p_{RR}^{\Delta_X}, \lambda := p_{RR}^R, \mu := p_{RR}^{R^c}$ are called the *parameters* of a strongly regular graph (X, R). A strongly regular graph with parameters v, k, λ, μ is also referred to as a (v, k, λ, μ) strongly regular graph. Note that a complement of a strongly regular graph is a strongly regular graph, too. Strongly regular bi-Cayley graphs were studied in [12, 17], and in particular for bicirculant graphs, see also [15, 14].

Theorem 2.4 ([17, Theorem 4.1])**.** *If (X, R) is a $(2n, k, \lambda, \mu) - srg$ with $k < n$, which is also a connected bicirculant graph, and n is odd, then $2n = (2s+1)^2 + 1$, $k = s(2s+1)$, $\lambda = s^2 - 1$, $\mu = s^2$.*

It is well known that connected strongly regular graphs have three eigenvalues: one of them is always the degree of the graph, and the other two are also referred to as the nontrivial eigenvalues. We will use the following corollary of Theorem 2.4.

Corollary 2.5. *For a connected strongly regular, bicirculant graph with* $2n$ *vertices where* n *is odd, the sum of its nontrivial eigenvalues is* -1.

3. Biabelian association schemes

Let $H \leq \mathsf{Sym}(X)$ be an abelian group acting semiregularly on a set X with two orbits, say X_1 and X_2. The centralizer ring [22] $\mathcal{V} := \mathcal{V}(H)$ of H is isomorphic to the matrix algebra $M_2(\mathbb{C}[H])$. In order to describe this isomorphism we fix an arbitrary pair $(x_1, x_2) \in X_1 \times X_2$ and define an $X_i \times X_j$ matrix $\Psi_{ij}(\alpha)$ with $\alpha = \sum_{h\in H} \alpha_h h \in \mathbb{C}[H]$ and $i, j = 1, 2$ by setting $\big(\Psi_{ij}(\alpha)\big)(x_i^a, x_j^b) := \alpha_{a^{-1}b}$, where a, b run through H. We shall refer to x_1 and x_2 as the *base points* of H. Now the mapping $\Psi : M_2(\mathbb{C}[H]) \to \mathcal{V}$ defined by

$$\Psi\colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \Psi_{11}(a) & \Psi_{12}(b) \\ \Psi_{21}(c) & \Psi_{22}(d) \end{pmatrix}$$

is an algebra isomorphism. Thus $\dim(\mathcal{V}) = 4|H|$.

For two elements X and Y in $M_2(\mathbb{C}[H])$, their Schur-Hadamard product is

$$(X \circ Y)_{ij} := X_{ij} \circ Y_{ij}.$$

Note that Ψ also preserves the Schur-Hadamard product.

As was shown in [10], each H-invariant binary relation R on X may be encoded by its *symbol*: a 2-by-2 matrix $\begin{pmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{pmatrix}$, where $R_{ij} := \{h \in H \mid (x_i, x_j^h) \in R\}$ and $i, j = 1, 2$. The adjacency matrix of R has the following form:

$$\begin{pmatrix} \Psi_{11}(\underline{R_{11}}) & \Psi_{12}(\underline{R_{12}}) \\ \Psi_{21}(\underline{R_{21}}) & \Psi_{22}(\underline{R_{22}}) \end{pmatrix}.$$

The 2-orbits of H have the following symbols:

$$\begin{pmatrix} h & \emptyset \\ \emptyset & \emptyset \end{pmatrix}, \begin{pmatrix} \emptyset & h \\ \emptyset & \emptyset \end{pmatrix}, \begin{pmatrix} \emptyset & \emptyset \\ h & \emptyset \end{pmatrix}, \begin{pmatrix} \emptyset & \emptyset \\ \emptyset & h \end{pmatrix}, h \in H.$$

The center $Z(M_2(\mathbb{C}[H]))$ has dimension $|H|$ and consists of all "scalar" matrices, that is, the matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},\ a \in \mathbb{C}[H],$$

which we shall abbreviate as aI_2. Since $\mathcal{V} \cong M_2(\mathbb{C}[H])$ is semisimple, the number of irreducible representations of $M_2(\mathbb{C}[H])$ is $\dim(Z(M_2(\mathbb{C}[H]))) = |H|$.

All irreducible representations of $M_2(\mathbb{C}[H])$ are of dimension 2. These representations are parameterized by irreducible characters of H: the representation $\widehat{\chi}$ of $M_2(\mathbb{C}[H])$ corresponding to a character $\chi \in \mathsf{Irr}(H)$ has the form

$$\widehat{\chi}\colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \chi(a) & \chi(b) \\ \chi(c) & \chi(d) \end{pmatrix}.$$

The central idempotent $e_{\widehat{\chi}}$ corresponding to $\widehat{\chi}$ has the form

$$e_{\widehat{\chi}} = e_\chi I_2,$$

where e_χ is the central idempotent corresponding to the character χ (see (2.1)).

Now let $\mathfrak{X} = (X, \mathcal{R})$ be an H-invariant association scheme and $\mathcal{A} := \Psi^{-1}(\mathbb{C}[\mathcal{R}])$. Since $\mathcal{A} \subseteq M_2(\mathbb{C}[H])$, each irreducible representation of $\mathcal{A}$ is either one- or two-dimensional.

All matrices of $\mathbb{C}[\mathcal{R}]$ have constant row sum. This yields a one-dimensional irrep ρ of $\mathbb{C}[\mathcal{R}]$ which is called *principal*. If R is a basic relation of $\mathcal{R}$, then $\rho(A(R))$ is the degree $\deg(R)$ of the graph (X, R).

Proposition 3.1. *If $\mathcal{A}$ has an irrep of dimension 2, then $\mathfrak{X}$ is imprimitive.*

Proof. Let ρ be a 2-dimensional irrep of $\mathcal{A}$. By Corollary 2.3, $e_\rho \in \Psi^{-1}(Z(\mathcal{V}))$. Since $e_\rho \neq I_2$, the dimension of $\mathcal{A} \cap \Psi^{-1}(Z(\mathcal{V}))$ is at least two. Therefore $\mathcal{A}$ contains a matrix of the form aI_2 where $a \in \mathbb{C}[H]$ is not proportional to 1_H. Hence $\mathbb{C}[\mathcal{R}] = \Psi(\mathcal{A})$ contains the matrix $M := \Psi(aI_2) = \begin{pmatrix} \Psi_{11}(a) & 0 \\ 0 & \Psi_{22}(a) \end{pmatrix}$. Write $M = \sum_{R\in\mathcal{R}} \mu_R A(R)$. Since M is a block-diagonal matrix, each basic relation R with $\mu_R \neq 0$ has a block-diagonal adjacency matrix. Since a is not proportional to 1_H, the matrix M is nonscalar. Therefore there exists a basic relation $R \neq \Delta_X$ with $\mu_R \neq 0$. Since $A(R)$ is block-diagonal, the basic digraph (X, R) is disconnected, contrary to the primitivity of $\mathcal{R}$. □

The following proposition generalizes [10, (1.2) Theorem].

Proposition 3.2. *Let σ be a nonprincipal irrep of $\mathcal{A}$ and $L := \{\chi \in \mathsf{Irr}(H) \mid m_{\widehat{\chi}\sigma} \neq 0\}$. If $\mathfrak{X}$ is primitive, then $\langle L\rangle = \mathsf{Irr}(H)$.*

Proof. If $\mathfrak{X}$ is primitive, then by Proposition 3.1 all irreps of $\mathbb{C}[\mathcal{R}]$ are one-dimensional. So, $\mathfrak{X}$ is a commutative association scheme.

Since $1_H I_2 = \sum_{\chi\in\mathsf{Irr}(H)} e_{\widehat{\chi}}$ and $e_\sigma e_{\widehat{\chi}} = 0$ for each $\chi \notin L$ (Proposition 2.2), we obtain

$$e_\sigma = e_\sigma \sum_{\chi\in L} e_{\widehat{\chi}} = e_\sigma \sum_{\chi\in\langle L\rangle} e_{\widehat{\chi}} = e_\sigma \sum_{\chi\in\langle L\rangle} e_\chi I_2 = e_\sigma \frac{1}{|K|}\underline{K} I_2,$$

where $K := \bigcap_{\chi\in L} \mathsf{Ker}(\chi)$. Set $E_\sigma := \Psi(e_\sigma)$, $E := \Psi\big(\underline{K} I_2\big)$. Then E_σ is a primitive idempotent of the algebra $\mathcal{A}$ corresponding to the irrep σ. Since $K \leq H$, the matrix E is the adjacency matrix of an equivalence relation. If K is nontrivial, then the equality $E_\sigma E = |K|E_\sigma$ implies that E_σ has repeated columns. By Theorem 9.3 [1] $\mathfrak{X}$ is imprimitive, a contradiction. □

4. Bicirculant association schemes and conjugations

In this section $\mathfrak{X} = (X, \mathcal{R})$ will denote a bicirculant scheme of order $2n$. Let H denote the cyclic, semiregular subgroup of $\mathsf{Aut}(\mathfrak{X})$ having two orbits of length n, and let h be a generator for H.

Let $\mathcal{A} := \Psi^{-1}(\mathbb{C}[\mathcal{R}])$ be the embedding of the adjacency algebra $\mathbb{C}[\mathcal{R}]$ into $M_2(\mathbb{C}[H])$. Thus for each $R \in \mathcal{R}$ we have that

$$\Psi^{-1}(A(R)) = \begin{pmatrix} \underline{R_{11}} & \underline{R_{12}} \\ \underline{R_{21}} & \underline{R_{22}} \end{pmatrix},$$

where (R_{ij}) is a symbol of R. In what follows we identify $\Psi^{-1}(A(R))$ with R; in particular, we will write $R = (\underline{R_{ij}})$. Observe that

$$R = \begin{pmatrix} \underline{R_{11}} & \underline{R_{12}} \\ \underline{R_{21}} & \underline{R_{22}} \end{pmatrix} \implies R^t = \begin{pmatrix} \underline{R_{11}^{(-1)}} & \underline{R_{21}^{(-1)}} \\ \underline{R_{12}^{(-1)}} & \underline{R_{22}^{(-1)}} \end{pmatrix}.$$

In what follows we shall write $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^*$ for the matrix $\begin{pmatrix} a^{(-1)} & c^{(-1)} \\ b^{(-1)} & d^{(-1)} \end{pmatrix}$ in $M_2(\mathbb{C}[H])$. We define $\mathrm{Tr}(R) := \underline{R_{11}} + \underline{R_{22}}$ for $R \in \mathcal{R}$.

For $i \in [n-1]$, let ρ_i denote the restriction of $\widehat{\chi}_i$ onto $\mathcal{A}$. The action of $\mathbb{Z}_n^*$ on $\{\chi_i\}_{i=0}^{n-1}$ induces an action on the set $\{\rho_i\}_{i=0}^{n-1}$. For $k \in \mathbb{Z}_n^*$, the *conjugation* $\rho_i^{(k)}$ of ρ_i by k is the representation which maps $R = (\underline{R_{uv}}) \in \mathcal{A}$ to $(\chi_i(\underline{R_{uv}})^{(k)}) = (\chi_{ki}(\underline{R_{uv}}))$. Thus $\rho_i^{(k)} = \rho_{ki}$ for each $k \in \mathbb{Z}_n^*$ and $i \in [n]$. Note that $\mathrm{Tr}(\rho_i(R)) = \chi_i(\mathrm{Tr}(R)) = \chi_i(\underline{R_{11}} + \underline{R_{22}})$.

For the rest of the paper we assume that $\mathfrak{X}$ is a primitive bicirculant scheme with r classes. Then $\dim(\mathcal{A}) = r+1$. By Proposition 3.1, $\mathcal{A}$ is commutative. Therefore $\mathcal{A}$ has $r+1$ complex irreducible one-dimensional representations, say $\sigma_0, ..., \sigma_r$. We assume that σ_0 is a principal representation of $\mathcal{A}$, that is, $\sigma_0(R) = \deg(R)$. Note that $\{\sigma_i(R)\}_{i=0}^r$ coincides with the spectrum of the digraph $(X, R), R \in \mathcal{R}$.

Since $\dim(\rho_i) = 2$ for each $i \in [n-1]$, we obtain that $\rho_i = \sigma_j + \sigma_k$ for certain $j, k \in [r]$. In particular, $\rho_0 = \sigma_0 + \sigma_1$, where σ_1 is the only nonprincipal irrep of $\mathcal{A}$ appearing in a decomposition of ρ_0. Since $\deg(R) = |R_{11}| + |R_{12}| = |R_{21}| + |R_{22}| = |R_{11}| + |R_{21}|$, the matrix

$$\rho_0(R) = \begin{pmatrix} |R_{11}| & |R_{12}| \\ |R_{21}| & |R_{22}| \end{pmatrix}$$

has two eigenvalues: $\deg(R) = |R_{11}| + |R_{12}|$ and $|R_{22}| - |R_{12}|$. Therefore $\sigma_1(R) = |R_{22}| - |R_{12}|$. Since $\sigma_0(R) = \sigma_0(R^t)$, we always have $|R_{11}| = |R_{22}|$ and $|R_{12}| = |R_{21}|$. Hence $\sigma_1(R) = |R_{11}| - |R_{12}|$ for each $R \in \mathcal{R}$.

For the rest of the paper we assume that $n = p^e$, where p is an odd prime. Since $\mathcal{R}$ is primitive, we obtain $|\sigma_i(R)| < \sigma_0(R)$ for each $0 < i \le r$ and $R \in \mathcal{R}$.

It is well known that $\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p-1}$. For $i \in [e-1]$, let $P_i \le \mathbb{Z}_{p^e}^*$ denote the subgroup of order p^i, and for a divisor l of $p-1$, let Q_l denote the subgroup of order l.

Proposition 4.1. *For each $j = 2, ..., r$, there exists $i \in [p^e - 1]$ coprime to p such that $\rho_i = \sigma_1 + \sigma_j$. In particular, $\sigma_j(R) \in \mathbb{Q}(\xi_{p^e})$ for each $j \in [r]$ and $R \in \mathcal{R}$.*

Proof. By Proposition 3.2 there exists $i \in [p^e - 1]$ coprime to p such that $m_{\rho_i \sigma_j} > 0$. Thus $\rho_i = \sigma_j + \sigma_k$ for a suitable $k \in [r]$. By the same proposition, there exists $\ell \in [p^e - 1]$ coprime to p with $m_{\rho_\ell \sigma_1} > 0$. Hence $\rho_\ell = \sigma_1 + \sigma_m$ for some $m \in [r]$. Since $\sigma_1(R) \in \mathbb{Q}$ for every $R \in \mathcal{R}$, we obtain that $\sigma_m(R) \in \mathbb{Q}(\xi_{p^e})$. Thus $\sigma_m(R)^{(u)}$ is well defined for each $u \in \mathbb{Z}_{p^e}^*$ and, therefore, the mapping $R \mapsto \sigma_m(R)^{(u)}$ is an irrep of $\mathcal{A}$. Since i and ℓ are coprime to p, there exists $u \in \mathbb{Z}_{p^e}^*$ such that $u\ell = i$. Therefore

$$\sigma_j + \sigma_k = \rho_i = \rho_\ell^{(u)} = \sigma_1 + \sigma_m^{(u)}$$

implying $k = 1$ and $\sigma_j(R) = \sigma_m(R)^{(u)} \in \mathbb{Q}(\xi_{p^e})$. □

It follows from the above proposition that $\mathbb{Z}_{p^e}^*$ acts on $\sigma_0, \sigma_1, ..., \sigma_r$ via conjugation $\sigma_i \mapsto \sigma_i^{(u)}$, $u \in \mathbb{Z}_{p^e}^*$. The properties of this action are studied in the statement below.

Proposition 4.2. *Let $i \in [p^e-1]$ such that $i = p^j k$, $\gcd(k,p)=1$. Then the action of $\mathbb{Z}_{p^e}^*$ via conjugation has the following properties:*

(a) the stabilizer of ρ_i in $\mathbb{Z}_{p^e}^*$ contains P_j;

(b) $\mathbb{Z}_{p^e}^*$ has the following orbits in its action on $\mathsf{Irr}(\mathcal{A})$:

$$\{\sigma_0\},\ \{\sigma_1\},\ \{\sigma_2,\dots,\sigma_r\};$$

(c) if $m_{\rho_i\sigma_1} < 2$, then P_j fixes every irrep of $\mathcal{A}$. In particular,

$$r \le 1 + (p-1)p^{e-1-j};$$

(d) if $K := (\mathbb{Z}_{p^e}^*)_{\sigma_2}$, then $\mathrm{Tr}(R)^{(K)} = \mathrm{Tr}(R)$ for each $R \in \mathcal{R}$.

Proof. (a) If $x \in P_j$, then $x = yp^{e-j}+1$, $y \in [p^j-1]$. Hence the Galois automorphism ${}^{(x)}$ fixes each matrix $\rho_i(R)$, $R \in \mathcal{R}$, entrywise. This gives $\rho_i = \rho_i^{(x)}$.

(b) For $t = 0, 1$, $\sigma_t(R)$ is an integer for all $R \in \mathcal{R}$; hence σ_t is fixed by $\mathbb{Z}_{p^e}^*$.

Now let $\sigma_\imath$ and $\sigma_\jmath$ be arbitrary irreps of $\mathcal{A}$ with $\imath, \jmath \in \{2, ..., r\}$. By Proposition 4.1 there exist $i, j \in [p^e-1]$ coprime to p such that $\rho_i = \sigma_1 + \sigma_\imath, \rho_j = \sigma_1 + \sigma_\jmath$. Observe that $\mathbb{Z}_{p^e}^*$ is transitive on the set of all representations ρ_ℓ with $\gcd(\ell, p) = 1$. Hence $\rho_i = \rho_j^{(k)}$ for a suitable $k \in \mathbb{Z}_{p^e}^*$ implying $\sigma_\jmath^{(k)} = \sigma_\imath$.

(c) Let $\rho_i = \sigma_u + \sigma_v$, where one of u and v is larger than 1, say u. As P_j fixes ρ_i, see (a), P_j fixes σ_u as well. Now (b) shows that P_j fixes all irreps of $\mathcal{A}$.

(d) Since K fixes each irrep of $\mathcal{A}$, the equality $\rho_i^{(K)} = \rho_i$ holds for each $i \in [p^e-1]$. Thus $\rho_i(R)^{(K)} = \rho_i(R)$ implying that $\chi_i(\mathrm{Tr}(R)^{(K)}) = \chi_i(\mathrm{Tr}(R))$ for each $i \in [p^e-1]$. Finally $\mathrm{Tr}(R)^{(K)} = \mathrm{Tr}(R)$. □

5. The proof of Theorem 1.2, $e = 1$

We start with the following statement which is of independent interest.

Proposition 5.1. *Let $\mathfrak{X} = (X, \mathcal{R})$ be a commutative bi-abelian association scheme and $\mathcal{A} = \Psi^{-1}(\mathbb{C}[\mathcal{R}]) \subseteq M_2(\mathbb{C}[H])$ the image of its BM-algebra. Let $\mathcal{B} \subseteq \mathcal{A}$ be a subspace consisting of all matrices $M \in \mathcal{A}$ with $M_{1,1} = M_{2,2}$. Then there exists a fusion scheme $\mathcal{S}$ of $\mathcal{R}$ such that $\mathbb{C}[\mathcal{S}] = \Psi(\mathcal{B})$.*

Proof. By Theorem 2.1, $\Psi(\mathcal{B})$ is an adjacency algebra of a fusion scheme if and only if it is a subalgebra of $\mathbb{C}[\mathcal{R}]$ which contains I_X, J_X and is closed with respect to $\circ$ and ^{t}.

Let us show first that $\Psi(\mathcal{B})$ is a subalgebra of $\mathbb{C}[\mathcal{R}]$, or equivalently, $\mathcal{B}$ is a subalgebra of $\mathcal{A}$. Note that $\mathcal{B}$ is a fixed point subspace of the mapping

$$\Phi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & b \\ c & a \end{pmatrix}.$$

A direct computation shows that Φ is an anti-automorphism of the matrix algebra $M_2(\mathbb{C}[H])$. Since $\mathcal{A}$ is commutative, a fixed point subspace of an anti-automorphism is a subalgebra of $\mathcal{A}$.

Since $\mathcal{B}$ is $\circ$-closed and Ψ preserves $\circ$, the image $\Psi(\mathcal{B})$ is $\circ$-closed, too. The subspace $\mathcal{B}$ is also closed with respect to *. Therefore $\Psi(\mathcal{B})^t = \Psi(\mathcal{B})$.

To finish the proof, it remains to note that the inclusions $1_H I_2 \in \mathcal{B}$ and $\begin{pmatrix} \underline{H} & \underline{H} \\ \underline{H} & \underline{H} \end{pmatrix} \in \mathcal{B}$ imply $I_X, J_X \in \Psi(\mathcal{B})$. □

For $A \in M_2(\mathbb{C}[H])$, we let ${}^tA$ denote the matrix $\Phi(A)$, and call A *secondary symmetric* if $A = {}^tA$.

Proposition 5.2. *Let $\mathfrak{X} = (X, \mathcal{R})$ be a primitive bicirculant scheme on $2n$ points and $\mathcal{A} = \Psi^{-1}(\mathbb{C}[\mathcal{R}]) \subseteq M_2(\mathbb{C}[H])$, and further let each $M \in \mathcal{A}$ be secondary symmetric. Then the symmetrization $\mathfrak{X}^*$ of $\mathfrak{X}$ is a Cayley scheme over the dihedral group D_{2n} of order $2n$. Furthermore, if $\mathfrak{X}$ is nontrivial, then so is $\mathfrak{X}^*$.*

Proof. As $\mathcal{X}$ is primitive, each irrep of the BM-algebra $\mathbb{C}[\mathcal{R}]$ is of dimension 1. This is equivalent with that $\mathbb{C}[\mathcal{R}]$ is commutative [22, Theorem 29.3]. It is well known that the symmetrization $\mathcal{R}^* = \{R \cup R^t \mid R \in \mathcal{R}\}$ of $\mathcal{R}$ is a symmetric association scheme on X. Write $\mathfrak{X}^* = (X, \mathcal{R}^*)$. For $i = 1, 2$, denote by X_i the two orbits of H with base points x_i, and define the involution τ in $\mathsf{Sym}(X)$ by

$$\tau \colon x_1^h \leftrightarrow x_2^{h^{-1}}, \quad h \in H.$$

As $R = R^t$ for each $R \in \mathcal{R}^*$, $\tau \in \mathsf{Aut}((X, R))$, and hence $\tau \in \mathsf{Aut}(\mathfrak{X}^*)$. It can be seen that $\langle \tau, H \rangle = D_{2n}$, and it is regular on X. It remains to prove that $\mathfrak{X}^*$ is nontrivial whenever $\mathfrak{X}$ is nontrivial. Otherwise, we have that $\mathcal{R} = \{\Delta_X, R, R^t\}$. However, (X, R) and (X, R^t) have the same degree, and hence $2\deg(R) + 1 = \deg(R) + \deg(R^t) + 1 = |X| = 2n$, a contradiction. □

For the rest of the section we assume that $\mathfrak{X} = (X, \mathcal{R})$ is a nontrivial primitive bicirculant scheme on $2p$ points, p a prime.

Proposition 5.3. *The following equality holds in the group algebra $\mathbb{C}[H]$ for each pair $R, S \in \mathcal{R}$:*

$$\mathrm{Tr}(R)\mathrm{Tr}(S) - \sigma_1(R)\mathrm{Tr}(S) - \sigma_1(S)\mathrm{Tr}(R) + 2\sigma_1(R)\sigma_1(S)1_H = \sum_{T \in \mathcal{R}} p_{RS}^T \mathrm{Tr}(T), \tag{5.1}$$

where p_{RS}^T are the structure constants of $\mathcal{R}$.

Proof. Pick an arbitrary $i \in [p-1]$. It follows from Proposition 4.1 that the mapping

$$R \mapsto \mathrm{Tr}(\rho_i(R)) - \sigma_1(R) = \chi_i(\mathrm{Tr}(R)) - \sigma_1(R)$$

is a one-dimensional representation of $\mathcal{A}$. Therefore

$$\big(\chi_i(\mathrm{Tr}(R)) - \sigma_1(R)\big)\big(\chi_i(\mathrm{Tr}(S)) - \sigma_1(S)\big) = \sum_{T \in \mathcal{R}} p_{RS}^T (\chi_i(\mathrm{Tr}(T)) - \sigma_1(T)).$$

Since χ_i is a representation of H we can rewrite the above equality as follows:

$$\chi_i\big((\mathrm{Tr}(R) - \sigma_1(R)1_H)(\mathrm{Tr}(S) - \sigma_1(S)1_H) - \sum_{T \in \mathcal{R}} p_{RS}^T (\mathrm{Tr}(T) - \sigma_1(T)1_H)\big) = 0.$$

Opening the brackets and taking into account that $\sigma_1(R)\sigma_1(S) = \sum_{T \in \mathcal{R}} p_{RS}^T \sigma_1(T)$ we obtain

$$\chi_i\big(\mathrm{Tr}(R)\mathrm{Tr}(S) - \sigma_1(R)\mathrm{Tr}(S) - \sigma_1(S)\mathrm{Tr}(R) + 2\sigma_1(R)\sigma_1(S)1_H - \sum_{T \in \mathcal{R}} p_{RS}^T \mathrm{Tr}(T)\big) = 0.$$

Since this equality holds for all $i \in [p-1]$, it implies (5.1). □

Since $\mathrm{Tr}(T) \circ 1_H = 0$ for all $T \in \mathcal{R}^\#$ (we let $\mathcal{R}^\# = \mathcal{R} \setminus \{\Delta_X\}$), the coefficient of 1_H in the right-hand side of (5.1) is $2\sigma_0(R)$ if $R = S^t$ and zero otherwise. Suppose that $R, S \in \mathcal{R}^\#$. The coefficient of 1_H in the left-hand side of (5.1) is then

$$2\sigma_1(R)\sigma_1(S) + |R_{11} \cap S_{22}^{(-1)}| + |R_{22} \cap S_{11}^{(-1)}| + \delta_{R,S^t}(|R_{11}| + |R_{22}|),$$

where δ is the Kronecker delta. Comparing both equations we obtain

$$2\sigma_1(R)\sigma_1(S) + |R_{11} \cap S_{22}^{(-1)}| + |R_{22} \cap S_{11}^{(-1)}| + \delta_{R,S^t}(|R_{11}| + |R_{22}|) = 2\sigma_0(R)\delta_{R,S^t},$$

which is equivalent to

$$2\sigma_1(R)\sigma_1(S) + |R_{11} \cap S_{22}^{(-1)}| + |R_{22} \cap S_{11}^{(-1)}| = 2\delta_{R,S^t}|R_{12}|. \tag{5.2}$$

Proof of Theorem 1.1 *for* $e = 1$. Consider the following subset: $\mathcal{S} := \{R \in \mathcal{R}^\# \mid \sigma_1(R) \neq 0\}$. All relations in $\mathcal{S}$ are symmetric, since for a nonsymmetric R the equation (5.2) implies $\sigma_1(R) = 0$ (take $R = S$ in (5.2)). Since $\sum_{R\in\mathcal{R}^\#} \sigma_1(R) = -1$, the set $\mathcal{S}$ contains at least one relation. If $\mathcal{S}$ contains a unique relation, say S, then $\sigma_1(S) = -1$. Since $\sigma_1(R) = 0$ for each $R \notin \mathcal{S}$, the primitive idempotent of the BM-algebra $\mathbb{C}[\mathcal{R}]$ corresponding to the irrep σ_1 is a linear combination of I_X and $A(S)$. This implies that $S \cup \Delta_X$ is an equivalence relation on X, a contradiction.

Thus $|\mathcal{S}| \geq 2$. If $\mathcal{S}$ has more than two relations, then there exist $U, V \in \mathcal{S}$ such that $\sigma_1(U)\sigma_1(V) > 0$. But this contradicts (5.2). Thus $\mathcal{S} = \{R, S\}$ for suitable $R, S \in \mathcal{R}^\#$. Now pick an arbitrary $T \notin \mathcal{S}$ and plug the pair T, T^t into (5.2). This yields us $|T_{11} \cap T_{22}| = |T_{12}|$. Since $\sigma_1(T) = 0$, $|T_{12}| = |T_{11}|$. Hence $|T_{11} \cap T_{22}| = |T_{11}|$. Together with $|T_{22}| = |T_{11}|$ we obtain $T_{11} = T_{22}$.

Consider now the subalgebra $\mathcal{B}$ of $\mathcal{A}$ consisting of those matrices M which satisfy $M_{11} = M_{22}$. Since each $T \notin \mathcal{S}$ has the property $T_{11} = T_{22}$, the dimension of $\mathcal{B}$ is either r or $r+1$. In the first case $R \cup S$ is a basic relation of the scheme corresponding to $\mathcal{B}$. But now the restriction of σ_1 on $\mathcal{B}$ is an irreducible representation for which $S \cup R$ is the only nondiagonal relation with nonzero value of σ_1. Hence $\Delta_X \cup R \cup S$ is an equivalence relation on X implying $\Delta_X \cup R \cup S = X^2$ and $r = 2$.

If $\dim(\mathcal{B}) = r + 1$, then $\mathcal{B} = \mathcal{A}$, which means that T is secondary symmetric for each $T \in \mathcal{R}$. By Proposition 5.2, $\mathfrak{X}^*$ is a primitive Cayley scheme over D_{2p}. According to a result of Wielandt [21, Satz 2], such a scheme must be trivial, a contradiction. □

6. The proof of Theorem 1.2, $e > 1$

We keep here the notation from Section 4. For the rest of the paper H_i will denote a unique subgroup of H of order p^i.

For $R \in \mathcal{R}$, we introduce parameters $a_i(R)$ as

$$a_i(R) := \frac{|R_{11} \cap (H_{i+1} \setminus H_i)| + |R_{22} \cap (H_{i+1} \setminus H_i)|}{p^i(p-1)}, \quad i \in [e-1],$$

where $R = (\underline{R_{ij}})$ in $\mathcal{A}$. The following equations are clear:

$$\sum_{R\in\mathcal{R}} a_i(R) = 2, \quad i \in [e-1]. \tag{6.1}$$

For the sake of simplicity, we put

$$m_i = m_{\rho_{p^i}\sigma_1}, \quad i \in [e-1],$$

and define the number f as

$$f := \max\{\, i \in [e-1] \mid m_i < 2 \,\}.$$

Note that f is well defined, since $m_0 < 2$ follows from Proposition 4.1.

Lemma 6.1. *For every* $R \in \mathcal{R}$, $\mathrm{Tr}(R)^{(P_{e-1})} = \mathrm{Tr}(R)$.

Proof. It is enough to show that

$$r \leq p. \tag{6.2}$$

Indeed, this implies that P_{e-1} fixes all irreps σ_i and, therefore, all ρ_i as well. Thus for all $i \in [p^e - 1]$ and all $x \in P_{e-1}$ we have that $\chi_i(\mathrm{Tr}(R)^{(x)}) = \chi_i(\mathrm{Tr}(R))$ implying $\mathrm{Tr}(R)^{(P_{e-1})} = \mathrm{Tr}(R)$.

We may assume that $\rho_{p^{e-1}} = 2\sigma_1$, since otherwise (6.2) follows from Proposition 4.2.(c). We have that $f < e - 1$. In view of (6.1), in order to obtain (6.2), it is enough to show that

$$\forall R \in \mathcal{R}^{\#} : a_{e-1}(R) \geq \frac{2}{p}. \tag{6.3}$$

Choose an $R \in \mathcal{R}^{\#}$, and for short put

$$k = \deg(R) \quad \text{and} \quad d = \sigma_1(R).$$

Identify H/H_{f+1} with a complete set of coset representatives of H_{f+1} in H. It can be assumed that the representative chosen from H_{f+1} is equal to 1_H, the identity of H. Let $(H/H_{f+1})^{\#} = H/H_{f+1} \setminus \{1_{H/H_{f+1}}\}$. We show next that there exists an even number $m \in \mathbb{N}$ such that

$$\forall x \in (H/H_{f+1})^{\#} \colon |R_{11} \cap H_{f+1}x| + |R_{22} \cap H_{f+1}x| = m. \tag{6.4}$$

Let

$$b_x := |R_{11} \cap H_{f+1}x| + |R_{22} \cap H_{f+1}x|, \quad x \in H/H_{f+1},$$

and define the element β in $\mathbb{Q}[H/H_{f+1}]$ as $\beta := \sum_{x \in H/H_{f+1}} b_x x$. By the definition of f, $\chi_i(\mathrm{Tr}(\underline{R})) = 2d$ whenever $i > 0$ and $p^{f+1} \mid i$. One can deduce from this that $\chi(\beta) = 2d$ for each nonprincipal $\chi \in \mathsf{Irr}(H/H_{f+1})$. This is equivalent to the existence of an $m \in \mathbb{N}_0$ such that

$$b_{1_{H/H_{f+1}}} = m + 2d \quad \text{and} \quad \forall x \in (H/H_{f+1})^{\#} \colon b_x = m.$$

Then $2|R_{11}| = |R_{11}| + |R_{22}| = p^{e-f-1}m + 2d$; hence m must be an even number. It remains to show that $m \neq 0$. Otherwise, $2d = \chi_{p^{e-1}}(\mathrm{Tr}(R)) = |R_{11}| + |R_{22}| = \chi_0(\mathrm{Tr}(R)) = k + d$, $k = d$ implying $\sigma_0(R) = \sigma_1(R)$, which is impossible since $\mathfrak{X}$ is a primitive scheme.

We show next that $m \geq 2p^f$. By the definition of f, $m_{\rho_{p^f}\sigma_1} < 2$; hence P_f fixes each irrep σ_i, and so all ρ_i, and we have that

$$\forall i \in [p^e - 1], \forall x \in P_f \colon \chi_i(\mathrm{Tr}(R)^{(x)}) = \chi_i(\mathrm{Tr}(R)).$$

From this $\mathrm{Tr}(R)^{(P_f)} = \mathrm{Tr}(R)$. Note that P_{f+1}, and hence P_f, acts trivially on H/H_{f+1}. So, if $x \in H \setminus H_{e-1}$, then P_f acts fixed-point-freely on $H_{f+1}x$. This gives $p^f \mid m$, and as $m > 0$ and being even, $m \geq 2p^f$ as required. Putting this into (6.4), one obtains that

$$\begin{aligned} a_{e-1}(R) &= \frac{|R_{11} \cap (H \setminus H_{e-1})| + |R_{22} \cap (H \setminus H_{e-1})|}{p^{e-1}(p-1)} \\ &= \frac{p^{e-f-2}(p-1)m}{p^{e-1}(p-1)} \geq \frac{2}{p}. \end{aligned}$$

The lemma is proved. □

Lemma 6.2. *For every $R \in \mathcal{R}$ and $i \in [e-1] \setminus \{0\}$, $a_i(R) \in \{0,1,2\}$, and we have that*

$$\mathrm{Tr}(R) = \underline{A} + 2\,\underline{B} + \sum_{i=1}^{e-1} a_i(R)\,\underline{H_{i+1} \setminus H_i}$$

with suitable $A, B \in H_1^{\#} = H_1 \setminus \{1_H\}$, $A \cap B = \emptyset$.

Proof. For short, put $k = \deg(R)$ and $d = \sigma_1(\underline{R})$. For $i \in [e-1]$, let us fix an orbit C_i of the subgroup $Q_{p-1} \leq \mathbb{Z}_n^*$ which is contained in $H_{i+1} \setminus H_i$. It is clear that, for every $i \in [e-1]$, the mapping

$$C_i \to H_1^{\#}, \quad x \mapsto x^{p^i} \quad (x \in C_i) \tag{6.5}$$

is a bijection.

$\mathrm{Tr}(R)^{(P_{e-1})} = \mathrm{Tr}(R)$; see Lemma 6.1. Hence $\mathrm{Tr}(R)$ can be written in the form

$$\mathrm{Tr}(R) = \sum_{i=0}^{n-1} \Big(\underline{A_i H_i} + 2\,\underline{B_i H_i} \Big), \tag{6.6}$$

where A_i and B_i are suitable subsets of $C_i^{\#}$ with $A_i \cap B_i = \emptyset$. The lemma is equivalent to showing that

$$\forall i \in [e-1] \setminus \{0\}\colon\ (A_i, B_i) \in \big\{ (\emptyset,\emptyset), (C_i^{\#},\emptyset), (\emptyset, C_i^{\#}) \big\}.$$

In fact, $a_i(R) = 0/1/2$ corresponds to the cases $(A_i,B_i) = (\emptyset,\emptyset)/(C_i^{\#},\emptyset)/(\emptyset,C_i^{\#})$, resp. The above possibilities for the pairs (A_i, B_i) will follow from showing that

$$\forall i \in [e-1] \setminus \{0\}\colon\ \chi_{p^i}(\underline{A_i} + 2\underline{B_i}) \in \mathbb{Q}. \tag{6.7}$$

To see this, let $\psi \in \mathsf{Irr}(H_1)$ be defined by

$$\psi(h^{p^{n-1}j}) = \chi_1(h^{p^{n-1}j}), \quad j \in [p-1].$$

Now, if $i \in [e-1] \setminus \{0\}$, then $\chi_{p^i}(\underline{A_i} + 2\underline{B_i}) = \psi(\underline{A_i^{(p^i)}} + 2\underline{B_i^{(p^i)}})$. In view of (6.5), this is in $\mathbb{Q}$ if and only if $(A_i^{(p^i)}, B_i^{(p^i)}) \in \big\{ (\emptyset,\emptyset), (H_1^{\#},\emptyset), (\emptyset, H_1^{\#}) \big\}$. This yields the required possibilities for (A_i, B_i).

For our later convenience, let us introduce the numbers $b_i(R)$ as:

$$b_i(R) = \sum_{j=0}^{i} \big(p^j |A_j| + 2p^j |B_j| \big), \quad i \in [e-1].$$

For ease of notation, let us write a_i and b_i for $a_i(R)$ and $b_i(R)$, resp. It is easy to see that these are related as

$$b_i = b_0 + (p-1) \sum_{j=1}^{i} p^j a_j, \quad i \in [e-1] \setminus \{0\}. \tag{6.8}$$

Fix an $i \in [n-1] \setminus \{0\}$. The possibilities according to the value m_i are discussed separately.

Case 1 ($m_i = 0$).

There exist $u, v \in [p^e - 1]$ with $\gcd(u,p) = \gcd(v,p) = 1$ such that $\chi_{p^i}(\mathrm{Tr}(R)) = \chi_u(\mathrm{Tr}(R)) + \chi_v(\mathrm{Tr}(R)) - 2d$. Using (6.6), this becomes

$$b_{i-1} + p^i \psi\big(\underline{A_i^{(p^i)}} + 2\,\underline{B_i^{(p^i)}} \big) = \psi\big(\underline{A_0}^{(u)} + 2\,\underline{B_0}^{(u)} + \underline{A_0}^{(v)} + 2\,\underline{B_0}^{(v)} \big) - 2d.$$

Thus ψ vanishes at the $\mathbb{Q}[H_1]$-element

$$(b_{i-1}+2d)\,\underline{1}+p^i\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)-\underline{A_0}^{(u)}-2\,\underline{B_0}^{(u)}-\underline{A_0}^{(v)}-2\,\underline{B_0}^{(v)}.$$

From this,

$$p^i\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)-\underline{A_0}^{(u)}-2\,\underline{B_0}^{(u)}-\underline{A_0}^{(v)}-2\,\underline{B_0}^{(v)}=(b_{i-1}+2d)\,\underline{H_1^{\#}};$$

hence

$$\underline{A_0}^{(u)}+2\,\underline{B_0}^{(u)}+\underline{A_0}^{(v)}+2\,\underline{B_0}^{(v)}\equiv(b_{i-1}+2d)\,\underline{H_1^{\#}}\pmod{p^i}.$$

From $A_0\cap B_0=\emptyset$ it follows that the largest coefficient appearing on the left side is at most 4. Thus it is easy to see that each coefficient has to be the same if $p^i>3$. If $p^i=3$, then the same conclusion can be drawn after a direct case analysis on all possible A_0, B_0. Summing up, we have that

$$\underline{A_0}^{(u)}+2\,\underline{B_0}^{(u)}+\underline{A_0}^{(v)}+2\,\underline{B_0}^{(v)}=\frac{2b_0}{p-1}\,\underline{H_1^{\#}}.$$

From this,

$$p^i\psi\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)=-\frac{2b_0}{p-1}-2d-b_{i-1},\tag{6.9}$$

and hence (6.7) holds.

Case 2 ($m_i=1$).

There exists $u\in[p^e-1]$ with $\gcd(u,p)=1$ such that $\chi_{p^i}(\mathrm{Tr}(R))=\chi_u(\mathrm{Tr}(R))$. This, by (6.6), yields the equation

$$b_{i-1}+p^i\psi\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)=\psi\big(\underline{A_0}^{(u)}+2\,\underline{B_0}^{(u)}\big).$$

Now, ψ vanishes at the $\mathbb{Q}[H_1]$-element $b_{i-1}\,\underline{1}+p^i\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)-\underline{A_0}^{(u)}-2\,\underline{B_0}^{(u)}$; hence

$$p^i\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)-\underline{A_0}^{(u)}-2\,\underline{B_0}^{(u)}=b_{i-1}\,\underline{H_1^{\#}}.$$

Similarly to Case 1, one obtains that $\underline{A_0}^{(u)}+2\,\underline{B_0}^{(u)}=\frac{b_0}{p-1}\,\underline{H_1^{\#}}$, and from this that

$$p^i\psi\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)=-\frac{b_0}{p-1}-b_{i-1};\tag{6.10}$$

hence (6.7) holds.

Case 3 ($m_i=2$).

Then $\chi_{p^i}(\mathrm{Tr}(R))=2d$, and by (6.6),

$$p^i\psi\big(\underline{A_i^{(p^i)}}+2\,\underline{B_i^{(p^i)}}\big)=2d-b_{i-1};\tag{6.11}$$

that is, (6.7) holds also in this case. □

Observe that we obtain in the proof of Lemma 6.2 that $\psi(A_i^{(p^i)}+2B_i^{(p^i)})=-a_i$ for each $i\in[e-1]\setminus\{0\}$. Now, comparing (6.8) with (6.9)-(6.11), the following recursion follows.

Corollary 6.3. *With the notation of Lemma* 6.2*, if* $i \in [e-2]$*, then*

$$p^{i+1}a_{i+1} = \begin{cases} \frac{b_0(p+1)}{p-1} + 2d + (p-1)\sum_{j=1}^{i} p^j a_j, & \text{if } m_{i+1} = 0, \\ \frac{b_0 p}{p-1} + (p-1)\sum_{j=1}^{i} p^j a_j, & \text{if } m_{i+1} = 1, \\ b_0 - 2d + (p-1)\sum_{j=1}^{i} p^j a_j, & \text{if } m_{i+1} = 2. \end{cases} \tag{6.12}$$

Proof of Theorem 1.1 *for* $e > 1$. Let $\mathfrak{X} = (X, \mathcal{R})$ be a primitive, bicirculant association scheme on p^e points, $p > 2$ is a prime, and $e > 1$. One possibility is that $\mathfrak{X}$ is trivial. From now on it is assumed that $\mathfrak{X}$ is nontrivial, that is, of class at least 2. The argument is broken into a few steps.

(a) $f = e - 1$.

To the contrary assume that $f < e-1$, and choose an $R \in \mathcal{R}^{\#}$. Then $a_{e-1}(R) = \frac{2m}{p} > 0$ for some $m \in \mathbb{N}$; see the proof of Lemma 6.1. But also $a_{e-1}(R) \in \{0, 1, 2\}$, see Lemma 6.2, and therefore $a_{e-1}(R) = 2$. Using (6.1), $R = X^2 \setminus \Delta_X$, which is impossible.

(b) If $R \in \mathcal{R}^{\#}$*, then* $\frac{1}{2}(p-1) \mid b_0(R)$ *and* $b_0(R) > 0$.

As $f = e - 1$, $m_{e-1} < 2$. Then $\frac{1}{2}(p-1) \mid b_0(R)$ follows from (6.12). Assume that $b_0(R) = 0$. By (6.12), $a_i(R)$ are even for all $i > 0$, and hence $R_{1,1} = R_{2,2} = R_{1,1}^{-1}$. (X, R) is a graph with eigenvalues $\deg(R)$, $\sigma_1(R)$ and $-\sigma_1(R)$. (X, R) is a connected, regular graph; hence it is strongly regular. It is also a bicirculant graph on $2p^e$ points; therefore the sum of the two nontrivial eigenvalues must be -1 (Corollary 2.5), a contradiction.

(c) If $R \in \mathcal{R}^{\#}$ *with* $b_0(R) = \frac{1}{2}(p-1)$ *and* $a_1(R) < 2$*, then* $m_i = 0$ *and* $a_i(R) = 1$ *for all* $i > 0$.

Let $R = (\underline{R_{i,j}})$ in $\mathcal{A}$, and let $k = \deg(R)$, $d = \sigma_1(R)$. For short, let a_i and b_i be written for $a_i(R)$ and $b_i(R)$, resp.

Observe that $m_i \neq 1$ for all $i > 0$. Putting $\tilde{a}_i = 2a_i$ for $i \in [e-1]$, (6.12) reduces to

$$p^{i+1}\tilde{a}_{i+1} = \begin{cases} p + (4d+1) + (p-1)\sum_{j=1}^{i} p^j \tilde{a}_j, & \text{if } m_{i+1} = 0, \\ p - (4d+1) + (p-1)\sum_{j=1}^{i} p^j \tilde{a}_j, & \text{if } m_{i+1} = 2, \end{cases} \quad 0 \leq i \leq e-2.$$

We show that $m_i = m_1$ for all i. Otherwise, $m_1 = \cdots = m_k \neq m_{k+1}$ for some $1 \leq k \leq e-2$. Then

$$p^{k+1}\tilde{a}_{k+1} = 2p - p\tilde{a}_1 + (p-1)\sum_{j=1}^{k} p^j \tilde{a}_j.$$

Since $\tilde{a}_j = \tilde{a}_1$ for all $1 \leq j \leq k$, $p^k a_{k+1} = 1 + (p^k - 2)a_1$ follows. This is impossible if $a_1 < 2$. Therefore, we can conclude that $m_i = 0$ for all i, and hence $a_i = a_1$ for all $i > 0$. If $a_i = 0$ for all $i > 0$, then $|R_{11}| = \frac{1}{4}(p-1)$ and $d = -\frac{1}{4}(p+1)$. However, $|R_{12}| = |R_{11}| - d = \frac{p}{2}$, a contradiction. As $a_1 < 2$, $a_i = 1$ for all $i > 0$.

(d) $\mathfrak{X}$ *is of class* 2.

To the contrary assume that $|\mathcal{R}| > 3$. In view of (b) and (c), the following description of $\mathcal{R}$ can be derived:

$$\mathcal{R} = \{\Delta_X, R_1, R_2, R_3\},$$

where if $t = 1, 2$, then $b_0(R_t) = \frac{1}{2}(p-1)$, $a_i(R_t) = 1$ for all i, and $b_0(R_3) = p - 1$ and $a_i(R_3) = 0$ for all i. The irreps of $\mathcal{A}$ are $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ with the corresponding

degrees

$$f_0 = 1, \quad f_1 = p^e - p^{e-1} + 1, \quad f_2 = f_3 = p^{e-1} - 1 + \frac{1}{2}(p^e - p^{e-1}).$$

Observe that R_3 is symmetric; thus we have that

$$\sum_{i=0}^{3} f_i \sigma_i(R_3)^2 = \sum_{i=0}^{3} f_i \sigma_i(R_3^2) = \mathrm{Tr}(R_3^2) = \deg(R_3) 2p^e. \tag{6.13}$$

We calculate next the values $\sigma_i(R_3)$. It is immediate to find that

$$\sigma_0(R_3) = \frac{1}{2}(p-1) + p \quad \text{and} \quad \sigma_1(R_3) = -\frac{1}{2}(p+1). \tag{6.14}$$

We may assume that $\rho_1 = \sigma_1 + \sigma_2$. The stabilizer $(\mathbb{Z}_{p^e}^*)_{\sigma_2}$ in the action of $\mathbb{Z}_{p^e}^*$ on the set of irreps is the unique subgroup $K \leq \mathbb{Z}_{p^e}^*$ of index 2. Thus

$$K = \{\, x \in \mathbb{Z}_{p^e}^* \mid \chi_1(\mathrm{Tr}(R_3)^{(x)}) = \chi_1(\mathrm{Tr}(R_3)) \,\}.$$

By Lemma 6.2,

$$\mathrm{Tr}(R_3) = \underline{A} + 2\underline{B}, \quad A, B \subset H_1^{\#} \text{ and } A \cap B = \emptyset.$$

Therefore,

$$K = \{\, x \in \mathbb{Z}_{p^e}^*) \mid \psi(\underline{A^{(x)}} + 2\underline{B^{(x)}}) = \psi(\underline{A} + 2\underline{B}) \,\}.$$

Using also that $|A| + 2|B| = b_0(R_3) = p - 1$, we obtain that $A = \emptyset$, and either B or $H_1^{\#} \setminus B$ is equal to $\bigcup_{x \in K} h^{p^{e-1}x} = \bigcup_{x \in Q_{(p-1)/2}} h^{p^{e-1}x}$. Since $B = B^{-1}$, $p \equiv 1 \pmod 4$. Then we have the Gauss sum

$$\sum_{x \in Q_{(p-1)/2}} \psi(h^{p^{e-1}x}) = \frac{1}{2}(\sqrt{p} - 1).$$

From this, $\sigma_2(R_3) = \sqrt{p} + \frac{1}{2}(p-1)$ or $\sigma_2(R_3) = -\sqrt{p} + \frac{1}{2}(p-1)$, and we can conclude that

$$\{\, \sigma_2(R_3), \sigma_3(R_3) \,\} = \{\, \pm\sqrt{p} + \frac{1}{2}(p-1) \,\}. \tag{6.15}$$

Plugging (6.14) and (6.15) into (6.13), one obtains that

$$-4 + 4p + p^{e-1} + 2p^e + p^{e+1} = 2p^{e-1}(3p-1).$$

This is impossible for any odd prime p, and by this (d) is proved.

(e) $2p^e = (2s+1)^2 + 1$, *the degrees of basic digraphs of* $\mathfrak{X}$ *are* 1, $s(2s+1)$, $(s+1)(2s+1)$, *and the degrees of irreps of* $\mathfrak{X}$ *are* 1, p^e, $p^{e-1} - 1$.

$\mathfrak{X}$ is of class 2. The basic digraphs (X, R), $R \neq \Delta_X$, are complementary strongly regular bicirculant graphs; hence their degrees follow from Theorem 2.4. The degrees of irreps of $\mathfrak{X}$ are equal to the multiplicities of eigenvalues of the digraphs (X, R). These are 1, p^e and $p^e - 1$. By this (e) is proved, and the proof of Theorem 1.1 for $e > 1$ is completed. □

Acknowledgments

A visit of the first author at Netanya Academic College in November 2006 helped us to proceed with the paper. The first author thanks grant OTKA T-043758 and also Netanya Academic College for supporting his trip. The third author was supported by the University of Primorska during his visit in September 2006.

The authors would like to thank the anonymous referee for valuable remarks and R. Guralnick for providing an outline of a classification of primitive permutation groups of degree $2p^e$, where $p > 2$ is a prime.

References

[1] E. Bannai and T. Ito, *Algebraic combinatorics I: Association schemes*, W. A. Benjamin, Menlo Park, CA, 1984. MR882540 (87m:05001)

[2] R. C. Bose and T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc. **47** (1952), 151-184. MR0048772 (14:67b)

[3] A. E. Brouwer, A. E. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, 1989. MR1002568 (90e:05001)

[4] C. W. Curtis and I. Reiner, *"Representation theory of finite groups and associative algebras",* John Wiley & Sons, New York, London, 1962. MR0144979 (26:2519)

[5] I. A. Faradžev, M. H. Klin and M. E. Muzychuk, *Cellular rings and automorphism groups of graphs In: Investigations on Algebraic Theory of Combinatorial Objects*, Mathematics and its Applications (Soviet Series), v. **84**, I. A. Faradev, A. A. Ivanov, M. H. Klin, A. J. Woldar (Eds.), Kluwer Acad. Publ., 1994. MR1273366 (95a:05049)

[6] R. Guralnick, *Private communication,* 2008.

[7] N. Ito, *On transitive simple permutation groups of degree* $2p$, Math. Z. **178** (1962), 453–468. MR0140564 (25:3982)

[8] N. Ito, *On uniprimitive groups of degree* $2p$, Math. Z. **102** (1967), 238–244. MR0219602 (36:2681)

[9] N. Ito and W. Tomoyuki, *A note on transitive permutation groups of degree* $2p$, Tensor (N.S.) **26** (1972), 105–106. MR0330271 (48:8608)

[10] I. Kovács, A. Malnič, D. Marušič and Š. Miklavič, *Transitive group actions: (Im)primitivity and semiregular subgroups*, submitted paper.

[11] W. Knapp, *On Burnside's Method,* J. Algebra **175** (1995), 644-660. MR1339661 (96i:20002)

[12] K. H. Leung and S. L. Ma, *Partial difference triples*, J. Algebr. Combin. **2** (1993), 397-409. MR1241508 (94h:05099)

[13] M.W. Liebeck and J. Saxl, *The finite primitive permutation groups of rank three,* Bull. London Math. Soc. **18** (1986), 165-172. MR818821 (87i:20007)

[14] A. Malnič, D. Marušič and P. Šparl, *On strongly regular bicirculants*, Europ. J. Combin. **28** (2007), 891-900. MR2300769 (2007m:05121)

[15] D. Marušič, *Strongly regular bicirculants and tricirculants*, Ars Combin. **25C** (1988), 11-15. MR943371 (89e:05105)

[16] P. Müller, *Permutation Groups with a Cyclic Two-Orbits Subgroup and Monodromy Groups of Siegel Functions*, http://arxiv.org/PS-cache/math/pdf/0110/0110060v1.pdf

[17] M. J. de Resmini and D. Jungnickel, *Strongly regular semi-Cayley graphs*, J. Algebr. Combin. **1** (1992), 171-195. MR1226350 (94d:05150)

[18] L. L. Scott, *On primitive permutation groups of degree* $2p$, Math. Z. **126** (1972), 227–229. MR0346034 (49:10760)

[19] L. L. Scott, *Estimates in permutation groups*, Geom. Dedicata **5** (1976), 219-227. MR0424911 (54:12869)

[20] W. R. Scott, *Group Theory*, Dover Publications, New York, 1987. MR896269 (88d:20001)

[21] H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen II,* Math. Z. **52** (1949), 384-393. MR0033817 (11:495a)

[22] H. Wielandt, *"Finite Permutation Groups",* Academic Press, New York, 1964. MR0183775 (32:1252)

[23] H. Wielandt, *Primitive Permutationsgruppen vom Grad* $2p$, Math. Z. **63** (1956), 478-485. MR0075200 (17:708c)
[24] P. H. Zieschang, *"An algebraic approach to association schemes"*, Lecture Notes in Math., Vol. 1628, Springer-Verlag, New York/Berlin, 1996. MR1439253 (98h:05185)

FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia
E-mail address: kovacs@pef.upr.si

IMFM, University of Ljubljana, Jadranska 19, 1000 Ljubljana, Slovenia – and – FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia
E-mail address: dragan.marusic@guest.arnes.si

Department of Computer Science and Mathematics, Netanya Academic College, 1 University St., 42365 Netanya, Israel
E-mail address: muzy@netanya.ac.il