J. Aust. Math. Soc. **111** (2021), 372–385
doi:10.1017/S1446788720000488

NEW CONSTRUCTIONS OF SELF-COMPLEMENTARY CAYLEY GRAPHS

CAI HENG LI, GUANG RAO and SHU JIAO SONG

(Received 18 September 2019; accepted 29 September 2020; first published online 12 January 2021)

Communicated by Michael Giudici

Abstract

Vertex-primitive self-complementary graphs were proved to be affine or in product action by Guralnick *et al.* ['On orbital partitions and exceptionality of primitive permutation groups', *Trans. Amer. Math. Soc.* **356** (2004), 4857–4872]. The product action type is known in some sense. In this paper, we provide a generic construction for the affine case and several families of new self-complementary Cayley graphs are constructed.

2020 *Mathematics subject classification*: primary 05C25; secondary 20B05.

Keywords and phrases: Cayley graph, metacirculant graph, self-complementary graph.

1. Introduction

We denote a graph by $\Gamma = (V, E)$ with vertex set V and edge set E. All graphs and groups discussed in this paper are finite. The *complement* $\overline{\Gamma}$ of a graph Γ is the graph with the same vertex set V such that $\{u, v\}$ is an edge of $\overline{\Gamma}$ if and only if $\{u, v\}$ is not an edge of Γ. A graph is said to be *self-complementary* if it is isomorphic to the complement. An isomorphism between Γ and $\overline{\Gamma}$ is called a *complementing isomorphism*.

The study of self-complementary vertex-transitive graphs has a long history. The first family of examples was constructed by Sachs [26] in 1962 and since then this class of graphs has been studied; see [7, 22, 24, 28] for the work before the 1980s. In the 1990s, the orders of self-complementary vertex-transitive graphs were determined by Muzychuck [23]; we also refer to [1, 8] for the orders of self-complementary circulants. More constructions and characterisations of self-complementary vertex-transitive graphs can be found in [7, 14, 17, 20, 21]. The first family of self-complementary vertex-transitive graphs that are not Cayley graphs was obtained by Li and Praeger [15] in 2001. After 2000, the study of self-complementary vertex-transitive graphs has

This work was partially supported by NSFC (Nos. 61771019, 11701497 and 11771200) and NSFS (No. ZR2017MA022).

been significantly advanced by the work in [11, 16]. More recently, self-complementary vertex-transitive graphs of order pq where p, q are primes were classified [18] and self-complementary metacirculants were studied in [19]. It was shown that the automorphism group of a self-complementary graph is either soluble or has a section of the form $\mathbb{Z}_p^2 : (\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$. One of the motivations of studying self-complementary vertex-transitive graphs is that such graphs are often effectively used as models to find good lower bounds of Ramsey numbers (see [5, 6, 10, 25] for references).

However, it is a bit surprising that there are not many graphs which are known to be self-complementary and vertex-transitive. For instance, to our best knowledge, all known examples of self-complementary Cayley graphs are Cayley graphs of abelian groups. Let ℓ be an integer; it is called a primitive divisor of $p^d - 1$ if $\ell \mid p^d - 1$ but $\ell \nmid p^r - 1$ for all $r < \ell$, where p is a prime. The first result of this paper presents a family of self-complementary Cayley graphs of non-nilpotent groups.

THEOREM 1.1. *Let $R = \mathbb{Z}_p^d{:}\mathbb{Z}_\ell \le \mathrm{AGL}(1, p^d)$, where d is even and p is an odd prime, and ℓ is a primitive divisor of $p^d - 1$. Then there exist Cayley graphs of R which are self-complementary.*

Vertex-primitive self-complementary graphs were proved to be affine or in product action in [11]. The product action type is known in some sense. We present here a generic construction for the affine case. For an integer n and a prime divisor p of n, let n_p be the p part of n, namely, $n_p = p^r$ for some integer r and $n_p \mid n$ such that $\gcd(n_p, n/n_p) = 1$.

THEOREM 1.2. *Let $\Gamma = (V, E)$ be a self-complementary graph such that $\mathsf{Aut}\,\Gamma$ is a primitive affine group on V such that $|V|$ is not a prime. Then $|V| = p^d \equiv 1 \pmod 4$ with p prime and, identifying V with a vector space on $\mathbb{F}_p$ of dimension d, a complementing isomorphism σ has the form*

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_r),$$

where $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ is such that V_i is a subspace of dimension 2^{e_i} $1 \le i \le r$ and $d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r}$, and for each i with $1 \le i \le r$:

(i) *σ_i is an element of $\mathrm{GL}(1, p^{2^{e_i}})$ of order $2^{e_i-1}(p^2-1)_2$; or*
(ii) *$e_i = 1$ and $p \equiv 3 \pmod 4$, the order $o(\sigma_i) \ge 4$.*

We remark that, although Theorem 1.2 provides a generic construction method for self-complementary vertex-primitive graphs of affine type, not every example constructed in this way is vertex-primitive. This motivated us to propose a problem.

PROBLEM 1.3. Given a linear transformation σ of a vector space $V = \mathbb{F}_p^d$ of 2-power order which fixes no nonzero vector, determine irreducible subgroups H of $\mathrm{GL}(d, p)$ such that σ normalises H and $\sigma^2 \in H$ fixes no orbit of H on $V \setminus \{0\}$.

Finally, we present a construction of nonabelian metacirculants which are self-complementary. These are Cayley graphs of nonabelian groups.

THEOREM 1.4. *Every metacyclic p-group with* $p \equiv 1 \pmod 4$ *has Cayley graphs which are self-complementary.*

By Berkovic [3], a nonabelian metacyclic group does not have fixed-point-free automorphisms. Thus, self-complementary Cayley graphs of a nonabelian metacyclic group stated in this theorem cannot be constructed by automorphisms of the group; refer to Lemma 3.1.

We end this section with a problem regarding self-complementary metacirculants. It is conjectured in [19] that self-complementary metacirculants are Cayley graphs. We further propose here the following conjecture.

CONJECTURE 1.5. Let R be a metacyclic group that has self-complementary Cayley graphs. Then, for each prime divisor p of $|R|$, either $p \equiv 1 \pmod 4$ or a Sylow p-subgroup of R is homocyclic; that is, R is isomorphic to either a cyclic group of order p^k or the direct product of two cyclic groups of order p^k.

2. Preliminaries

All results stated in this section are standard observations in relation to this topic. We just list them here and give some short explanations. For a self-complementary graph Γ, an automorphism of Γ is also an automorphism of $\overline{\Gamma}$ and hence $\mathsf{Aut}\,\Gamma = \mathsf{Aut}\,\overline{\Gamma}$. Let σ be an isomorphism σ between Γ and $\overline{\Gamma}$. Then $\Gamma^\sigma = \overline{\Gamma}$ and $\overline{\Gamma}^\sigma = \Gamma$. Further, $(\mathsf{Aut}\,\Gamma)^\sigma = \mathsf{Aut}\,\overline{\Gamma} = \mathsf{Aut}\,\Gamma$, namely, a complementing isomorphism normalises the automorphism group. Thus, the following lemma holds.

LEMMA 2.1. *Let* Γ *be a self-complementary graph and let* σ *be a complementing isomorphism. Then* σ *normalises* $\mathsf{Aut}\,\Gamma$ *and* $\sigma^2 \in \mathsf{Aut}\,\Gamma$.

Let $\Gamma = (V, E)$ be a regular self-complementary graph of order n and valency k. Then the complement $\overline{\Gamma}$ is of valency k. Hence, $(n-1)/2 = k$ is an integer and n is odd. The number of edges $|E| = nk/2$ is an integer. Thus, $k = (n-1)/2$ is even and $n-1$ is divisible by 4.

LEMMA 2.2. *The order of a regular self-complementary graph is congruent to* 1 *modulo* 4.

Since a complementing isomorphism σ interchanges Γ and $\overline{\Gamma}$, replacing σ by an odd power of σ, we may assume that σ is of 2-power order. Since n is odd, σ fixes some vertex and, since σ fixes no edge of Γ and $\overline{\Gamma}$, this implies that σ fixes exactly one vertex. Furthermore, σ does not fix any 2-subset of the vertex set and, therefore, σ is of order divisible by 4.

LEMMA 2.3. *A complementing isomorphism of a regular self-complementary graph has order divisible by* 4 *and fixes exactly one vertex of the graph.*

Suppose that $\Gamma = (V, E)$ is self-complementary and vertex-transitive. Let $G = \mathsf{Aut}\,\Gamma$ and let σ be a complementing isomorphism. Let $X = \langle G, \sigma\rangle$. Then G is normal in X of index 2. Let B be a block for X acting on V that is fixed by σ setwise, and let $[B]_\Gamma$ be the *induced subgraph* of Γ on B. Then we have the following result.

LEMMA 2.4. *The induced subgraph $[B]_\Gamma$ is self-complementary, G_B^B is vertex-transitive on $[B]_\Gamma$, and the restriction $\sigma|_B$ is a complementing isomorphism between $[B]_\Gamma$ and $\overline{[B]_\Gamma} = [B]_{\overline{\Gamma}}$.*

We remark, however, that a quotient graph $\Gamma_{\mathcal{B}}$ of a self-complementary graph Γ is not necessarily self-complementary; refer to [16].

Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ be graphs. Then the *lexicographic product* of Γ_1 and Γ_2 is the graph with vertex set $V_1 \times V_2$ such that two vertices (u_1, u_2) and (v_1, v_2) are adjacent if and only if either $\{u_1, v_1\} \in E_1$, or $u_1 = v_1$ and $\{u_2, v_2\} \in E_2$. This graph is denoted by $\Gamma_1[\Gamma_2]$. The lexicographic product provides a method for constructing self-complementary vertex-transitive graphs based on the following proposition; see [2].

PROPOSITION 2.5. *If both Γ_1 and Γ_2 are self-complementary (vertex-transitive), then so is $\Gamma_1[\Gamma_2]$.*

Most known examples of self-complementary vertex-transitive graphs are Cayley graphs. For a finite group R with identity 1 and a subset $S \subset R^\#$ where $R^\# = R \setminus \{1\}$, a *Cayley graph* $\mathsf{Cay}(R, S)$ is the graph with vertex set R such that two vertices $x, y \in R$ are adjacent if and only if $yx^{-1} \in S$. By the definition, we have:

(1) $\mathsf{Cay}(R, S)$ is undirected if and only if $S = S^{-1} = \{s^{-1} \mid s \in S\}$;
(2) the complement of $\mathsf{Cay}(R, S)$ is the Cayley graph $\mathsf{Cay}(R, R^\# \setminus S)$;
(3) $\mathsf{Cay}(R, S)$ is vertex-transitive because the right multiplications of elements of R on the vertex set are automorphisms of the Cayley graph and regular on the vertex set.

The next lemma is well known; see, for instance, [4, Proposition 16.3].

LEMMA 2.6. *A graph Γ is a Cayley graph of a group R if and only if $\mathsf{Aut}\,\Gamma$ contains a subgroup which is isomorphic to R and regular on the vertex set.*

We shall study a method for constructing self-complementary Cayley graphs in the next section.

For an element g of a group G, let g_p be the *p-part* of g, which is such that $g = g_p h = h g_p$, the order $o(g_p)$ is a power of p, and the order of h is coprime to p. Recall that for a prime p and a positive integer d, a *primitive divisor* of $p^d - 1$ is a divisor of $p^d - 1$ that does not divide $p^i - 1$ for any integer $i < d$.

3. Fixed-point-free automorphisms of groups

We first introduce a classical method for constructing self-complementary Cayley graphs, which has been used to construct most known examples of self-complementary vertex-transitive graphs in the literature.

Observe that, given a Cayley graph $\Gamma = \mathsf{Cay}(R, S)$, each automorphism $\sigma \in \mathsf{Aut}(R)$ induces an isomorphism from $\mathsf{Cay}(R, S)$ to $\mathsf{Cay}(R, S^\sigma)$. Thus, if a subset $S \subset R$ and an automorphism σ are such that

$$S^\sigma = R^\# \setminus S,$$

then Γ is self-complementary, and σ is a complementing isomorphism because

$$\Gamma = \mathsf{Cay}(R, S) \cong \mathsf{Cay}(R, S^\sigma) = \mathsf{Cay}(R, R^\# \setminus S) = \overline{\Gamma}.$$

We shall refer to such a set S as an *SC-subset* with respect to σ.

Since $S \cap S^\sigma = S \cap (R^\# \setminus S) = \emptyset$, the automorphism σ is *fixed-point-free*, namely, σ fixes no nonidentity element of R. Moreover, if Γ is undirected, then $S = S^{-1}$, the square σ^2 is fixed-point-free too, and, since σ^2 fixes both S and $R^\# \setminus S$ setwise, we may choose σ to be a 2-*element*, that is, the order of σ is a power of 2.

This observation leads to the following lemma, which is well known.

LEMMA 3.1. *Let R be a group that has an automorphism σ of order a power of 2 such that σ^2 is fixed-point-free. Then there exist Cayley graphs of R that are self-complementary with complementing isomorphism σ.*

PROOF. Let $\Delta_1, \Delta_2, \ldots, \Delta_{2m}$ be the orbits of $\langle \sigma^2 \rangle$ on $R^\#$ such that $\Delta_i^\sigma = \Delta_{i+1}$ for all odd subscripts i. Let

$$S = \Delta_1 \cup \Delta_3 \cup \cdots \cup \Delta_{2m-1},$$

that is, S is the union of all Δ_{2i-1} with $1 \le i \le m$. Then

$$R^\# \setminus S = \Delta_2 \cup \Delta_4 \cup \cdots \cup \Delta_{2m} = \Delta_1^\sigma \cup \Delta_3^\sigma \cup \cdots \cup \Delta_{2m-1}^\sigma = S^\sigma.$$

Let $\Gamma = \mathsf{Cay}(R, S)$. Then $\Gamma = \mathsf{Cay}(R, S) \cong \mathsf{Cay}(R, S^\sigma) = \mathsf{Cay}(R, R^\# \setminus S) = \overline{\Gamma}$ and $\mathsf{Cay}(R, S)$ is self-complementary. □

This lemma provides a generic method for constructing self-complementary Cayley graphs. It has been used to construct examples of self-complementary circulants in the literature by Sachs in 1962 [26], Zelinka in 1979 [28], Suprunenko in 1985 [27], Rao in 1985 [24], and more recent work [7, 29].

This construction method leads us to the following group-theoretic problem.

PROBLEM 3.2. Characterise finite groups that have fixed-point-free automorphisms of order a power of 2.

This problem has been studied in the literature. Gorenstein and Herstein [9] showed that if a group has a fixed-point-free automorphism of order 4, then its commutator subgroup is nilpotent. Later, Huhro [13] proved the following general result.

THEOREM 3.3 (Huhro). *If a finite group R has a fixed-point-free automorphism of order 2^n, then its nilpotent height $h(R)$ is at most n.*

Next, we give simple properties regarding groups with fixed-point-free automorphisms.

https://doi.org/10.1017/S1446788720000488 Published online by Cambridge University Press

LEMMA 3.4. *If A has a fixed-point-free automorphism σ and B has a fixed-point-free automorphism τ, then (σ, τ) is a fixed-point-free automorphism of $A \times B$.*

PROOF. Suppose that (σ, τ) fixes a nonidentity element (a, b), where $a \in A$ and $b \in B$. Then $(a, b) = (a, b)^{(\sigma,\tau)} = (a^\sigma, b^\tau)$. Thus, $a^\sigma = a$ and $b^\tau = b$. Since (a, b) is not an identity element, $a \neq 1$ or $b \neq 1$, which is a contradiction. □

For two groups A and B with g.c.d. $(|A|, |B|) = 1$, suppose that $A \times B$ has a fixed-point-free automorphism. Then, for each $b \in B$, only the identity automorphism fixes $(1_A, b)$. Thus, B has a fixed-point-free automorphism and similarly we can show that A also has one. Thus, by Lemma 3.4, the following proposition holds.

PROPOSITION 3.5. *A nilpotent group has a fixed-point-free automorphism if and only if each of its Sylow subgroups has a fixed-point-free automorphism.*

LEMMA 3.6. *If a group has a fixed-point-free automorphism of order a power of a prime p, then so does each of its Sylow subgroups.*

PROOF. Let G be a group that has a fixed-point-free automorphism σ of order p^f. Then the order $|G|$ is coprime to p. Let P be a Sylow subgroup of G. Then P^σ is a Sylow subgroup and, by Sylow's theorem, there exists an element $g \in G$ such that $P^{\sigma g} = (P^\sigma)^g = P$.

Suppose that a nonidentity element $x \in P$ is fixed by σg. Then

$$x^\sigma = x^{g^{-1}}$$

and so $x = x^{\sigma^{p^f}} = x^{g^{-p^f}}$. Since the order $o(g)$ is relatively prime to p, we conclude that $x^{g^{-1}} = x$ and so $x^\sigma = x$, which is a contradiction. □

This shows that a critical case for solving Problem 3.2 is to characterise finite p-groups with p prime that have fixed-point-free automorphisms of order a power of 2.

4. Self-complementary Cayley graphs of non-nilpotent groups

In this section, we present an infinite family of self-complementary Cayley graphs of non-nilpotent groups.

Let $F = \mathbb{F}_{p^d}$ be a field of order p^d, where p is a prime and d is a positive integer. Then the additive group F^+ and the multiplicative group $F^\times$ are such that

$$F^+ \cong \mathbb{Z}_p^d, \quad F^\times = \mathbb{Z}_{p^d-1}.$$

The group $F^\times$ naturally acts on F^+ by multiplication, giving rise to the group $\mathrm{AGL}(1, p^d) = F^+{:}F^\times \cong \mathbb{Z}_p^d{:}\mathbb{Z}_{p^d-1}$. The field F has an automorphism ρ of order d, also called a *Frobenius automorphism*, such that

$$g^\rho = g^p, \quad \text{where } g \in F^\times.$$

This action defines groups: $\Gamma\mathrm{L}(1, p^d) = \langle F^\times, \rho\rangle \cong \mathbb{Z}_{p^d-1}{:}\mathbb{Z}_d$ and

$$\mathrm{A}\Gamma\mathrm{L}(1, p^d) = (F^+{:}F^\times){:}\langle\rho\rangle \cong (\mathbb{Z}_p^d{:}\mathbb{Z}_{p^d-1}){:}\mathbb{Z}_d \cong \mathbb{Z}_p^d{:}\Gamma\mathrm{L}(1, p^d).$$

Now we are ready to construct new self-complementary Cayley graphs.

Construction 4.1. Let p be an odd prime and $d = 2^f m$, where $f \geq 2$ and m is odd. Let $\ell = \prod_i l_i$ be such that each l_i is a primitive prime divisor of $p^d - 1$ and $l_i \neq l_j$ if $i \neq j$. Let $g \in F^\times$ be of order ℓ and let

$$R = F^+{:}\langle g\rangle = \mathbb{Z}_p^d{:}\mathbb{Z}_\ell \leq \mathrm{AGL}(1, p^d).$$

Let $z \in F^\times$ be of order $(p^d - 1)_2$ and $\sigma = \rho^m$, and let

$$\tau = \sigma z.$$

The group R is a Frobenius group, so it is not nilpotent. The next lemma shows that τ is a fixed-point-free automorphism of R, giving rise to self-complementary graphs.

Lemma 4.2. *The automorphism $\tau \in \mathrm{Aut}(R)$ is of order $(p^d - 1)_2 = 2^f(p - 1)_2$ and τ^2 fixes no nonidentity element of R.*

Proof. Since the order of the Frobenius automorphism ρ is $2^f m$, the order of $\sigma = \rho^m$ equals 2^f and, by definition,

$$x^\sigma = x^{p^m}, \quad \text{where } x \in \mathrm{GL}(1, p^d).$$

In particular, $z^\sigma = z^{p^m}$, and so $\tau^2 = \sigma z \sigma z = \sigma^2 z^{p^m+1}$, and

$$\tau^{2^i} = \sigma^{2^i} z^{(p^{2^{i-1}m}+1)\cdots(p^{2m}+1)(p^m+1)}.$$

Let $2^s = (p^m - 1)_2$ be the 2-part of $p^m - 1$. Then $2^s = (p - 1)_2$. Since $\sigma^{2^f} = 1$, we have that $\tau^{2^f} \in \langle z\rangle$ is of order 2^s and τ is of order $2^f \cdot 2^s = o(\tau) = o(z) = 2^f(p^m - 1)_2$. Further, as m is odd, $(p^m - 1)_2 = (p - 1)_2$. Thus, $o(\tau) = o(z) = 2^f(p - 1)_2$.

Let z_0 be the unique involution of $\langle z\rangle$. Then $z_0 \in \langle\tau^{2^f}\rangle$. Now any element of R may be written as ax such that $a \in \mathbb{Z}_p^d$ and $x \in \langle g\rangle \leq F^\times$. If $a \neq 1$, then

$$(ax)^{z_0} = a^{-1}x \neq ax.$$

Thus, z_0 fixes no point of $R \setminus \langle g\rangle$. This implies that τ^2 and τ fix no point of $R \setminus \langle g\rangle$. On the other hand, if $a = 1$ and $x \neq 1$, then $o(x) \mid \ell$ and, since $xz = zx$,

$$x^{\tau^{2^{f-1}}} = x^{\sigma^{2^{f-1}} z^{(p^{2^{f-2}m}+1)\cdots(p^{2m}+1)(p^m+1)}} = x^{p^{2^{f-1}}}.$$

If $x^{p^{2^{f-1}}} = x^{\tau^{2^{f-1}}} = x$, then $x^{p^{2^{f-1}}-1} = 1$, which is not possible since x is of order dividing ℓ and ℓ is the product of primitive prime divisors of $p^d - 1$. Therefore, τ^2 is a fixed-point-free automorphism of the group R; in particular, τ is a fixed-point-free automorphism of R. □

Proof of Theorem 1.1. By Lemma 3.1, there exist Cayley graphs of R that are self-complementary and τ is a normal complementing isomorphism. □

https://doi.org/10.1017/S1446788720000488 Published online by Cambridge University Press

5. The primitive self-complementary graphs

Let $\Gamma = (V, E)$ be a self-complementary graph and let σ be a complementing isomorphism. Then $\sigma^2 \in \mathsf{Aut}\,\Gamma$ and hence σ normalises $\mathsf{Aut}\,\Gamma$. Let $G = \mathsf{Aut}\,\Gamma$ and let $X = \langle G, \sigma\rangle$. Then G is a normal subgroup of X of index 2 and $X = G.\mathbb{Z}_2$.

Assume that X is primitive on the vertex set V. It is shown in [11, Theorem 1.3] that either:

(i) X is an affine group with socle of odd order; or
(ii) X is in product action with socle $\mathrm{PSL}(2, q^2)^\ell$, and $|V| = (q^2(q^2 + 1)/2)^\ell$, where q is odd and $\ell \geq 2$.

The triple (G, X, Γ) in item (ii) is in some sense known, which gives rise to vertex-transitive self-complementary graphs that are not Cayley graphs; refer to [11] and [15]. On the other hand, the graphs in item (i) are all Cayley graphs of elementary abelian p-groups. In this section, we present a generic construction for this type of self-complementary graph.

Identify the vertex set V with a vector space $\mathbb{F}_p^d$ with p prime. Then the vertices form an additive group which is isomorphic to the elementary abelian group $\mathbb{Z}_p^d$. Since $|V| \equiv 1 \pmod 4$, the prime p is odd. The complementing isomorphism $\sigma \in \mathrm{GL}(d, p)$ is a linear transformation of V and fixes no nonzero vector in V.

CONSTRUCTION 5.1. Decompose the dimension d and the vector space as follows:

$$d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r},$$
$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

where $e_i \geqslant 0$ and V_i is a subspace of V of dimension 2^{e_i}. For each $i (1 \leq i \leq r)$, let $\sigma_i \in \mathrm{GL}_1(p^{2^{e_i}}) \leqslant \mathrm{GL}_{2^{e_i}}(p) = \mathrm{GL}(V_i)$ be such that:

(i) σ_i is of order a 2-power at least 4, if either $e_i = 0$ or both $e_i = 1$ and $p \equiv 3 \pmod 4$;
(ii) σ_i is of order $2^{e_i-1}(p^2 - 1)_2$ for $e_i \geqslant 2$.

Let

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_r).$$

By definition, every σ_i fixes no nonzero vector of V_i and, by Lemma 3.4, σ fixes no nonzero vector of V. The next lemma shows that every complementing isomorphism σ of a primitive affine self-complementary graph is as in the construction.

LEMMA 5.2. *Assume that X is a primitive affine group on the vertex set V. Then each complementing isomorphism has the form given in Construction 5.1.*

PROOF. Let σ be a complementing isomorphism between Γ and $\overline{\Gamma}$. As mentioned before, we may assume that σ is of order 2^f with $f \geq 2$. Let N be the unique minimal

https://doi.org/10.1017/S1446788720000488 Published online by Cambridge University Press

normal subgroup of X. Then $N \cong \mathbb{Z}_p^d$ is regular on the vertex set V and is normalised by σ. Let

$$Y = \langle N, \sigma\rangle = N{:}\langle\sigma\rangle \cong \mathbb{Z}_p^d{:}\mathbb{Z}_{2^f}.$$

Then Y is a subgroup of X and vertex-transitive on the graph Γ.

Case 1. Assume that Y is primitive on the vertex set V. Then the cyclic group $\langle\sigma\rangle$ is irreducible on V and hence the order 2^f is a primitive divisor of $p^d - 1$, that is,

$$2^f \mid (p^d - 1), \text{ but } 2^f \nmid (p^i - 1) \text{ for any } i < d.$$

First, suppose that d is odd. Then

$$p^d - 1 = (p-1)(p^{d-1} + \cdots + p + 1) = (p-1)\ell$$

and ℓ is odd. Thus, $2^f \mid (p-1)$ and, since 2^f is a primitive divisor of $p^d - 1$, we conclude that $d = 1$ and σ is as in Construction 5.1 with $r = 1$.

Assume next that d is even. Write $d = 2^k m$, where m is odd. