Michigan Math. J. 58 (2009)

On Generalized Paley Graphs and Their Automorphism Groups

Tian Khoon Lim & Cheryl E. Praeger

Dedicated to the memory of Donald G. Higman

1. Introduction

The generalized Paley graphs are, as their name suggests, a generalization of the Paley graphs, first defined by Paley in 1933 (see [15]). They arise as the relation graphs of symmetric cyclotomic association schemes. However, their automorphism groups may be much larger than the groups of the corresponding schemes. We determine the parameters for which the graphs are connected, or equivalently, the schemes are primitive. Also we prove that generalized Paley graphs are sometimes isomorphic to Hamming graphs and consequently have large automorphism groups, and we determine precisely the parameters for this to occur. We prove that in the connected, non-Hamming case, the automorphism group of a generalized Paley graph is a primitive group of affine type, and we find sufficient conditions under which the group is equal to the one-dimensional affine group of the associated cyclotomic association scheme. The results have been applied in [11] to distinguish between cyclotomic schemes and similar twisted versions of these schemes in the context of homogeneous factorizations of complete graphs.

Let $\mathbb{F}_q$ be a finite field with q elements such that $q \equiv 1 \pmod 4$. Let ω be a primitive element in $\mathbb{F}_q$ and S the set of nonzero squares in $\mathbb{F}_q$, so $S = \{\omega^2, \omega^4, \dots, \omega^{q-1} = 1\} = -S$. The *Paley graph,* denoted by Paley(q), is the graph with vertex set $\mathbb{F}_q$ and edges all pairs $\{x, y\}$ such that $x - y \in S$. The class of Paley graphs is one of the two infinite families of self-complementary arc-transitive graphs characterized by Peisert in [16]. Moreover, Paley graphs are also examples of distance-transitive graphs, of strongly regular graphs, and of conference graphs; see [8, Sec. 10.3]. The automorphism group Aut(Paley(q)) of Paley(q) is of index 2 in the affine group $\mathrm{A\Gamma L}(1,q)$, and each permutation in $\mathrm{A\Gamma L}(1,q) \setminus \mathrm{Aut}(\mathrm{Paley}(q))$ interchanges Paley(q) and its complementary graph. The generalized Paley graphs are defined similarly.

Definition 1.1 (Generalized Paley graph). Let $\mathbb{F}_q$ be a finite field of order q, and let k be a divisor of $q-1$ such that $k \geq 2$; and if q is odd, then in addition $\frac{q-1}{k}$ is even. Let S be the subgroup of order $\frac{q-1}{k}$ of the multiplicative group $\mathbb{F}_q^*$. Then the *generalized Paley graph* GPaley$\left(q, \frac{q-1}{k}\right)$ of $\mathbb{F}_q$ is the graph with vertex set $\mathbb{F}_q$ and edges all pairs $\{x, y\}$ such that $x - y \in S$.

Received December 14, 2006. Revision received June 29, 2007.

The generalized Paley graphs $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ are the relation graphs of the symmetric cyclotomic association scheme $\mathrm{Cyc}(q,k)$ defined in Section 1.1. They also arise as the factors of cyclotomic homogeneous factorizations of complete graphs [11, Thm. 1.1]. Our main theorem determines precise conditions under which $\mathrm{Cyc}(q,k)$ is primitive (defined in Section 1.1) and shows how the automorphism group of a generalized Paley graph depends heavily on the parameters k and q.

Theorem 1.2. *Let $V = \mathbb{F}_q$, where $q = p^R$ with p a prime, and let $k \mid (q-1)$ be such that $k > 1$ and either q is even or $\frac{q-1}{k}$ is even. Let $\mathrm{Cyc}(q,k)$ be a k-class symmetric cyclotomic scheme with relation graphs $\Gamma_1, \dots, \Gamma_k$, and let $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$. Then $\Gamma_i \cong \Gamma$ for each i, and the following statements hold.*

(1) *$\mathrm{Cyc}(q,k)$ is primitive if and only if k is not a multiple of $\frac{q-1}{p^a-1}$ for any proper divisor a of R.*
(2) *Γ is a Hamming graph if and only if $k = \frac{a(q-1)}{R(p^a-1)}$ for some proper divisor a of R.*
(3) *If Γ is connected and is not a Hamming graph, then $\mathrm{Aut}(\Gamma)$ is a primitive subgroup of $\mathrm{AGL}(R,p)$ containing the group of translations $\mathbb{Z}_p^R$.*
(4) *If k divides $p-1$, then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathrm{Cyc}(q,k)) < \mathrm{A\Gamma L}(1,q)$.*

Commentary on the significance and consequences of this result is given in Section 1.2. In particular, Hamming graphs and their automorphism groups are discussed there. The theorem may be contrasted with McConnel's theorem [14], proved in 1963, that the automorphism group of $\mathrm{Cyc}(q,k)$ (the intersection of the automorphism groups of its relation graphs) is always a subgroup of $\mathrm{A\Gamma L}(1,q)$.

1.1. Cyclotomic Association Schemes and Cyclotomic Factorizations

Here we describe briefly the relationship between generalized Paley graphs, symmetric cyclotomic association schemes, and cyclotomic homogeneous factorizations of complete graphs. Symmetric association schemes are defined as follows.

Definition 1.3 [4, p. 43]. A *symmetric k-class association scheme* is a pair $(V, \mathcal{R})$ such that:

(1) $\mathcal{R} = \{R_0, R_1, \dots, R_k\}$ is a partition of $V \times V$;
(2) $R_0 = \{(x,x) \mid x \in V\}$;
(3) $R_i = R_i^T$ (i.e., $(x,y) \in R_i$ implies $(y,x) \in R_i$) for all $i \in \{0,1,\dots,k\}$;
(4) there are constants p_{ij}^h (called the *intersection numbers* of the scheme) such that, for any pair $(x,y) \in R_h$, the number of elements $z \in V$ with $(x,z) \in R_i$ and $(z,y) \in R_j$ equals p_{ij}^h.

For each $i \geq 1$, the class R_i corresponds to the undirected graph $\Gamma_i = (V, E_i)$, where $E_i = \{\{x,y\} \mid (x,y) \in R_i\}$ (see e.g. [7, Chap. 12]). These graphs are called the *relation graphs* of the scheme and are not in general isomorphic. The scheme is said to be *primitive* if each of the Γ_i is connected, and otherwise it is called *imprimitive*. The automorphism group $\mathrm{Aut}(V, \mathcal{R})$ is the largest subgroup of $\mathrm{Sym}(V)$

that, in its natural action on $V \times V$, fixes each of the relations $R_1, \dots, R_k$ setwise; that is to say, $\mathrm{Aut}(V, \mathcal{R}) = \bigcap_{i=1}^{k} \mathrm{Aut}(\Gamma_i)$. The edge sets of the Γ_i form a partition $\mathcal{E} = \{E_1, \dots, E_k\}$ of the edge set of the complete graph K_n, where $|V| = n$, and hence the relation graphs form a factorization of K_n. If the subgroup of $\mathrm{Sym}(V)$ fixing $\mathcal{R}$ setwise permutes transitively the set $\{\Gamma_1, \dots, \Gamma_k\}$ and if $\mathrm{Aut}(V, \mathcal{R})$ is transitive on V, then the factorization is called *homogeneous.* In particular, in this case the relation graphs Γ_i are pairwise isomorphic.

