SIAM J. DISCRETE MATH.
Vol. 28, No. 1, pp. 8–17

SELF-COMPLEMENTARY CIRCULANTS OF PRIME-POWER ORDER*

CAI HENG LI†, SHAOHUI SUN‡, AND JING XU§

Abstract. Let Γ be a self-complementary circulant of prime power order. It is shown that either Γ is a lexicographic product of two small self-complementary circulants or there exists a multiplicative automorphism of a regular cyclic subgroup that maps Γ to its complement.

Key words. self-complementary graph, circulant, lexicographic product, self-complementary-normal Cayley graph

AMS subject classifications. 05C25, 20B25

DOI. 10.1137/120870025

1. Introduction. A digraph (or an undirected graph) Γ is called a *circulant* of order n if it has a cyclic group of automorphisms which is regular on the vertex set. Recall that a permutation group is *regular* if it is transitive and the only element that fixes a point is the identity.

Moreover, for undirected graphs we introduce the concept of being self-complementary. Let $\Gamma = (V, E)$ be an undirected graph with vertex set V and edge set E. The *complement* $\overline{\Gamma}$ of Γ is the undirected graph with vertex set V such that $\{u, v\}$ is an edge of $\overline{\Gamma}$ if and only if $\{u, v\} \notin E$. An undirected graph Γ is called *self-complementary* if $\Gamma \cong \overline{\Gamma}$.

This paper aims to classify self-complementary (undirected) circulants of prime-power order p^d, where p is a prime and $d \geq 1$.

In the literature, self-complementary circulants have received attention for a long time, dating back to Sachs in 1962; refer to [1, 4, 7, 19, 20, 22]. More recently, study has been extended to self-complementary graphs which are vertex-transitive; refer to the articles [3, 6, 13, 18, 23] and the survey [2] and references therein.

In [4], Fronček, Rosa, and Širáň determined the order of self-complementary circulants. They then proposed the question of whether each self-complementary circulant could be produced by a multiplicative automorphism of a regular cyclic subgroup in the sense of Construction 3.2. This question was answered in [7, 16] in the negative. A natural next step is to seek a classification of self-complementary circulants. By Muzychuck's theorem [17], self-complementary circulants of square-free order can be constructed by multiplicative automorphisms of the regular cyclic subgroup, see Construction 3.2. The purpose of this paper is to determine the other extremal case, namely, the prime power order case.

*Received by the editors March 14, 2012; accepted for publication (in revised form) October 31, 2013; published electronically January 2, 2014. This work was partially supported by the National Natural Science Foundation of China (10901110, 11171231) and by the Tian Yuan Special Funds of the Natural science Foundation of China (11126293) and also by an ARC Discovery Project grant.
http://www.siam.org/journals/sidma/28-1/87002.html
†School of Mathematics and Statistics, Yunnan University, Kunming, Yunnan 650091, People's Republic of China, and School of Mathematics and Statistics, University of Western Australia, Crawley 6009 WA, Australia (cai.heng.li@uwa.edu.au).
‡Department of Mathematics, Hunan Normal University, Hunan 410081, People's Republic of China (sunsh@hunnu.edu.cn).
§Department of Mathematics, Capital Normal University, Beijing 100048, People's Republic of China (xujing@cnu.edu.cn).

We next introduce two typical constructions for self-complementary circulants.

Let G be a finite group. We remark here that throughout this paper we use multiplicative notation for our groups, so the identity element of the group G is denoted by 1. In general, let S be a subset of G which does not contain the identity, and the *Cayley digraph* $\mathrm{Cay}(G, S)$ is the digraph with vertex set G such that u is adjacent to v if and only if $vu^{-1} \in S$. It follows from the definition that the automorphism group $\mathrm{Aut}\,\mathrm{Cay}(G, S)$ has a subgroup $\hat{G} \cong G$, where

$$\hat{G} = \{\hat{g} \in \mathrm{Sym}(G) :\ x \mapsto xg\ \forall x \in G \mid g \in G\}.$$

So $\hat{G}$ is regular on the vertex set of $\mathrm{Cay}(G, S)$, and $\hat{G}$ is actually the right regular representation of the group G which is also denoted by G_R in some literature. In fact, it is well known that a digraph Γ is a Cayley digraph if and only if $\mathrm{Aut}\,\Gamma$ contains a regular subgroup. A circulant is therefore a Cayley digraph of a cyclic group. Clearly the Cayley digraph $\mathrm{Cay}(G, S)$ is undirected if and only if $S = S^{-1} = \{s^{-1} \mid s \in S\}$. From now on, when we say "a Cayley graph" or "a self-complementary circulant (graph)," we always mean it is undirected.

For a self-complementary graph $\Gamma = (V, E)$, an isomorphism σ between Γ and its complement $\overline{\Gamma}$ is called a *self-complementary isomorphism*, or an *sc-isomorphism* for short. An sc-isomorphism σ of Γ is a permutation of the vertex set V such that $\sigma^2 \in \mathrm{Aut}\,\Gamma$ and so σ normalizes $\mathrm{Aut}\,\Gamma$. Assume further that $\Gamma = \mathrm{Cay}(G, S)$ is a Cayley graph of the group G and so $\mathrm{Aut}\,\Gamma$ contains the regular group $\hat{G}$. Now an extremal case is where σ normalizes $\hat{G}$. Such a self-complementary Cayley graph is called a *self-complementary-normal Cayley graph with respect to* σ, or an *sc-normal* graph for short. It is easy to show that Γ is an sc-normal circulant if and only if there exists a multiplicative automorphism of a regular cyclic subgroup that maps Γ to its complement; see section 3. Construction 3.2 provides us with a method for constructing all sc-normal circulants of prime power order.

Another typical construction comes from a special graph product. In general, for a digraph Σ with vertex set U and a digraph Δ with vertex set W, the *lexicographic product* $\Sigma[\Delta]$ (this graph construction is also called the *wreath product*) is the digraph with vertex set $U \times W$ such that the vertex (u, w) is adjacent to (u', w') if and only if either u is adjacent to u' in Σ or $u = u'$ and w is adjacent in Δ to w'. If both Σ and Δ are self-complementary graphs, then so is $\Sigma[\Delta]$; see Lemma 2.4.

The main result of this paper is the following theorem. Note that by the definition, it is easy to deduce that the order of a self-complementary circulant must be an odd integer.

THEOREM 1.1. *Let Γ be a self-complementary circulant of order p^d, where p is a prime and $d \geq 1$. Then p is odd, and either Γ is sc-normal or $\Gamma = \Sigma_1[\Sigma_2]$, where Σ_i is a self-complementary circulant of order p^{n_i} for $i = 1, 2$ and $n_1 + n_2 = d$.*

2. Preliminary results. Throughout the paper, let p be an odd prime. A finite permutation group is called a *c-group* if it contains a cyclic regular subgroup. Since the automorphism group of a circulant must contain a cyclic regular group, the studies of circulants are closely related to the studies of c-groups. The research of c-groups was initiated by Burnside in 1900, and recently a precise list of primitive c-groups was obtained by using the classification of finite simple groups and a classical result of Schur; see, for example, [8, 11, 15].

In this paper we always use the notation $\mathbb{Z}_n$ to denote an abstract cyclic multiplicative group of order n.

LEMMA 2.1 (see [15, Lemma 2.3]). *Suppose that X is a primitive permutation group on Ω and X contains a cyclic regular subgroup. Then one of the following holds:*

(i) $|\Omega| = q$, *and* $X \leq \mathrm{AGL}(1, q)$, *where q is a prime.*

(ii) $|\Omega| = 4$, *and* $X = S_4$.

(iii) *X is almost simple and 2-transitive on Ω.*

COROLLARY 2.2. *Suppose that X is a solvable primitive c-group on Ω, where $|\Omega| = p^d$ is an odd prime power. Then $|\Omega| = p$ and $\mathbb{Z}_p \leq X \leq \mathrm{AGL}(1, p)$.*

Next we introduce the concept of the normal Cayley digraph. Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph. Let $\mathrm{Aut}(G, S) = \{\sigma \in \mathrm{Aut}(G) \mid S^\sigma = S\}$. Then each element in $\mathrm{Aut}(G, S)$ induces an automorphism of the Cayley digraph $\Gamma = \mathrm{Cay}(G, S)$ and it is well known that the normalizer of the regular subgroup $\hat{G}$ in $\mathrm{Aut}(\Gamma)$ is $\hat{G} \rtimes \mathrm{Aut}(G, S)$. A Cayley digraph $\Gamma = \mathrm{Cay}(G, S)$ is called *normal* if $\hat{G}$ is normal in $\mathrm{Aut}(\Gamma)$ or equivalently if $\mathrm{Aut}(\Gamma) = \hat{G} \rtimes \mathrm{Aut}(G, S)$; see [5, 21].

The finite arc-transitive circulants were classified independently, and via two different methods, by Kovács [9] and Li [12]. Note that in [12, Theorem 1.3], the orders of the deleted lexicographic product type digraphs cannot be a prime power. Then the following result concerning arc-transitive circulants of order p^d is an immediate corollary of Theorem 1.3 in [12]. As usual, denote by K_n the complete graph of order n and by $\overline{K}_n$ the complement of K_n.

THEOREM 2.3. *Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ be a connected arc-transitive directed (or undirected) circulant of order p^d, where p is an odd prime and $d \geq 1$ is an integer. Then one of the following holds:*

(i) *Γ is a complete graph.*

(ii) *Γ is a normal circulant.*

(iii) *There exists an arc-transitive circulant Σ of order p^{d-i} such that $\Gamma = \Sigma[\overline{K}_{p^i}]$, where $1 \leq i < d$. Let $\mathbb{Z}_{p^i} \leq \mathbb{Z}_{p^d}$ be the subgroup of order p^i; then $s\mathbb{Z}_{p^i} \subseteq S$ for any $s \in S$.*

The next lemma concerns the lexicographic product of two graphs; refer to [14] or [2, Theorem 4.3] and [10, Lemma 2.2].

LEMMA 2.4. *Let $\Gamma = \Sigma[\Delta]$, where Σ and Δ are two graphs. Then we have the following statements:*

(i) *If both Σ and Δ are self-complementary, then so is Γ.*

(ii) *If both Σ and Δ are circulants, then so is Γ.*

We also need the following theorem.

THEOREM 2.5 (see [15, Theorem 1.4]). *The automorphism group of a self-complementary circulant is solvable.*

3. Two constructions. In this section we discuss two constructions of self-complementary circulants.

Let $G = \mathbb{Z}_{p^d}$ be a multiplicative cyclic group of order p^d and the identity element of G is 1. Let $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant of odd prime power order (so $S = S^{-1}$), and let σ be an sc-isomorphism of Γ. Let $G^\# = G \backslash \{1\}$. Since Γ is vertex transitive, without loss of generality, we may suppose that σ fixes the vertex 1, and hence $S^\sigma = G^\# \backslash S$. Moreover replacing σ by σ^m for some odd integer m, we may assume that the order $o(\sigma)$ is a power of 2.

We first construct sc-normal circulants. Suppose $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ is sc-normal with respect to σ. As explained above we may suppose that σ fixes 1 and $o(\sigma)$ is a power of 2. Since Γ is sc-normal, σ can be viewed as an automorphism of the group $\mathbb{Z}_{p^d}$, and so we may assume that $\sigma \in \mathrm{Aut}(\mathbb{Z}_{p^d})$. Note that $\mathrm{Aut}(\mathbb{Z}_{p^d}) \cong \mathbb{Z}_{p^{d-1}(p-1)}$ is a cyclic group and the unique involution $(g \to g^{-1})$ in $\mathrm{Aut}(\mathbb{Z}_{p^d})$ preserves S, so we have $o(\sigma) \geq 4$. Define

$$S(p^d, \sigma) := \{S \mid S \subset (\mathbb{Z}_{p^d})^{\#}, S^{\sigma} = (\mathbb{Z}_{p^d})^{\#} \backslash S\}. \tag{3.1}$$

It is easy to prove the following lemma.

LEMMA 3.1. *The circulant* $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ *is sc-normal if and only if* $S \in S(p^d, \sigma)$ *for some* $\sigma \in \mathrm{Aut}(\mathbb{Z}_{p^d})$ *such that* $o(\sigma) \geq 4$ *is a power of* 2.

Therefore, to classify all sc-normal circulants, it is sufficient to determine the set $S(p^d, \sigma)$ for each σ in the Sylow 2-subgroup of $\mathrm{Aut}(\mathbb{Z}_{p^d})$ with $o(\sigma) \geq 4$. The following construction, which is an application of Suprunenko's construction in [20], tells us how to obtain the set $S(p^d, \sigma)$, and so we are able to construct all sc-normal circulants of order p^d.

CONSTRUCTION 3.2. Let $G = \mathbb{Z}_{p^d}$. Let τ_k be an element of $\mathrm{Aut}(G)$ with order 2^k for $k \geq 2$. Clearly, both $\langle \tau_k \rangle$ and $\langle \tau_k^2 \rangle$ act semiregularly on $G^{\#}$. Let $m = \frac{p^d - 1}{2^k}$. Then τ_k^2 has $2m$ orbits on $G^{\#}$: $O_1, \ldots, O_{2m}$. Relabeling these orbits if necessary, we may assume that $O_{2i-1}^{\tau_k} = O_{2i}$ for each $i \in \{1, 2, \ldots, m\}$. We observe

(1) $S \in S(p^d, \tau_k)$ if and only if $S = \cup_{i=1}^{m} O_{2i - j_i}$, where $j_i = 0$ or 1;
(2) $\mathrm{Cay}(G, S)$ is sc-normal if and only if $S \in S(p^d, \tau_k)$ for some $k \geq 2$.

The second special construction is the lexicographic product of small self-complementary ciruculants. In general, let $\Gamma = \mathrm{Cay}(G, S)$, where G is a finite group. If S is a union of some left cosets of a subgroup H and $H \cap S = \emptyset$, then $sH \subseteq S$ for any $s \in S$. In this case, it is proved in [10, Lemma 2.2] that $\Gamma = \Sigma[\overline{\mathrm{K}}_m]$, where $m = |H|$ and Σ is a graph of order $|G|/|H|$. In particular, if $H \lhd G$, then $\Sigma = \mathrm{Cay}(G/H, \overline{S})$, where $\overline{S}$ is the image of S in G/H. Applying this general result to the self-complementary lexicographic product circulants, we have the following useful lemma.

LEMMA 3.3. *Let* $G = \mathbb{Z}_{p^d}$ *and let* $G_i = \mathbb{Z}_{p^i}$ *be the unique subgroup of order* p^i*, where* $1 \leq i \leq d-1$*. The graph* $\Gamma = \mathrm{Cay}(G, S)$ *is self-complementary such that* $sG_i \subset S$ *for any* $s \in S$ *with* $o(s) > p^i$ *if and only if* $\Gamma = \Sigma[\Gamma_1]$ *is a lexicographic product of a self-complementary circulant* Σ *of order* p^{d-i} *by a self-complementary circulant* Γ_1 *of order* p^i.

Proof. Suppose $\Gamma = \mathrm{Cay}(G, S)$ is a self-complementary circulant of order p^d such that $sG_i \subset S$ for any $s \in S$ with $o(s) > p^i$. Let

$$S_1 = \{s \in S \mid o(s) \leq p^i\} \text{ and } S_2 = \{s \in S \mid o(s) > p^i\}.$$

Let $\Gamma_1 = \mathrm{Cay}(G_i, S_1)$. Then the graph $\mathrm{Cay}(G, S_2) = \Sigma[\overline{K}_{p^i}]$, where $\Sigma = \mathrm{Cay}(G/G_i, \overline{S}_2)$ and $\overline{S}_2 = \{\overline{s} = sG_i \mid s \in S_2\}$. Moreover, $\Gamma = \Sigma[\Gamma_1]$ is a lexicographic product graph. By Corollary 4.5 (proved in the next section), it is easy to deduce that Σ and Γ_1 are also self-complementary circulants of order p^{d-i} and order p^i, respectively.

Conversely, suppose we have a self-complementary circulant $\Gamma_1 = \mathrm{Cay}(G_i, S_1)$ of order p^i and a self-complementary circulant $\Sigma = \mathrm{Cay}(G/G_i, \overline{S}_2)$ of order p^{d-i}. (Here we use the notation of quotient groups just for convenience.) Put $S_2 = \{s \mid s \in G, sG_i \in \overline{S}_2\}$. Let $S = S_1 \cup S_2$ and $\Gamma = \mathrm{Cay}(G, S)$. By the argument of the preceding paragraph, we have that $\Gamma = \Sigma[\Gamma_1]$ such that $sG_i \subset S$ for any $s \in S$ with $o(s) > p^i$. Since Σ and Γ_1 are self-complementary, by Lemma 2.4, Γ is also self-complementary as required. ∎

4. Cayley subsets. We begin to study the self-complementary circulant $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ by analyzing the Cayley subset S of Γ. The main result of this section is Proposition 4.2 that divides the Cayley subset S into two parts.

4.1. Notation. We first fix the notation. Throughout this section, let $G = \mathbb{Z}_{p^d}$ be a cyclic multiplicative group of odd prime power order. Let $G_i \le G$ be the unique cyclic subgroup of G with order p^i, where $i \in \{1, 2, \ldots, d-1\}$. For convenience, set $G_d = G$. Let $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant and let σ be an sc-isomorphism of Γ that fixes 1 and is of order a power of 2. Moreover, we have $(\mathrm{Aut}(\Gamma))^\sigma = \mathrm{Aut}(\overline{\Gamma}) = \mathrm{Aut}(\Gamma)$ and $\sigma^2 \in \mathrm{Aut}(\Gamma)$. We list the following assumption for the proof of Proposition 4.2.

Assumption 4.1. Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ be a self-complementary circulant and let $\sigma : \Gamma \to \overline{\Gamma}$ be an sc-isomorphism that fixes 1 and is of order a power of 2. Let $G = \mathbb{Z}_{p^d}$ and let

$$\hat{G} \le X \le \mathrm{Aut}(\Gamma) \tag{4.1}$$

such that $X^\sigma = X$ and $\sigma^2 \in X$. Let

$$Y = \langle X, \sigma \rangle. \tag{4.2}$$

For example, the pair $(X, Y) = (\mathrm{Aut}(\Gamma), \langle \mathrm{Aut}(\Gamma), \sigma \rangle)$ satisfies Assumption 4.1. Under Assumption 4.1, we have that the quotient group Y/X is a cyclic group of order 2. By Theorem 2.5, X is solvable and hence Y is also solvable.

Moreover suppose B is a block of Y; we denote Y_B^B to be the induced permutation group on B by the setwise stabilizer Y_B.

We now prove a proposition, which is one of the key ingredients in the proof of the main theorem.

PROPOSITION 4.2. *With the above notation, suppose* $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S), \sigma, X, Y$ *satisfy Assumption* 4.1. *Then there exists* $n \in \{1, \ldots, d\}$ *such that* $G_n = \mathbb{Z}_{p^n}$ *is a block of* Y *and* $\hat{G}_n \lhd Y_{G_n}^{G_n}$, *in particular,* $\sigma|_{G_n} \in \mathrm{Aut}(G_n)$. *Moreover, for each* $s \in S$ *with* $o(s) > p^n$, $sG_1 \subset S$.

4.2. Proof of Proposition 4.2. With the above notation, suppose the hypothesis of Proposition 4.2 holds throughout this subsection. We first note that Y is imprimitive when $d \ge 2$.

LEMMA 4.3. *Under the hypothesis of Proposition* 4.2, *let* $d \ge 2$. *Then* Y *is imprimitive. Moreover, let* B *be a minimal block of* Y *such that* $1 \in B$. *Then* $B = G_1 = \mathbb{Z}_p$. *Moreover,* $\hat{G}_1 \lhd Y_{G_1}^{G_1}$.

Proof. Since Y is a solvable c-group of degree p^d with $d \ge 2$, Corollary 2.2 implies that Y is not primitive. Let B be a minimal block of Y such that $1 \in B$; then Y_B^B is primitive. Consider the right multiplications by the elements in B; we have $BB = B$. Thus B is a subgroup of G. It follows that Y_B^B is a primitive group containing a cyclic regular subgroup $\hat{B}$. Since Y_B^B is solvable, Corollary 2.2 implies that $B = G_1$ and $\hat{G}_1 \lhd Y_{G_1}^{G_1} \le \mathrm{AGL}(1, p)$. ∎

LEMMA 4.4. *For each* $i \in \{1, 2, \ldots, d-1\}$, G_i *is a block of* Y.

Proof. Suppose that $d - 1 \ge 2$. Let $\mathcal{B} = \{xG_1 \mid x \in G\}$ be the complete block system containing the block G_1. Let $\overline{Y} = Y^{\mathcal{B}}$ be the permutation group on $\mathcal{B}$ induced by Y. Then $\overline{G} = G/G_1 \cong \hat{G}^{\mathcal{B}}$ is regular on $\mathcal{B}$. Thus $\overline{Y}$ is also a solvable c-group of degree p^{d-1}. Applying the same argument of Lemma 4.3, $\overline{G}_2 = G_2/G_1$ is the unique minimal block (containing G_1) of $\overline{Y}$; therefore G_2 is a block of Y. Repeating this argument, we conclude that G_i is a block of Y for each $i \in \{1, 2, \ldots, d-1\}$. ∎

COROLLARY 4.5. *Let* $g \in G$ *with order* p^i, *where* $i \in \{1, 2, \ldots, d\}$. *Let* Y_0 *be the point stabilizer of* 1 *in* Y. *Then each element in the orbit* g^{Y_0} *is of order* p^i. *Moreover,*

$\Gamma_i = \mathrm{Cay}(G_i, S(i))$, *where* $S(i) = \{s \in S \mid o(s) \le p^i\}$ *is a self-complementary graph and* $\sigma|_{G_i} : \Gamma_i \to \overline{\Gamma}_i$ *is an sc-isomorphism.*

Proof. The proof follows from the fact that the point stabilizer Y_0 fixes each block G_i setwise for $i \in \{1, 2, \ldots, d-1\}$. $\square$

Let $\Omega = G$ be the vertex set of Γ. An orbit Δ of Y on $\Omega \times \Omega$ is called an *orbital* of Y on Ω, and the digraph with vertex set Ω and arc set Δ is called an *orbital digraph* of Y. Clearly Y is a subgroup of the automorphism group of this orbital digraph and Y is transitive on both the vertex set Ω and the arc set Δ (that is, this orbital digraph is both Y-vertex-transitive and Y-arc-transitive). We next consider the orbital digraphs of Y. The main tool of our analysis is Theorem 2.3 which is true for both directed and undirected arc-transitive circulants.

LEMMA 4.6. *Under the hypothesis of Proposition* 4.2*, let* $d \ge 2$*. Then either* $\hat{G} \lhd Y$ *and* $\sigma \in \mathrm{Aut}(G)$ *or* $sG_1 \subset S$ *for each* $s \in S$ *with* $o(s) = p^d$*.*

Proof. Let X_0 and Y_0 be the point stabilizers of 1 in X and Y, respectively. Take any $g \in S$ with $o(g) = p^d$. Consider the orbital digraph Γ_g of Y with arc set $\Delta = \{1, g\}^Y$. Then $\Gamma_g = \mathrm{Cay}(G, S_g \cup T_g)$, where $S_g = g^{X_0}$ is a subset of S and $T_g = S_g^\sigma$. Since $o(g) = p^d$, Γ_g is a connected Y-arc-transitive circulant of order p^d.

By Corollary 4.5, $o(h) = p^d$ for any $h \in S_g \cup T_g$. In particular, Γ_g is not the complete graph K_{p^d}. Applying Theorem 2.3, we have either

(i) $\hat{G} \lhd Y$, that is, $Y \le \hat{G} \rtimes \mathrm{Aut}(G)$, in particular, $\sigma \in \mathrm{Aut}(G)$; or

(ii) $gG_1 \subset S_g \cup T_g$.

In the latter case, we claim that $gG_1 \subset S_g \subset S$. Note that by Lemma 4.3, $\mathcal{B} = \{xG_1 \mid x \in G\}$ is a block system of Y. Thus $(gG_1)^\sigma = g^\sigma G_1$. If $gG_1 \cap T_g \ne \varnothing$, then $g^\sigma G_1 \cap S_g \ne \varnothing$, and so there exists $x \in X_0$ such that $g^x \in g^\sigma G_1$. It follows that $(gG_1)^\sigma = (gG_1)^x$ and so $|gG_1 \cap T_g| = |gG_1 \cap S_g|$, contradicting the fact that p is odd. Hence $gG_1 \subset S_g$. The lemma is proved. $\square$

Proof of Proposition 4.2*:* By Lemma 4.6, we may assume that $sG_1 \subset S$ for each $s \in S$ with $o(s) = p^d$. The case $d - 1 = 1$ is an immediate consequence of this and Lemma 4.3.

We can now assume that $d-1 \ge 2$. Note that G_{d-1} is a block of Y. Let $S(d-1) = \{s \in S | o(s) \le p^{d-1}\}$. It follows from Corollary 4.5 that $\Gamma_{d-1} = \mathrm{Cay}(G_{d-1}, S(d-1))$ is self-complementary and $\sigma|_{G_{d-1}}$ is an sc-isomorphism of Γ_{d-1}. Let $X_{d-1} = X_{G_{d-1}}^{G_{d-1}}$ and $Y_{d-1} = Y_{G_{d-1}}^{G_{d-1}}$. Assumption 4.1 holds for Γ_{d-1} when we take $X = X_{d-1}, Y = Y_{d-1}$ in this case. Therefore applying Lemma 4.6, we deduce that either $\widehat{G_{d-1}} \lhd Y_{d-1}$ and $\sigma|_{G_{d-1}} \in \mathrm{Aut}(G_{d-1})$ or $sG_1 \subset S$ for any $s \in S$ with order p^{d-1}.

Continuing in this fashion (note that $\hat{G}_1 \lhd Y_{G_1}^{G_1}$ by Lemma 4.3) we have that an integer n exists such that $n \in \{1, \ldots, d\}$, $\hat{G_n} \lhd Y_{G_n}^{G_n}$ and for each $s \in S$ with $o(s) > p^n$, $sG_1 \subset S$.

4.3. Cayley subsets *S*. Let $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant of order p^d and let $\sigma : \Gamma \to \overline{\Gamma}$ be a self-complementary isomorphism that fixes 1 and is of order a power of 2. We next discuss in more detail the properties of the Cayley subset S when $d \ge 2$.

With the notation of Proposition 4.2, let $X = \mathrm{Aut}(\Gamma)$ and $Y = \langle \mathrm{Aut}(\Gamma), \sigma\rangle$. Then there exists $n \in \{1, \ldots, d\}$ such that $\hat{G_n} \lhd Y_{G_n}^{G_n}$ and for each $s \in S$ with $o(s) > p^n$, $sG_1 \subset S$. Thus we divide the Cayley subset S into the following two parts. Let

$$S_1 = \{s \in S \mid o(s) \le p^n\} \text{ and } S_2 = \{s \in S \mid p^d \ge o(s) \ge p^{n+1}\}. \tag{4.3}$$

Then $S = S_1 \cup S_2$. Note that we set $S_2 = \varnothing$ if $n = d$.

LEMMA 4.7. *Let* $\Gamma = \mathrm{Cay}(G, S)$ *be a self-complementary circulant of order* $p^d (d \geq 2)$ *and let* $\sigma : \Gamma \to \overline{\Gamma}$ *be an sc-isomorphism that fixes* 1 *and is of order a power of* 2. *With the notation of Proposition* 4.2, *let* $X = \mathrm{Aut}(\Gamma)$ *and* $Y = \langle \mathrm{Aut}(\Gamma), \sigma\rangle$. *Suppose* n, S_1, S_2 *are defined as above in* (4.3). *Then the following hold:*

1. *For any* $s \in S_2$, *we have* $sG_1 \subseteq S_2$.
2. $\hat{G}_n \lhd Y_{G_n}^{G_n}$, *in particular,* $\sigma|_{G_n} := \tau \in \mathrm{Aut}(G_n)$.
3. $\Gamma_n := \mathrm{Cay}(G_n, S_1)$ *is self-complementary, and* τ *is an isomorphism from* Γ_n *to its complement. So* Γ_n *is sc-normal and* $S_1 \in S(p^n, \tau)$ *that is defined in* (3.1) *in section* 3.
4. *Let* $X_n = X_{G_n}^{G_n}$ *and let* $S(p^n, \tau, X_n)$ *be the subset of* $S(p^n, \tau)$ *such that each element of* $S(p^n, \tau, X_n)$ *is the union of some orbits of the stabilizer of* 1 *in* X_n *on the set* $G_n^{\#}$. *Then* $S_1 \in S(p^n, \tau, X_n)$.
5. *Given* $R \in S(p^n, \tau, X_n)$, *let* $S' = R \cup S_2$. *Then* $\Gamma' = \mathrm{Cay}(G, S')$ *is also self-complementary such that* $(\Gamma')^\sigma = \overline{\Gamma'}$ *and* $X = \mathrm{Aut}(\Gamma) \leq \mathrm{Aut}(\Gamma')$.
6. *Suppose further that* $n \geq 2$. *Then there exists* $R \in S(p^n, \tau, X_{G_n}^{G_n})$ *such that* $rG_1 \subset R$ *for any* $r \in R$ *with order greater than* p.

Proof. Parts (1) and (2) follow from Proposition 4.2. Part (3) follows from Corollary 4.5 and Lemma 3.1.

(4) Let L be the stabilizer of 1 in X_n. Since $X_n = \hat{G}_n \rtimes L$, where $L \subset \mathrm{Aut}(G_n, S_1)$, we have that S_1 is the union of the orbits of L on $G_n^{\#}$.

(5) The result is trivial if $d = n$, so we suppose that $d > n$. Since $R \in S(p^n, \tau)$, it follows from Lemma 3.1 that $\mathrm{Cay}(G_n, R)$ is self-complementary such that τ maps $\mathrm{Cay}(G_n, R)$ to its complement. Moreover, $X_{G_n}^{G_n} \leq \mathrm{Aut}(\mathrm{Cay}(G_n, R))$ as $R \in S(p^n, \tau, X_n)$.

For any $x \in X$, $g \in G$, and $r \in S' = R \cup S_2$, we have $(g, rg)^x = (1, r)^{\hat{g}x}$. Since $X = \hat{G}X_0$, where X_0 is the point stabilizer of vertex 1 and $\hat{g}x \in X$, there exist $g_0 \in G$ and $x_0 \in X_0$ such that $\hat{g}x = x_0\hat{g}_0$. Therefore, $(g, rg)^x = (1, r)^{x_0\hat{g}_0}$. Note that $X_0 \leq X_{G_n}$. If $r \in R$, then $(1, r)^{x_0} = (1, r')$ for some $r' \in R$. If $r \in S_2$, then by Corollary 4.5 we have $(1, r)^{x_0} = (1, r')$ for some $r' \in S_2$. It then follows easily that X preserves the edge set of Γ', and so $X \leq \mathrm{Aut}(\Gamma')$.

Next we show that Γ' is self-complementary. Since $(\hat{G})^\sigma \leq X^\sigma = X$ for any $g \in G$, there exists $x \in X$ such that $\hat{g}\sigma = \sigma x$. It then follows that $(g, s'g)^\sigma = (1, s')^{\sigma x}$ for any $s' \in S'$. By our definition of Γ', $(1, s')^\sigma$ is not an edge in Γ'. Hence $X \leq \mathrm{Aut}(\Gamma')$ implies that $\Gamma' = \mathrm{Cay}(G, S')$ is also self-complementary and $(\Gamma')^\sigma = \overline{\Gamma'}$. Part 5 is proved.

(6) Suppose that $X_n = \hat{G}_n \rtimes L$, where $L \leq \mathrm{Aut}(G_n, S_1)$ and $\tau^2 \in L$. By Lemma 4.4, $\mathcal{B}_1 = \{gG_1 \mid g \in G_n\}$ forms a complete block system of $\langle X_n, \tau\rangle$ on G_n. For any $gG_1 \in \mathcal{B}_1$ such that $gG_1 \neq G_1$, we have $|gG_1 \cap S_1| \neq |g^\tau G_1 \cap S_1|$ as p is odd, and so $g^\tau G_1 \neq (gG_1)^x$ for any $x \in L$. Thus we may suppose that L has even, say, $2m_2$, orbits on $\mathcal{B}_1 \backslash \{G_1\}$. After relabeling if necessary, we may suppose that $\{\Sigma_1, \ldots, \Sigma_{2m_2}\}$ are L-orbits such that τ interchanges Σ_{2i-1} and Σ_{2i} for each i.

Let

$$R_1 = \bigcup_{i=0}^{m_2-1} \Sigma_{2i+1} \text{ and } S_0 = \{s \in S_1 \mid o(s) = p\}.$$

Take $R = S_0 \cup R_1$. It is easy to see that $R \in S(p^n, \tau, X_n)$ and $rG_1 \subset R$ for any $r \in R$ with order $> p$. ∎

With the notation of Lemma 4.7, take R as in Lemma 4.7(6) and construct $\Gamma' = \mathrm{Cay}(G, R \cup S_2)$. Then Γ' is closely related to the original Γ by the above lemma.

It now follows from Lemma 3.3 that Γ' is a lexicographic product self-complementary circulant. We summarize this observation in the following corollary that allows us to use induction to classify all self-complementary circulants of order p^d.

COROLLARY 4.8. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant of order $p^d (d \geq 2)$ and let $\sigma : \Gamma \to \overline{\Gamma}$ be an sc-isomorphism that fixes 1 and is of order a power of 2. Suppose further that n, S_1, S_2 are defined as in (4.3). Then there exists a self-complementary circulant $\Gamma' = \mathrm{Cay}(G, S')$ satisfying the following conditions:*

(i) *σ is also an sc-isomorphism of Γ' and $\mathrm{Aut}(\Gamma) \leq \mathrm{Aut}(\Gamma')$.*

(ii) *For any $r \in S'$ such that $o(r) > p$, we have $rG_1 \subseteq S'$. So $\Gamma' = \Sigma[\Gamma_1]$, where Γ_1 is a self-complementary circulant of order p and Σ is a self-complementary circulant of order p^{d-1}.*

(iii) *Let $S'_2 = \{r \in S' | o(r) > p^n\}$; then $S'_2 = S_2$.*

(iv) *Let $S'_1 = \{r \in S' | o(r) \leq p^n\}$ and let $\tau = \sigma|_{G_n}$. Then $\tau \in \mathrm{Aut}(G_n)$ and $\tau : S'_1 \to G_n^{\#} \backslash S'_1$.*

5. Proof of Theorem 1.1.

PROPOSITION 5.1. *Suppose that $\Gamma = \mathrm{Cay}(\mathbb{Z}_p, S)$ is a self-complementary circulant of order p. Then Γ is sc-normal.*

Proof. The proof follows from Proposition 4.2 easily. $\square$

Hence Construction 3.2 tells us how to construct all self-complementary circulants of order p.

Suppose $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ is sc-normal with respect to $\tau \in \mathrm{Aut}(\mathbb{Z}_{p^d})$ and $o(\tau)$ is a power of 2. We next study the properties of τ.

LEMMA 5.2. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant of order p^d and $G = \mathbb{Z}_{p^d}$. Let $\tau \in \mathrm{Aut}(G)$ be an sc-isomorphism of order 2^{k_1} from Γ to its complement. Then the following hold:*

(1) *Let $\sigma \in \mathrm{Aut}(G)$. Then σ is an sc-isomorphism of order 2^{k_2} from Γ to its complement if and only if $o(\sigma) = o(\tau)$.*

(2) *Let $\tau_i = \tau|_{G_i} \in \mathrm{Aut}(G_i)$, where G_i is the subgroup of order p^i and $1 \leq i \leq d$. Then $o(\tau_i) = o(\tau)$ and $\tau_i : S \cap G_i \to G_i^{\#} \backslash (S \cap G_i)$.*

(3) *Let $d \geq 2$ and $1 \leq i < d$. Suppose further that $sG_i \subset S$ for any $s \in S$ with $o(s) > p^i$. Let $\overline{S} = \{sG_i | s \in S, o(s) > p^i\}$ and let $\bar{\tau} \in \mathrm{Aut}(G/G_i)$ which is induced by τ. Then $\mathrm{Cay}(G/G_i, \overline{S})$ is sc-normal with respect to $\bar{\tau}$ and $o(\bar{\tau}) = o(\tau)$.*

Proof. (1) Note that $\tau^m \in \mathrm{Aut}(\Gamma)$ if m is even, while τ^m is an sc-isomorphism if m is odd. The result now follows from the fact that $\mathrm{Aut}(\mathbb{Z}_{p^d})$ is cyclic.

(2) Note that the unique involution $\varsigma : g \mapsto g^{-1}$ is not trivial on G_i; the result then follows from Corollary 4.5.

(3) Let $\mathrm{Aut}(G) = \langle \mu \rangle \times \langle \gamma \rangle = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{d-1}}$. It is easy to check that $\mathrm{Aut}(G/G_i) = \mathrm{Aut}(G)/\langle \gamma^{p^{d-1-i}} \rangle$ and so $o(\tau) = o(\bar{\tau})$. By Lemma 4.4, τ preserves $\mathcal{B} = \{xG_i | x \in G\}$ and hence $\overline{\tau} : \overline{S} \to (G/G_i)^{\#} \backslash \overline{S}$. $\square$

We give some explanation of the above lemma which is useful when we handle sc-normal circulants. Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^d}, S)$ be an sc-normal circulant with respect to $\tau \in \mathrm{Aut}(\mathbb{Z}_{p^d})$ with order 2^{k_1}. Lemma 5.2(1) gives a characterization for all sc-isomorphisms in the Sylow 2-subgroup of $\mathrm{Aut}(\mathbb{Z}_{p^d})$. Next, for any subgroup $\mathbb{Z}_{p^i}$, let $S(i) = \{s \in S | o(s) \leq p^i\}$. We obtain a subgraph $\mathrm{Cay}(\mathbb{Z}_{p^i}, S(i))$ of Γ; Lemma 5.2(1) and (2) tells us this subgraph is also sc-normal with respect to σ_i, where $\sigma_i \in \mathrm{Aut}(\mathbb{Z}_{p^i})$ and $o(\sigma_i) = 2^{k_1}$. Moreover, suppose further that this sc-normal Γ is of lexicographic product type as well, that is, $s\mathbb{Z}_{p^i} \subset S$ for any $s \in S$ with $o(s) > p^i$. Let $\overline{S} = \{s\mathbb{Z}_{p^i} | s \in S, o(s) > p^i\}$. We obtain a quotient graph $\mathrm{Cay}(\mathbb{Z}_{p^d}/\mathbb{Z}_{p^i}, \overline{S})$ of Γ in this case.

Lemma 5.2(1) and (3) tells us that this quotient graph is also sc-normal with respect to $\bar{\sigma}$, where $\bar{\sigma} \in \mathrm{Aut}(\mathbb{Z}_{p^d}/\mathbb{Z}_{p^i})$ is induced by some $\sigma \in \mathrm{Aut}(\mathbb{Z}_{p^d})$ with $o(\sigma) = 2^{k_1}$.

We are ready to prove Theorem 1.1.

Proof of Theorem 1.1. We proceed by induction on d. If $d = 1$, the result follows from Proposition 5.1. Assume inductively the result holds for self-complementary circulants of order $\leq p^{d-1}$, where $d \geq 2$.

Let $G = \mathbb{Z}_{p^d}$ and $\Gamma = \mathrm{Cay}(G, S)$ be a self-complementary circulant of order p^d. Let $\sigma : \Gamma \to \overline{\Gamma}$ be an sc-isomorphism that fixes 1 and is of order a power of 2. Let G_i be the subgroup of order p^i in G for any $i \in \{1, \ldots, d\}$. By Proposition 4.2, there exists $n \in \{1, \ldots, d\}$ such that $\sigma|_{G_n} \in \mathrm{Aut}(G_n)$. If $n = d$, then Γ is sc-normal as required. So we assume next that $n < d$.

By Proposition 4.2, $sG_1 \subseteq S$, where $s \in S$ with $o(s) > p^n$. Let $S_1 = \{s \in S \mid o(s) \leq p^n\}$ and $S_2 = \{s \in S \mid o(s) \geq p^{n+1}\}$. By Corollary 4.8, there exists a self-complementary circulant $\Gamma' = \mathrm{Cay}(G, S')$ such that $\Gamma' = \Sigma[\Gamma_1]$, where Γ_1 is a self-complementary circulant of order p and Σ is a self-complementary circulant of order p^{d-1}. Moreover, letting $S_1' = \{r \in S' | o(r) \leq p^n\}$ and $S_2' = \{r \in S' | o(r) > p^n\}$, we have $S_2' = S_2$.

If $i (\geq 1)$ is maximal such that $\Gamma' = \Sigma_1'[\Sigma_2']$, where Σ_2' is a self-complementary circulant of order p^i and Σ_1' is a self-complementary circulant of order p^{d-i}, then Σ_1' cannot be a lexicographic product of two smaller self-complementary circulants. By induction, Σ_1' is sc-normal.

Suppose first that $i \geq n$; then $rG_i \subseteq S'$ for any $r \in S_2'$ with $o(r) > p^i$ by Lemma 3.3. Since $S_2' = S_2$, $sG_i \subseteq S$ for any $s \in S$ with $o(s) > p^i$. By Lemma 3.3 again, $\Gamma = \Sigma_1[\Sigma_2]$, where Σ_2 is a self-complementary circulant of order p^i and Σ_1 is a self-complementary circulant of order p^{d-i}.

Suppose next that $i < n$. We will show that Γ is sc-normal in this case.

Let $\tau = \sigma|_{G_n}$ and suppose that $o(\tau) = 2^{k_1}$ (as $o(\tau) | o(\sigma)$). By Proposition 4.2 $\tau \in \mathrm{Aut}(G_n)$ and $\tau : S_1 \to G_n^{\#} \backslash S_1$. By Lemma 5.2(1), any element of order 2^{k_1} in $\mathrm{Aut}(G_n)$ maps S_1 to $G_n^{\#} \backslash S_1$. To show Γ is sc-normal, Lemma 5.2 implies that we need to find $\psi \in \mathrm{Aut}(G)$ such that $o(\psi) = 2^{k_1}$ and $\psi(s) \notin S_2$ for any $s \in S_2$.

By Corollary 4.8, $\Gamma_n' = \mathrm{Cay}(G_n, S_1')$ is also sc-normal with respect to τ. On the other hand, $\Gamma' = \Sigma_1'[\Sigma_2']$, where $\Sigma_1' = \mathrm{Cay}(G/G_i, \overline{S}')$ and $\overline{S}' = \{rG_i | r \in S', o(r) > p^i\}$. By induction, we have seen that Σ_1' is sc-normal. Suppose $\bar{\psi} \in \mathrm{Aut}(G/G_i)$ is an sc-isomorphism of Σ_1'. Without loss of generality, we may suppose that $o(\bar{\psi}) = 2^{k_2}$ and $\bar{\psi}$ is induced by $\psi \in \mathrm{Aut}(G)$, where $o(\psi) = 2^{k_2}$. Since $i < n$, we have $rG_i \subseteq S_1'$, where $r \in S_1'$ with $o(r) > p^i$, and so the sc-normal circulant Γ_n' is of lexicographic product type as well. In order to apply Lemma 5.2(2) and (3), we consider $\Gamma'' = \mathrm{Cay}(G_n/G_i, \overline{S}_1')$, where $\overline{S}_1' = \{rG_i | r \in S_1'\}$. By the explanation after Lemma 5.2, Γ'' is both a subgraph of the sc-normal circulant Σ_1' and a quotient graph of the sc-normal circulant Γ_n'. This forces $o(\psi) = o(\tau) = 2^{k_1}$ by Lemma 5.2. By Lemma 4.4 and noting that $S_2' = S_2$ and $\bar{\psi} : \overline{S}' \to (G/G_i)^{\#} \backslash \overline{S}'$, it follows that $\psi(S_2) \cap S_2 = \emptyset$. Therefore Γ is sc-normal with respect to ψ. This completes the proof of the theorem.

REFERENCES

[1] B. Alspach, J. Morris, and V. Vilfred, *Self-complementary circulant graphs*, Ars Combin., 53 (1999), pp. 187–191.

[2] R. A. Beezer, *Sylow subgraphs in self-complementary vertex transitive graphs*, Expo. Math., 24 (2006), pp. 185–194.

[3] E. Dobson, *On self-complementary vertex-transitive graphs of order a product of distinct primes*, Ars Combin., 71 (2004), pp. 249–256.
[4] D. Fronček, A. Rosa, and J. Širáň, *The existence of selfcomplementary circulant graphs*, European J. Combin., 17 (1996), pp. 625–628.
[5] C. D. Godsil, *On the full automorphism group of a graph*, Combinatorica, 1 (1981), pp. 243–256.
[6] R. M. Guralnick, C. H. Li, C. E. Praeger, and J. Saxl, *On orbital partitions and exceptionality of primitive permutation groups*, Trans. Amer. Math. Soc., 356 (2004), pp. 4857–4872.
[7] R. Jajcay and C. H. Li, *Constructions of self-complementary circulants with no multiplicative isomorphisms*, European J. Combin., 22 (2001), pp. 1093–1100.
[8] G. Jones, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory, 5 (2002), pp. 403–407.
[9] I. Kovács, *Classifying arc-transitive circulants*, J. Algebraic Combin., 20 (2004), pp. 353–358.
[10] C. H. Li, *Finite Abelian groups with the m-DCI property*, Ars Combin., 51 (1999), pp. 77–88.
[11] C. H. Li, *The finite primitive permutation groups containing an Abelian regular subgroup*, Proc. London Math. Soc., 87 (2003), pp. 725–748.
[12] C. H. Li, *Permutation groups with a cyclic regular subgroup and arc transitive circulants*, J. Algebraic Combin., 21 (2005), pp. 131–136.
[13] C. H. Li and C. E. Praeger, *Self-complementary vertex-transitive graphs need not be Cayley graphs*, Bull. London Math. Soc., 33 (2001), pp. 653–661.
[14] C. H. Li and C. E. Praeger, *Constructing homogeneous factorisations of complete graphs and digraphs*, Graphs Combin., 18 (2002), pp. 757–761.
[15] C. H. Li and C. E. Praeger, *Finite permutation groups with a transitive cyclic subgroup*, J. Algebra, 349 (2012), pp. 117–127.
[16] V. Liskovets and R. Pöschel, *Non-Cayley-isomorphic self-complementary circulant graphs*, J. Graph Theory, 34 (2000), pp. 128–141.
[17] M. Muzychuk, *Ádám's conjecture is true in the square-free case*, J. Combin. Theory Ser. A, 72 (1995), pp. 118–134.
[18] M. Muzychuk, *On Sylow subgraphs of vertex-transitive self-complementary graphs*, Bull. London Math. Soc., 31 (1999), pp. 531–533.
[19] H. Sachs, *Über selbstcomplementäre graphen*, Publ. Math. Debrecen, 9 (1962), pp. 270–288.
[20] D. A. Suprunenko, *Self-complementary graphs*, Cybernetics, 21 (1985), pp. 559–567.
[21] M. Y. Xu, *Automorphism groups and isomorphisms of Cayley digraphs*, Discrete Math., 182 (1998), pp. 309–320.
[22] B. Zelinka, *Self-complementary vertex-transitive undirected graphs*, Math. Slovaca, 29 (1979), pp. 91–95.
[23] H. Zhang, *Self-complementary symmetric graphs*, J. Graph Theory, 16 (1992), pp. 1–5.