Let $V = \mathbb{F}_q$, let $k | (q-1)$ be such that $k > 1$ and either q is even or $\frac{q-1}{k}$ is even, and let $S(k) = \langle \omega^k \rangle \subseteq V^* = \mathbb{F}_q^*$ (the multiplicative group of $\mathbb{F}_q$). Then the *k-class symmetric cyclotomic scheme* $\mathrm{Cyc}(q,k) = (V, \mathcal{R})$ has $R_i = \{(x,y) \mid y - x \in S(k)\omega^i\}$ for $1 \le i \le k$. Note that condition (3) of Definition 1.3 holds since $-1 \in S(k)$. Also, the relation graph Γ_k is the generalized Paley graph of $\mathbb{F}_q$ relative to $S(k)$, and in particular if $k = 2$ then Γ_2 is the Paley graph of $\mathbb{F}_q$ (see [4, p. 66]). Moreover, the affine group $\mathrm{AGL}(1,q)$ fixes $\mathcal{R}$ setwise and permutes the relation graphs transitively, and $\mathrm{Aut}(\mathrm{Cyc}(q,k)) = \bigcap_{i-1}^{k} \mathrm{Aut}(\Gamma_i)$ contains the group of translations that is transitive on V. Thus the relation graphs for $\mathrm{Cyc}(q,k)$ form a homogeneous factorization of K_q called a *cyclotomic factorization.* In particular, all of the relation graphs are isomorphic to $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$, and $\mathrm{Aut}\big(\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)\big)$ contains the subgroup of $\mathrm{AGL}(1,q)$ of order $q\frac{q-1}{k}$ acting arc-transitively.

1.2. Commentary on Theorem 1.2: Automorphism Groups of Graphs and Schemes

In 1963, McConnel [14] proved that the full automorphism group of $\mathrm{Cyc}(q,k)$ is a subgroup of $\mathrm{A\Gamma L}(1,q)$. However, the automorphism groups of the relation graphs of $\mathrm{Cyc}(q,k)$, that is, of the generalized Paley graphs $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$, may be much larger. This paper initiates a study of these automorphism groups for various ranges of values of the parameters q and k.

The “easiest” way for the automorphism group of $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ to be larger is if the graph is not connected. Since all the relation graphs of $\mathrm{Cyc}(q,k)$ are isomorphic to $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$, it follows that $\mathrm{Cyc}(q,k)$ is primitive if and only if $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected. We determine in Theorem 1.2(1) the precise parameter values for $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ to be connected or, equivalently, for $\mathrm{Cyc}(q,k)$ to be primitive. In Theorem 2.2, a more detailed version of this result, we also prove that, if $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is disconnected, then its connected components are generalized Paley graphs over a proper subfield and generate a cyclotomic scheme over this subfield.

Suppose now that $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected. It is possible for $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ to be a Hamming graph, for certain q and k, and hence have a large automorphism group. For positive integers $a > 1$ and $b > 1$, the *Hamming graph* $H(a,b)$ has as vertices all b-tuples with entries from a set Δ of size a. Two vertices are adjacent in $H(a,b)$ if and only if the two b-tuples differ in exactly one entry. The full automorphism group of $H(a,b)$ is the wreath product $S_a \wr S_b$ in its product action on

Δ^b; see [4, Thm. 9.2.1]. Section 2 contains details about the product action. We determine in Theorem 1.2(2) the precise parameter values for $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ to be a Hamming graph.

Moreover we prove, in Theorem 1.2(3), that if $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected and not a Hamming graph, then its automorphism group is a primitive group of affine type. Although this gives a lot of information about the group, it does not determine it completely. In a special case that is relevant to our work on homogeneous factorizations in [11], we were able to show that the automorphism group of $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is indeed equal to the automorphism group of $\mathrm{Cyc}(q, k)$ (and no larger); see Theorem 1.2(4).

We make additional detailed comments about Theorem 1.2 and its consequences in Remark 1.4.

REMARK 1.4. (a) The graph $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is a Cayley graph for the translation subgroup T of $\mathrm{A\Gamma L}(1, q)$; see Section 2.2. Theorem 1.2(3) proves that, if $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected and not a Hamming graph, then it is a *normal Cayley graph*—that is, the translation subgroup T of automorphisms is normal in the full automorphism group.

(b) The condition $k \mid (p-1)$ holds in particular if $q = p$ (i.e., if $R = 1$). In this case, Theorem 1.2(4) follows from an old result of Burnside about primitive permutation groups of prime degree; see [20, 11.7].

(c) The proof of Theorem 1.2(3) uses results from [17; 18], and that of Theorem 1.2(4) depends heavily on results in [9]. Because the results used from these papers rely on the classification of the simple groups, these two parts of Theorem 1.2 also rely on that classification.

(d) Apart from the possibilities that $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ may be disconnected or isomorphic to a Hamming graph, which are dealt with in parts (1) and (2) of Theorem 1.2, there are other cases where $\mathrm{Aut}\big(\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)\big)$ is not a one-dimensional affine group. In Example 1.6, we give an explicit example. Thus, despite our identifying the disconnected and Hamming cases precisely in Theorem 1.2, there remain some mysteries to be solved concerning generalized Paley graphs: Problem 1.5 is still largely open.

(e) Our interest in generalized Paley graphs arose from our study of homogeneous factorizations of complete graphs (see Section 1.1). These factorizations were introduced in [12] as a generalization of vertex-transitive self-complementary graphs. Our study in [11] gave a classification of arc-transitive homogeneous factorizations of complete graphs. In addition to the cyclotomic factorizations, we discovered a new family of examples that generalize an infinite family of vertex-transitive self-complementary graphs constructed and characterized by Peisert [16]. They may be viewed as a twisted version of cyclotomic factorizations. Using Theorem 1.2(4), we proved in [11] that factor graphs in these two homogeneous factorizations, with the same parameters q and k, were nonisomorphic; we showed that their automorphism groups had nonisomorphic intersections with $\mathrm{A\Gamma L}(1, q)$.

Problem 1.5. Determine the precise conditions on k and p^R under which the conclusion of Theorem 1.2(4) holds.

Example 1.6. Take $R = 4$, $p = 3$, and $k = 4$, so that $\frac{p^R-1}{k} = 20$, and let $\Gamma = \mathrm{GPaley}(81, 20)$. Then $k \neq \frac{a(p^R-1)}{R(p^a-1)}$, and k is not a multiple of $\frac{q-1}{p^a-1}$, for any proper divisor a of R. Hence, by Theorem 1.2, Γ is connected and not a Hamming graph, and $\mathrm{Aut}(\Gamma)$ is a primitive subgroup of $\mathrm{AGL}(4, 3)$. Using Magma [3], we computed $\mathrm{Aut}(\Gamma)$. Its order is $|\mathrm{Aut}(\Gamma)| = 233280$, greater than $|\mathrm{A\Gamma L}(1, 81)| = 25920$. Thus $\mathrm{Aut}(\Gamma)$ is not contained in the one-dimensional affine group. A further check using Magma showed that a point-stabilizer A_0 of $A := \mathrm{Aut}(\Gamma)$, which has order 2880, contains a normal subgroup B isomorphic to A_6, and $A_0/B \cong D_8$, so $\mathrm{Aut}(\Gamma) = Z_3^4 \rtimes (A_6 \cdot D_8)$.

In Section 2, we introduce some terminology and definitions needed for subsequent results and we prove Theorem 1.2(1). We prove parts (2), (3), and (4) of Theorem 1.2 in Sections 3, 4, and 5, respectively.

2. Preliminaries and Proof of Theorem 1.2(1)

2.1. Cayley Graphs

All graphs considered are finite, undirected, and without loops or multiple edges. Thus a graph $\Gamma = (V, E)$ consists of a vertex set V and a subset E of unordered pairs from V, called the *edge set*. An arc is an ordered pair (u, v) where $\{u, v\}$ is an edge. The generalized Paley graphs belong to a larger class of graphs called the Cayley graphs, defined as follows.

Definition 2.1 (Cayley graph). For a group K and a nonempty subset H of K such that $1_K \notin H$ and $H = H^{-1} = \{h^{-1} \mid h \in H\}$, the *Cayley graph* $\Gamma = \mathrm{Cay}(K, H)$ of K relative to H is the graph with vertex set K such that $\{x, y\}$ is an edge if and only if $xy^{-1} \in H$.

A Cayley graph $\Gamma = \mathrm{Cay}(K, H)$ is connected if and only if $\langle H\rangle = K$. Furthermore, if $\Gamma = \mathrm{Cay}(K, H)$ is disconnected, then each connected component is isomorphic to $\mathrm{Cay}(\langle H\rangle, H)$ and the number of connected components equals $\frac{|K|}{|\langle H\rangle|}$. A permutation group G on V is *semiregular* if the only element fixing a point in V is the identity element of G; and G is *regular* on V if it is both semiregular and transitive. In Definition 2.1, the group K acts regularly on vertices by $y\colon x \to xy$ for $x, y \in K$. Conversely (see [2, Lemma 16.3]), a graph Γ is isomorphic to a Cayley graph for some group if and only if $\mathrm{Aut}(\Gamma)$ has a subgroup that is regular on vertices.

2.2. Generalized Paley Graphs as Cayley Graphs

It follows from Definition 1.1 that

$$\mathrm{GPaley}\left(q, \frac{q-1}{k}\right) = \mathrm{Cay}(V, S),$$

where V is the additive group of the field $\mathbb{F}_q$ and S is the unique subgroup of order $\frac{q-1}{k}$ of the multiplicative group $\mathbb{F}_q^*$. Let ω be a primitive element of $\mathbb{F}_q$. Then $S = \langle \omega^k \rangle$. Thus $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ admits the additive group of $\mathbb{F}_q$ acting regularly by $t_y \colon x \to x + y$ (for $x, y \in \mathbb{F}_q$) as a subgroup of automorphisms. To distinguish this subgroup from the vertex set V, we denote it by $T = \{t_y \mid y \in \mathbb{F}_q\}$ and call it the *translation group* of $\mathrm{A\Gamma L}(1,q)$.

Now $T \cong \mathbb{Z}_p^R$, where $q = p^R$ with p prime, and T is the unique minimal normal subgroup of $\mathrm{A\Gamma L}(1,q)$. Let $\hat{\omega}$ denote the scalar multiplication map $\hat{\omega} \colon x \to x\omega$ (for all $x \in \mathbb{F}_q$) corresponding to the primitive element ω, and let α denote the Frobenius automorphism of $\mathbb{F}_q$; that is, $\alpha \colon x \to x^p$. Then $\mathrm{A\Gamma L}(1,q) = T \rtimes \langle \hat{\omega}, \alpha \rangle$, and the one-dimensional general semilinear group $\Gamma\mathrm{L}(1,q) = \langle \hat{\omega}, \alpha \rangle$. Now both $\hat{\omega}^k$ and α fix $\mathbf{0}$ and fix S setwise; hence $T \rtimes \langle W, \alpha \rangle$ is a subgroup of automorphisms of $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$, where $W := \langle \hat{\omega}^k \rangle$. In fact, $T \rtimes W$ is arc-transitive, and W is transitive on $S = \{1, \omega^k, \omega^{2k}, \dots, \omega^{((q-1)/k)-k}\} = 1^W$. (For a permutation group K on V and a point $v \in V$, we denote by v^K the K-orbit $\{v^x \mid x \in K\}$ containing v.)

2.3. Hamming Graphs and Cayley Graphs

Let H be a group, b a positive integer, and K a subgroup of the symmetric group S_b. Then the *wreath product* $H \wr K$ is the semidirect product $H^b \rtimes K$ where elements of K act on H^b by permuting the "entries" of elements of H^b. That is, $(h_1, h_2, \dots, h_b)^{k^{-1}} = (h_{1^k}, h_{2^k}, \dots, h_{b^k})$ for all $(h_1, h_2, \dots, h_b) \in H^b$ and $k \in K$. Now suppose $H \le \mathrm{Sym}(\Delta)$. Then the *product action* of $H \wr K$ on Δ^b is defined as follows. Elements of H^b act coordinate-wise on Δ^b and elements of K permute the coordinates: for $(h_1, \dots, h_b) \in H^b$, $k \in K$, and $(\delta_1, \dots, \delta_b) \in \Delta^b$,

$$(\delta_1, \dots, \delta_b)^{(h_1, \dots, h_b)} = (\delta_1^{h_1}, \dots, \delta_b^{h_b}),$$

$$(\delta_1, \dots, \delta_b)^{k^{-1}} = (\delta_{1^k}, \dots, \delta_{b^k}).$$

If A is a regular subgroup of S_a, then $A^b < S_a \wr S_b$ and A^b acts regularly on the vertices of $H(a,b)$. Thus (see Section 2.1) $H(a,b)$ is a Cayley graph. If a is a prime power q, then A can be identified with the additive group of a finite field $\mathbb{F}_q$ and the vertex set of $H(a,b)$ can be identified with $\mathbb{F}_q^b$.

2.4. Primitive Permutation Groups

Let G be a transitive permutation group acting on a finite set V. A nonempty subset $\Delta \subseteq V$ is called a *block* for G if, for every $g \in G$, either $\Delta \cap \Delta^g = \emptyset$ or $\Delta = \Delta^g$. A block Δ is said to be *trivial* if $|\Delta| = 1$ or $\Delta = V$. Otherwise, Δ is called *nontrivial*. We say that the group G is *primitive* if the only blocks for G are the trivial ones.

The possible structures of finite primitive permutation groups up to permutational isomorphism are described by the O'Nan–Scott theorem (see e.g. [5; 13]). Here, we will briefly describe the three types of finite primitive permutation groups relevant to this paper (we refer readers to [5; 13] for further details about the remaining types).

A finite primitive permutation group G on V is of type HA (holomorph of an abelian group) if $G = T \rtimes G_0$ is a subgroup of an affine group $\mathrm{AGL}(R, p)$ on V, where $T \cong \mathbb{Z}_p^R$ is the (regular) group of translations (and we may identify V with $\mathbb{Z}_p^R$) and G_0 is an irreducible subgroup of $\mathrm{GL}(R, p)$. We often say that a primitive group of this type is of affine type. A primitive permutation group G is of type AS if G is an *almost simple group*—that is, if $N \le G \le \mathrm{Aut}(N)$, where N is a finite nonabelian simple group. Such a group can equivalently be defined as a primitive group G having a unique minimal normal subgroup N that is nonabelian and simple. Finally, a primitive permutation group G on V is of type PA (product action) if $V = \Delta^b$ and $N^b \le G \le H \wr S_b \le \mathrm{Sym}(\Delta) \wr S_b$ in its product action, where H is a primitive permutation group on Δ of type AS with simple normal subgroup N.

2.5. Proof of Theorem 1.2(1)

The following result relates the connectedness of Γ with the action of W on V, and Theorem 1.2(1) follows immediately from it.

THEOREM 2.2. *Let* $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big) = \mathrm{Cay}(V, S)$, *where* $V = \mathbb{F}_q$ *and* $S = \langle \omega^k \rangle$, *with* k *a divisor of* $q-1$ *such that* $k \ge 2$ *and either* q *or* $\frac{q-1}{k}$ *is even. Let* $q = p^R$ *with* p *prime, and let* $\mathrm{Cyc}(q,k) = (V, \mathcal{R})$.

(1) *The following are equivalent*:
   (i) Γ *is connected*;
   (ii) $\mathrm{Cyc}(q,k)$ *is primitive*;
   (iii) $\langle \hat{\omega}^k \rangle$ *acts irreducibly on* V;
   (iv) k *is not a multiple of* $\frac{q-1}{p^a-1}$ *for any proper divisor* a *of* R.

(2) *Suppose that* k *is a multiple of* $\frac{q-1}{p^a-1}$, *where* a *divides* R, *so that* Γ *is not connected. Then the connected components of* Γ *are all isomorphic, and the component* Γ_0 *containing* $\mathbf{0}$ *has vertex set* $\mathbb{F}_{p^a}$ *(a proper subfield of* $\mathbb{F}_q$*) containing* S *and is isomorphic to* $\mathrm{GPaley}\big(p^a, \frac{p^a-1}{k'}\big)$, *where* $k' = \frac{p^a-1}{q-1}k \ge 1$. *Furthermore,* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_0) \wr S_{p^{R-a}}$.

We note that, in part (2), k' may equal 1. When this happens we still use the notation $\mathrm{GPaley}\big(p^a, \frac{p^a-1}{k'}\big)$ for Γ_0 even though in this case $\Gamma_0 = \mathrm{Cay}(\mathbb{F}_{p^a}, S) \cong K_{p^a}$, the complete graph on p^a vertices.

Proof of Theorem 2.2. (1) The equivalence of parts (i) and (ii) follows from our discussion in Section 1.1. Let U be the $\mathbb{F}_p$-span of S; that is, $U = \big\{\sum_{\omega^{ik} \in S} \lambda_i \omega^{ik} \mid \lambda_i \in \mathbb{F}_p\big\}$. Since $W = \langle \hat{\omega}^k \rangle$ leaves S invariant, it also leaves invariant the $\mathbb{F}_p$-span U of S. Also we note that Γ is connected if and only if $U = V$ (see Definition 2.1).

Suppose W acts irreducibly on V. Then, since U is W-invariant and nonzero, $U = V$ and hence Γ is connected. Conversely, suppose Γ is connected. Then S is an $\mathbb{F}_p$-spanning set for V (i.e. $U = V$). Now S is the orbit $1^W = \langle \omega^k \rangle$ (note that W acts by field multiplication). Also, for each $\omega^i \in V^*$, $\hat{\omega}^i$ maps S to $S\omega^i$, and since $\hat{\omega}^i \in \mathrm{GL}(1, p^R)$ it follows that $S\omega^i$ is also an $\mathbb{F}_p$-spanning set for V. However, $S\omega^i$ is the W-orbit containing ω^i. Hence every W-orbit in V^* is a spanning set for V and so W is irreducible on V. Thus (i) and (iii) are equivalent.

Suppose that k is a multiple of $\frac{q-1}{p^a-1}$ for some proper divisor a of R. Then S is a subgroup of the multiplicative group of the proper subfield $\mathbb{F}_{p^a}$ of $\mathbb{F}_q$. Thus $U \subset \mathbb{F}_{p^a}$ and so Γ is disconnected. Therefore, condition (i) implies condition (iv). The reverse implication will follow from (2).

(2) Suppose Γ is disconnected. Let U be the vertex set of the connected component of Γ containing $1 \in \mathbb{F}_{p^R}$. Then U is the $\mathbb{F}_p$-span of S. It follows that all the connected components of Γ are isomorphic to $\mathrm{Cay}(U, S)$. We claim that U is a subfield of $V = \mathbb{F}_{p^R}$.

Because U is W-invariant, $U^{\hat{\omega}^{ik}} = U$ for each $\hat{\omega}^{ik} \in W$ and hence $U\omega^{ik} = U$ for each $\omega^{ik} \in S$. Thus U is closed under multiplication by elements of S. Now each element of U is of the form $\sum_{\omega^{ik}\in S} \lambda_i \omega^{ik}$ for some $\lambda_i \in \mathbb{F}_p$, and (by regarding λ_i as an integer in the range $0 \le \lambda_i \le p-1$) each $\lambda_i\omega^{ik}$ is equal to the sum $\omega^{ik} + \cdots + \omega^{ik}$ (λ_i times). Thus each element of U is a sum of a finite number of elements of S. Since U is closed under addition and under multiplication by elements of S, it follows that U is closed under multiplication. Thus U is a subring of V. Also, U contains the identity 1 of V (since $1 \in S$). Let $u \in U \setminus \{0\}$. Then, since V is finite, $u^i = u^{i+j}$ for some $i \ge 1$ and $j \ge 1$, and hence $u^{-1} = u^{j-1} \in U$. Thus U is a subfield of $V = \mathbb{F}_{p^R}$ as claimed.

Hence $|U| = p^a$ for some proper divisor a of R. Also, since $S \le U^*$, it follows that $|S| = \frac{p^R-1}{k}$ divides p^a-1. Let $k' = \frac{(p^a-1)k}{p^R-1}$. Then $|S| = \frac{p^R-1}{k} = \frac{p^a-1}{k'}$ and, by definition of a generalized Paley graph, we have $\mathrm{Cay}(U, S) = \mathrm{GPaley}\big(p^a, \frac{p^a-1}{k'}\big)$ (though perhaps $k' = 1$). Since there are p^{R-a} connected components in Γ, it follows that $\mathrm{Aut}(\Gamma) = \mathrm{Aut}\big(\mathrm{GPaley}\big(p^a, \frac{p^a-1}{k'}\big)\big) \wr S_{p^{R-a}}$. □

By Theorem 2.2, if $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is disconnected then the connected components are generalized Paley graphs for subfields. In the rest of the paper we will assume that $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected.

3. Proof of Theorem 1.2(2)

Suppose first that $\Gamma = \mathrm{GPaley}\big(p^R, \frac{p^R-1}{k}\big) \cong H(p^a, b)$, where $R = ab$ with $b > 1$. The valency of Γ is $\frac{p^R-1}{k} = b(p^a-1)$, so $k = \frac{p^R-1}{b(p^a-1)} = \frac{a(p^R-1)}{R(p^a-1)}$ as required. Conversely, suppose that $k = \frac{a(p^R-1)}{R(p^a-1)}$ where $R = ab$ and $1 \le a < R$. Then, since $\Gamma = \mathrm{GPaley}\big(p^R, \frac{p^R-1}{k}\big)$ is connected, the $\mathbb{F}_p$-span of $S = \langle \omega^k \rangle$ equals V; that is, $\big\{\sum_{\omega^{ik}\in S} \lambda_i\omega^{ik} \mid \lambda_i \in \mathbb{F}_p\big\} = V$. Let U be the $\mathbb{F}_{p^a}$-span of the set $X := \{1, \omega^k, \omega^{2k}, \ldots, \omega^{(b-1)k}\}$. We claim that $U = V$.

Now $\mathbb{F}_{p^a}, X \subseteq V = \mathbb{F}_{p^R}$, and hence $U \subseteq V$. Moreover, since $k = \frac{a(p^R-1)}{R(p^a-1)}$, the set $S = \langle \omega^k \rangle$ has order $\frac{p^R-1}{k} = \frac{R}{a} \cdot (p^a-1) = b(p^a-1)$ and also ω^{bk} has order $p^a - 1$. Thus $\langle \omega^{bk} \rangle = \mathbb{F}_{p^a}^*$. Now suppose $v \ne 0$ and $v \in V$. Then $v = \sum \lambda_i \omega^{ik}$, where $\lambda_i \in \mathbb{F}_p$ (not all zero) and the sum is over all $\omega^{ik} \in S$. Let $i = bx_i + r_i$ where $0 \le r_i < b$. Then $\omega^{ik} = \omega^{(bx_i+r_i)k} = \omega^{bx_ik} \cdot \omega^{r_ik}$ and we have

$$v = \sum \lambda_i \omega^{ik} = \sum \lambda_i \omega^{bx_ik} \cdot \omega^{r_ik}.$$

Since $\mathbb{F}_{p^a}^* = \langle \omega^{bk} \rangle$, it follows that $\omega^{bx_ik} \in \mathbb{F}_{p^a}$. Thus $\lambda_i \omega^{bx_ik} \in \mathbb{F}_{p^a}$ and so $v \in U$. Hence $U = V$ as claimed.

From now on we shall regard V as a vector space over $\mathbb{F}_{p^a}$. We have shown that V is spanned by the set $X = \{1, \omega^k, \omega^{2k}, \dots, \omega^{(b-1)k}\}$, and since $\dim_{\mathbb{F}_{p^a}}(\mathbb{F}_{p^R}) = b$ it follows that X is an $\mathbb{F}_{p^a}$-basis for V. Define $\Theta \colon V \to \mathbb{F}_{p^a}^b$ as follows. For $u = \sum_{j=0}^{b-1} \mu_j \omega^{jk}$ with $\mu_j \in \mathbb{F}_{p^a}$, let $\Theta(u) = (\mu_0, \mu_1, \dots, \mu_{b-1}) \in \mathbb{F}_{p^a}^b$. Since X is an $\mathbb{F}_{p^a}$-basis for V, Θ is a bijection.

Next, we determine the image of the connecting set $S \subset V$ under Θ. As we observed previously, $|S| = |\langle \omega^k \rangle| = b(p^a - 1)$. Thus each element of S can be expressed uniquely as ω^{ik} for some i such that $0 \le i \le b(p^a - 1) - 1$. As before, we write $i = bx_i + r_i$ where $0 \le r_i \le b - 1$. Thus $\omega^{ik} = \omega^{bx_ik} \cdot \omega^{r_ik}$. Now $\omega^{bx_ik} \in \mathbb{F}_{p^a}^* = \langle \omega^{bk} \rangle$, and so

$$\Theta(\omega^{ik}) = \Theta(\omega^{bx_ik} \cdot \omega^{r_ik}) = (0, \dots, 0, \underbrace{\omega^{bx_ik}}_{r_i\text{th}}, 0, \dots, 0).$$

Observe that x_i can be any integer satisfying $0 \le x_i \le p^a - 2$, and therefore ω^{bkx_i} takes on each of the values in $\mathbb{F}_{p^a}^*$. Moreover, each of these values occurs exactly once in each of the positions r for $0 \le r \le b - 1$. Thus $\Theta(S)$ is the set of all elements of $\mathbb{F}_{p^a}^b$ with exactly one component nonzero—that is, the set of "weight-1" vectors.

Now Θ determines an isomorphism from Γ to the Cayley graph for $\mathbb{F}_{p^a}^b$ with connecting set $\Theta(S)$. In this Cayley graph, two b-tuples $u, v \in \mathbb{F}_{p^a}^b$ are adjacent if and only if $u - v \in \Theta(S)$, that is, if and only if $u - v$ has exactly one nonzero component. Thus $\Gamma = \mathrm{GPaley}\big(p^R, \frac{p^R-1}{k}\big)$ is mapped under the isomorphism Θ to the Hamming graph $H(p^a, b)$ where $b = \frac{R}{a}$.

4. Proof of Theorem 1.2(3)

Recall that, by Theorem 2.2(1), if $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ is connected then $W = \langle \hat{\omega}^k \rangle$ acts irreducibly on V. It follows that the group $G = T \rtimes W$ is a vertex-primitive subgroup of $\mathrm{Aut}(\Gamma)$ of affine type. Thus $\mathrm{Aut}(\Gamma)$ is a primitive permutation group on V containing G. We will use results from [17; 18] concerning such groups.

Proof of Theorem 1.2(3). Suppose that $\Gamma = \mathrm{GPaley}\big(p^R, \frac{p^R-1}{k}\big) = \mathrm{Cay}(V, S)$ is connected and is not a Hamming graph. Let $G = T \rtimes W$ where $T \cong \mathbb{Z}_p^R$ and $W = \langle \hat{\omega}^k \rangle$, as in Section 2.2. By Theorem 1.2(2), $k \ne \frac{a(p^R-1)}{R(p^a-1)}$ for any $a \mid R$ with $1 \le a < R$. Also, by Section 2.2 and Theorem 2.2, $G \le X := \mathrm{Aut}(\Gamma)$ and W is irreducible on V, so G is a primitive subgroup of $\mathrm{AGL}(R, p)$. Suppose, for a contradiction, that X is not contained in $\mathrm{AGL}(R, p)$. Since $k \ge 2$, it follows that Γ is not a complete graph and so $X \ne S_{p^R}$ or A_{p^R}. Then, by [17, Prop. 5.1], X is primitive of type PA. Thus (see Section 2.4) $R = ab$ with $b \ge 2$, $V = \Delta^b$ where $|\Delta| = p^a$, and $N^b \le X \le H \wr S_b$ with H primitive on Δ of type AS with simple normal subgroup N. Moreover, by [17, Prop. 5.1] and [18, Prop. 2.1], either

$N = A_{p^a}$ or N and p^a are as listed in [17, Table 2] (denoted as L_1 in [17]). In all cases N acts 2-transitively on Δ, and since N is nonabelian simple it follows that $|\Delta| = p^a \geq 5$.

We will prove that $\frac{p^R-1}{k} = b(p^a - 1)$, contradicting the assumption on k and thereby proving the theorem. Let $\gamma \in \Delta$ and consider the point $u = (\gamma, \dots, \gamma) \in \Delta^b = V$. Since N^b is transitive on V we have $X = N^b X_u$, where X_u is the stabilizer of u in X. Now X_u contains $(N^b)_u = (N_\gamma)^b$, and N_γ is transitive on $\Delta - \{\gamma\}$. If $v \neq u$, then $v := (\delta_1, \dots, \delta_b)$ with, say, ℓ entries $(1 \leq \ell \leq b)$ different from γ and the length of the $(N^b)_u$-orbit containing v is $(p^a - 1)^\ell$.

Because X is a primitive subgroup of $\mathrm{Sym}(\Delta) \wr S_b$, X projects to a transitive subgroup of S_b (see e.g. [5, Thm. 4.5]). Moreover, since $X = N^b X_u$, it follows that X_u also projects to a transitive subgroup of S_b. Thus the ℓ-subset of subscripts i such that $\delta_i \neq \gamma$ has n_ℓ distinct images under X_u, where $n_\ell \geq b/\ell$. It follows that the length of the X_u-orbit containing v is at least $n_\ell \cdot (p^a - 1)^\ell \geq \frac{b}{\ell} \cdot (p^a - 1)^\ell$. Suppose now that the point v has been chosen to lie in $\Gamma(u)$ (the set of all vertices in Γ adjacent to u) so that $v^{X_u} = \Gamma(u)$ has size $\frac{p^R-1}{k}$. Then

$$\frac{p^R - 1}{k} \geq \frac{b}{\ell} \cdot (p^a - 1)^\ell. \tag{4.1}$$

On the other hand, X_u contains $G_u = W = \langle \hat{\omega}^k \rangle$, and all W-orbits in $V \setminus \{u\}$ have length $\frac{p^R-1}{k}$. It follows that all orbits of X_u in $V \setminus \{u\}$ have length a multiple of $\frac{p^R-1}{k}$. Now there exists an orbit of X_u in $V \setminus \{u\}$ of length $b(p^a - 1)$ (the set of b-tuples with exactly one entry different from γ), and so

$$b(p^a - 1) \geq \frac{p^R - 1}{k}. \tag{4.2}$$

Combining inequalities (4.1) and (4.2), we obtain

$$\ell \geq (p^a - 1)^{\ell - 1}. \tag{4.3}$$

Since $p^a \geq 5$, the inequality (4.3) holds if and only if $\ell = 1$, and hence $\frac{p^R-1}{k} = b(p^a - 1)$ as claimed. This implies that $k = \frac{p^R-1}{b(p^a-1)} = \frac{a(p^R-1)}{R(p^a-1)}$, which is a contradiction. Thus X is a primitive subgroup of $\mathrm{AGL}(R, p)$. □

5. The Case Where $k \mid (p - 1)$: Proof of Theorem 1.2(4)

Let $\Gamma = \mathrm{GPaley}\big(q, \frac{q-1}{k}\big) = \mathrm{Cay}(V, S)$, where $q = p^R$ and where V and S are as in Definition 1.1, and suppose that k divides $p - 1$. Let $A := \mathrm{Aut}(\Gamma)$. Recall from Section 1 that A contains $X := T \rtimes \langle W, \alpha \rangle$ as an arc-transitive subgroup, where $W = \langle \hat{\omega}^k \rangle$. We will prove that $A = X$.

If $k = 2$, then $\Gamma = \mathrm{GPaley}\big(p^R, \frac{p^R-1}{2}\big)$ is a Paley graph and (see e.g. [16]) $A = X$. Thus we may assume that $k \geq 3$. Then, since $p - 1 \geq k \geq 3$, we have $p \geq 5$. Suppose that $R = ab$ with $b > 1$. Then $\frac{p^R-1}{p^a-1} = (p^a)^{b-1} + p^{R-2a} + \cdots + p^a + 1 > p^{a(b-1)} \geq p > k$. Hence, by Theorem 1.2(1), Γ is connected and so, by Theorem 2.2, W is irreducible on V. Also, if $k = \frac{p^R-1}{b(p^a-1)}$ then

$$b = \frac{p^R - 1}{k(p^a - 1)} > \frac{p^R - 1}{p(p^a - 1)} > p^{ab-a-1} \geq p^{a(b-2)}.$$

It follows, since $p \geq 5$, that $b = 2$, $a = 1$, and $k = \frac{p+1}{2}$. However, this contradicts the assumption $k \,|\, (p-1)$. Thus it follows from Theorem 1.2(3) that $A = T \rtimes A_0 \leq \mathrm{AGL}(R, p)$, where $\langle W, \alpha \rangle \leq A_0 \leq \mathrm{GL}(R, p)$. Note that A_0 preserves $S \subset V$ and hence A_0 does not contain $\mathrm{SL}(R, p)$.

We identify $V = \mathbb{F}_{p^R}$ with an R-dimensional vector space over the prime field $\mathbb{F}_p$. Let a be minimal such that $a \geq 1$, $a \,|\, R$, and A_0 preserves on V the structure of an a-dimensional vector space over a field of order $q_0 = p^{R/a}$. Then $A_0 \leq \Gamma L(a, q_0)$ acting on $V = \mathbb{F}_{q_0}^a$. Let $Z := \langle \hat{\omega}^{(q-1)/(q_0-1)} \rangle = Z(\mathrm{GL}(a, q_0)) \cong \mathbb{Z}_{q_0-1}$.

Lemma 5.1. *If $a \leq 2$ then $A = X$.*

Proof. Suppose first that $a = 1$. Then $A_0 \leq \Gamma L(1, p^R) = \langle \hat{\omega}, \alpha \rangle$. Since $\langle \hat{\omega} \rangle$ is regular on V^* and since A_0 leaves $S = \langle \omega^k \rangle$ invariant, it follows that $A_0 \cap \langle \hat{\omega} \rangle = \langle \hat{\omega}^k \rangle$. Hence $A_0 = W$ and $A = X$.

Suppose now that $a = 2$. Consider the canonical homomorphism

$$\varphi\colon \mathrm{GL}(2, q_0) \to \mathrm{PGL}(2, q_0),$$

and for $H \leq \mathrm{GL}(2, q_0)$ let $\bar{H} := \varphi(H) = HZ/Z$. Now $\overline{A_0} \not\geq \mathrm{PSL}(2, q_0)$ since $A_0 \not\geq \mathrm{SL}(2, q_0)$. Also $\overline{W} = WZ/Z$, and, since $k \,|\, (p-1)$, $WZ = \langle \hat{\omega}^k, \hat{\omega}^{q_0+1} \rangle$ has order $q_0^2 - 1$ if k is odd and $\frac{q_0^2-1}{2}$ if k is even. Hence

$$\overline{\langle W, \alpha \rangle} \cong \begin{cases} D_{2(q_0+1)} & \text{if } k \text{ is odd,} \\ D_{q_0+1} & \text{if } k \text{ is even.} \end{cases}$$

It follows from the classification of the subgroups of $\mathrm{PGL}(2, q_0)$ and $\mathrm{PSL}(2, q_0)$ (see [19, p. 417]) that either $\overline{A_0} \leq \overline{\langle \hat{\omega}, \alpha \rangle} \cong D_{2(q_0+1)}$ or $\overline{A_0} \in \{A_4, S_4, A_5\}$. In the former case, $A_0 \leq \langle \hat{\omega}, \alpha \rangle = \mathrm{A\Gamma L}(1, q)$ and $a = 1$, which is a contradiction. In the latter case, since $\overline{A_0} \geq \mathbb{Z}_{(q_0+1)/2}$ and $p \geq 5$, it follows that $q_0 = p = 5$ or 7. Moreover, since $\overline{A_0} \geq D_{p+1}$ and $\overline{A_0} \not\geq \mathrm{PSL}(2, p)$, it follows that $\overline{A_0} = S_4$ and in both cases $\overline{A_0}$ is transitive on 1-spaces. Thus S consists of, say, s points from each 1-space and $|S| = (p+1)s$. Since $|S| = \frac{|V^*|}{k}$, we have $k = \frac{|V^*|}{(p+1)s} = \frac{p-1}{s}$. Also, since Γ is an undirected Cayley graph, $S = \langle \omega^k \rangle = -S$ and hence S contains -1 and $s \geq 2$. Thus $k \leq \frac{p-1}{2}$ and, since $k \geq 3$, we have $p = 7$, $k = 3$, and $s = 2$. This is impossible because in this case $W = \langle \hat{\omega}^3 \rangle \cong \mathbb{Z}_{16}$ projects to $\overline{W} \cong \mathbb{Z}_8$ yet $\overline{A_0} = S_4$ has no such subgroup. □

From now on we will assume that $a \geq 3$, $k \geq 3$, and $p \geq 5$. Then, by an old result of Zsigmondy [21] (or see [9]), there is a prime divisor r of $p^R - 1$ such that r does not divide $p^c - 1$ for any $c < R$. Then p has multiplicative order R modulo r, and in particular R divides $r - 1$. Thus $r = Rs + 1$ for some $s \geq 1$. Such a prime r is called a *primitive prime divisor* of $p^R - 1$.

Let $A_1 := A_0 \cap \mathrm{GL}(a, q_0)$. Since $W \subseteq \mathrm{GL}(a, q_0)$, it follows that $W \subseteq A_1$, so r divides $|A_1|$ and A_1 is irreducible. By the minimality of a, A_1 is not contained in a proper "extension field subgroup" of $\mathrm{GL}(a, q_0)$. Also, since $k \,|\, (p-1)$, the order of W is divisible by $\frac{p^R-1}{p-1}$; it follows that W, and hence also A_1, cannot be realized over a proper subfield of $\mathbb{F}_{q_0}$. By [9, Main Theorem] (noting that the groups in [9, Ex. 2.2–2.4] do not have all of these properties), either

(A) A_1 belongs to one of the families of Examples 2.1 or 2.5 in [9], or

(B) A_1 is *nearly simple*; that is, $L \le A_1/(A_1 \cap Z) \le \mathrm{Aut}(L)$ for some nonabelian simple group L, with L as in one of Examples 2.6–2.9 in [9].

LEMMA 5.2. *The group A_1 satisfies condition* (B).

Proof. Suppose that A_1 is a subgroup of $\mathrm{GL}(a, q_0)$ in [9, Ex. 2.1]. Then A_1 is a classical group containing $Y = \mathrm{SL}(a, q_0)$, or (for a even) $\mathrm{Sp}(a, q_0)$ or $\Omega^{\pm}(a, q_0)$, or (if aq_0 is odd) $\Omega(a, q_0)$, or (if q_0 is a square) $\mathrm{SU}(a, q_0)$. Since A_1 is not transitive on V^*, A_1 cannot contain $\mathrm{SL}(a, q_0)$ or $\mathrm{Sp}(a, q_0)$. Also, A_1 contains the irreducible element $\hat{\omega}^{p-1}$ of order $\frac{p^r-1}{p-1}$, whereas (see [1] or [10]) for the remaining groups Y we have $|\langle\hat{\omega}\rangle \cap N_{\mathrm{GL}(a,q_0)}(Y)| \le (q_0^{a/2} + 1)(q_0 - 1)$.

Next suppose that A_1 is as in [9, Ex. 2.5]. Then $a = 2^m$, $r = a + 1$, and A_1 is contained in $Z \circ (S \cdot M_0)$, where S and M_0 are as listed in Table 1. Also, since $r \ge R + 1$, it follows that $a = R$, and so $r = R + 1 = 2^m + 1 \ge 5$ and $q_0 = p$. Elements in S and M_0 have orders at most 4 and $2^{2m} - 1 = R^2 - 1$, respectively (see [1, Proof of Lemma 2]), and $S \cap Z \cong \mathbb{Z}_2$. Thus elements of A_1 have order at most $2(R^2 - 1)(p - 1)$ and, since A_1 contains $\hat{\omega}^{p-1}$ of order $\frac{p^R-1}{p-1}$, we have $\frac{p^R-1}{p-1} \le 2(R^2 - 1)(p - 1)$. Since $p \ge 5$ and $R \ge 4$,

$$5^{R-2} - 1 \le p^{R-2} - 1 < \frac{p^R - 1}{(p-1)^2} \le 2(R^2 - 1).$$

Since $R \ge 4$, this implies that $(R, p) = (4, 5)$. However, $r = R + 1 = 5$ does not divide $5^4 - 1$, contradicting the definition of r. □

Thus case (B) holds, and we need to consider the possibilities for A_1 from Examples 2.6–2.9 in [9] (see also Tables 2–5) with order divisible by the primitive prime divisor r of $p^R - 1$, where $R = ab$ ($a \ge 3$) and $q_0 = p^b \ge 5^b$. Here $L \le A_1/(A_1 \cap Z) \le \mathrm{Aut}(L)$ for some nonabelian simple group L. Note that, when applying the results of [9], the dimension a is equal to $d = e$ in [9] and b is the parameter a in [9]. Also, most of the examples in Tables 2–5 have additional conditions for q_0, p, r, or a. We will not mention these conditions except when they are necessary for our calculations.

Table 1

S	M_0	p
$4 \circ 2^{1+2m} = \mathbb{Z}_4 \circ D_8 \circ \cdots \circ D_8$	$\mathrm{Sp}(2m, 2)$	$p \equiv 1 \pmod 4$
$2_-^{1+2m} = D_8 \circ \cdots \circ D_8 \circ Q_8$	$\mathrm{O}^-(2m, 2)$	
$2_+^{1+2m} = D_8 \circ \cdots \circ D_8$	$\mathrm{O}^+(2m, 2)$	

Table 2

Example 2.6(b) of [9]

n	7	6	5	5	7	7
a	4	4	2	4	3	6
r	5	5	5	5	7	7
b	1	1	2	1	2	1

Table 3

Example 2.7 of [9]

L	M_{11}	M_{12}	M_{22}	M_{23}	J_2	J_3	Ru	Suz
a	10	10	10	22	6	18	28	12
r	11	11	11	23	7	19	29	13

Table 4

Example 2.9 of [9, Table 7]

L	$G_2(4)$	$\mathrm{PSU}(4,2)$	$\mathrm{PSU}(4,3)$	$\mathrm{PSL}(3,4)$
a	12	4	6	6
r	13	5	7	7

Table 5

Example 2.9 of [9, Table 8]

L	$\mathrm{PSL}(n,s)$	$\mathrm{PSU}(n,s)$	$\mathrm{PSp}(2n,s)$	$\mathrm{PSL}(2,s)$	$\mathrm{PSL}(2,s)$
	$n \geq 3$, n prime	$n \geq 3$, n prime	$n = 2^c \geq 2$	$s \geq 7$	$s \geq 7$
a	$\frac{s^n-1}{s-1} - 1$	$\frac{s^n+1}{s+1} - 1$	$\frac{1}{2}(s^n - 1)$	$s, s-1$, or $\frac{1}{2}(s-1)$	$\frac{1}{2}(s-1)$
r	$a+1$	$a+1$	$a+1$	$a+1$	$2a+1$

Lemma 5.3. *The group A_1 does not satisfy condition* (B).

Proof. Recall that $r \geq R+1 \geq a+1 \geq 4$ and $p \geq 5$. Also $\hat{\omega}^{p-1} \in A_1$ has order $\frac{p^R-1}{p-1}$, a multiple of r. Let $\max(A_1)$ denote the maximum order of an element of A_1 whose order is a multiple of r. An easy calculation shows that

$$\max(A_1) \geq \frac{p^R-1}{p-1} > \begin{cases} 2(p^2-1)(R+1) & \text{if either } R \geq 5 \text{ and } p \geq 5 \\ & \qquad \text{or } R = 4 \text{ and } p \geq 11 \\ (p^2-1)(R+1) & \text{if } R = 4 \text{ and } p = 7 \\ 2(p-1)(R+1) & \text{if } R \geq 4 \text{ and } p \geq 5. \end{cases} \tag{5.1}$$

Case [9, Example 2.6]. Suppose first that $A_n \leq A_1 \leq S_n \times Z$ with $n = a+1$ or $a+2$ and with $r = a+1$, so $R = a$ and $q_0 = p$. Then any element of S_n whose order is a multiple of r is an r-cycle, and therefore $\hat{\omega}^{p-1}$ has order at most $r(p-1)$. Hence $(R+1)(p-1) = r(p-1) \geq \frac{p^R-1}{p-1}$, contradicting (5.1). Thus $L = A_n$ with n, a, r, b as in one of the columns of Table 2 (see [9, Tables 2–4]). In all cases $r = ab+1 = R+1$ and $r \geq n - \delta$, where $\delta = 1$ (except for column 1, where $\delta = 2$). Thus any element of S_n whose order is a multiple of r has order at most δr. Hence an element of A_1 of order a multiple of r has order at most $\delta r(q_0 - 1) = \delta(p^b - 1)(R+1)$. By (5.1), column 3 of Table 2 holds but with $r = p = 5$, contradicting the definition of r.

Case [9, Example 2.7]. See Table 3, which contains the examples from [9, Table 5] for which r is a primitive prime divisor of $p^R - 1$. In all cases, $q = p$ and $r = R+1$. An element of $\mathrm{Aut}(L)$ of order a multiple of r has order at most $2r = 2(R+1)$ (see [6]), so $\max(A_1) \leq 2(p-1)(R+1)$, contradicting (5.1).

Case [9, Example 2.8]. These examples are listed in [9, Table 6], and the only ones for which r is a primitive prime divisor of $p^R - 1$ are $L = G_2(q_0)$ with $(a, p) = (6, 2)$ and $L = Sz(q_0)$ with $(a, p) = (4, 2)$. However, these are not examples for us because $p \geq 5$.

Case [9, Example 2.9]. See Tables 4 and 5, which contain the examples from Tables 7 and 8 (respectively) of [9] for which r is a primitive prime divisor of $p^R - 1$ and $p \geq 5$. We deal with Table 4 first. Here $R = a$ and $r = R+1$. An element of $\mathrm{Aut}(L)$ of order a multiple of r has order at most δr, where δ is 1, 2, 4, and 3 for the columns of Table 4, respectively (see [6]). Thus $\max(A_1) \leq \delta(p-1)(R+1)$, contradicting (5.1) in all four cases.

Now we turn to the examples in Table 5. In all cases $\gcd(s, p) = 1$, and we have $s = s_0^c$ for some prime $s_0 \neq p$ and $c \geq 1$. Following the notation used in [1], we let $m(K)$ denote the maximum of the orders of the elements of a finite group K. Then, by (5.1), $m(A_1) \geq \max(A_1) \geq \frac{p^R-1}{p-1} \geq \frac{q_0^a-1}{q_0-1} > q_0^{a-1}$. Moreover, in all cases, $m(A_1) \leq (q_0 - 1)m(\mathrm{Aut}(L))$, so

$$m(\mathrm{Aut}(L)) > q_0^{a-2}. \tag{5.2}$$

In column 1 of Table 5, $a \geq s^2 + s \geq 6$ and $m(\mathrm{Aut}(L)) \leq m(\mathrm{GL}(n, s)) \cdot 2c = 2c(s^n - 1) = 2c(s-1)(a+1) < s(s-1)(a+1) < a(a+1)$; it then follows from (5.2) that $q_0^{a-2} < a(a+1)$, which is a contradiction since $a \geq 6$ and $q_0 \geq 5$.

In column 2 of Table 5, $a \geq s^2 - s \geq s \geq c$ and

$$\begin{aligned} m(\mathrm{Aut}(L)) \leq m(\mathrm{GL}(n, s^2)) \cdot 2c = 2c(s^{2n} - 1) &< 2c(s^n + 1)^2 \\ &= 2c(s+1)^2(a+1)^2 \leq 2a(a+1)^4. \end{aligned}$$

By (5.2), $q_0^{a-2} < 2a(a+1)^4$ and, since $q_0 \geq 5$, this implies that $a \leq 9$. Also, since $r = \frac{s^n+1}{s+1} = a+1$ is prime, n is odd, and $3 \leq a \leq 9$, it follows that $(r,a,s,n) = (7,6,3,3)$ and $L = \mathrm{PSU}(3,3)$. By [6], $m(\mathrm{Aut}(\mathrm{PSU}(3,3))) = 12$ and we have a contradiction to (5.2).

In column 3 of Table 5, $a \geq s+1 > c$ and $m(\mathrm{Aut}(L)) \leq m(\mathrm{GL}(2n,s)) \cdot 2c = 2c(s^{2n}-1) = 2c \cdot 2a(2a+2) < 8a^2(a+1)$. By (5.2), $q_0^{a-2} < 8a^2(a+1)$ and, since $q_0 \geq 5$, this implies that $a \leq 6$. Also, since $r = \frac{s^n+1}{2} = a+1$ is prime, $n \geq 2$, and $3 \leq a \leq 6$, it follows that $(r,a,s,n) = (5,4,3,2)$ and $L = \mathrm{PSp}(4,3)$. By [6], $m(\mathrm{Aut}(\mathrm{PSp}(4,3))) = 12$ and we have a contradiction to (5.2).

In columns 4 and 5 of Table 5, $L = \mathrm{PSL}(2,s)$ with $s \geq 7$, $s \neq p$, and $a \geq \frac{s-1}{2} \geq 3$. Then $m(\mathrm{Aut}(L)) = s+1$ (see [1]) and hence (5.2) yields $q_0^{a-2} < s+1 \leq 2a+2$. Since $q \geq 5$ and $a \geq \frac{s-1}{2} \geq 3$, this implies that $a = 3 = \frac{s-1}{2}$ and $q_0 \leq 7$. Thus $L = \mathrm{PSL}(2,7)$ and $p \neq s = 7$. So $q_0 = p = 5$ (since $p \geq 5$) and $a = R = 3$. However, the only primitive prime divisor of $p^R - 1 = 5^3 - 1$ is 31 whereas, by Table 5, $r \leq s = 7$. □

It follows from the discussion and results of this section that Theorem 1.2(4) is proved.

ACKNOWLEDGMENTS. This paper forms part of the Ph.D. thesis of the first author, completed at the University of Western Australia under the supervision of Associate Professor Cai Heng Li and the second author. It also forms part of the Discovery Grant DP0449429 funded by the Australian Research Council. The second author acknowledges support of Australian Research Council Federation Fellowship FF0776186. The authors are grateful to Mikhail Klin for pointing out connections between their work and cyclotomic association schemes.

References

[1] Á. Bereczky, *Maximal overgroups of Singer elements in classical groups,* J. Algebra 234 (2000), 187–206.

[2] N. Biggs, *Algebraic graph theory,* Cambridge Univ. Press, Cambridge, 1993.

[3] W. Bosma and J. Cannon, *Handbook of MAGMA functions,* School of Mathematics and Statistics, Univ. of Sydney, 1993, ⟨http://magma.maths.usyd.edu.au/magma/⟩.

[4] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance regular graphs,* Ergeb. Math. Grenzgeb. (3), 18, Springer-Verlag, Berlin, 1989.

[5] P. J. Cameron, *Permutation groups,* London Math. Soc. Stud. Texts, 45, Cambridge Univ. Press, Cambridge, 1999.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups,* Oxford Univ. Press, Eynsham, 1985.

[7] C. D. Godsil, *Algebraic combinatorics,* Chapman & Hall, New York, 1993.

[8] C. D. Godsil and G. F. Royle, *Algebraic graph theory,* Grad. Texts in Math., 207, Springer-Verlag, New York, 2001.

[9] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors,* Proc. London Math. Soc. (3) 78 (1999), 167–214.

[10] B. Huppert, *Singer-zyklen in klassischen Gruppen,* Math. Z. 117 (1970), 141–150.

[11] C. H. Li, T. K. Lim, and C. E. Praeger, *Homogeneous factorisations of complete graphs with edge-transitive factors,* J. Algebraic Combin. 29 (2009), 107–132.

[12] C. H. Li and C. E. Praeger, *On partitioning the orbitals of a transitive permutation group,* Trans. Amer. Math. Soc. 355 (2003), 637–653.

[13] M. W. Liebeck, C. E. Praeger, and J. Saxl, *On the O'Nan–Scott theorem for finite primitive permutation groups,* J. Austral. Math. Soc. Ser. A 44 (1988), 389–396.

[14] R. McConnel, *Pseudo-ordered polynomials over a finite field,* Acta. Arith. 8 (1963), 127–151.

[15] R. E. A. C. Paley, *On orthogonal matrices,* J. Math. Phys. 12 (1933), 311–320.

[16] W. Peisert, *All self-complementary symmetric graphs,* J. Algebra 240 (2001), 209–229.

[17] C. E. Praeger, *The inclusion problem for finite primitive permutation groups,* Proc. London Math. Soc. (3) 60 (1990), 68–88.

[18] C. E. Praeger and J. Saxl, *Closures of finite primitive permutation groups,* Bull. London Math. Soc. 24 (1992), 251–258.

[19] M. Suzuki, *Group theory I,* Grundlehren Math. Wiss., 247, Springer-Verlag, New York, 1982.

[20] H. Wielandt, *Finite permutation groups,* Academic Press, New York, 1964.

[21] K. Zsigmondy, *Zur Theorie der Potenzreste,* Monatsh. Math. Phys. 3 (1892), 265–284.

T. K. Lim
45 Choa Chua Kang Loop #07-14
Singapore 689679

limtk@phillip.com.sg

C. E. Praeger
School of Mathematics and Statistics
University of Western Australia
Crawley WA 6009
Australia

praeger@maths.uwa.edu.au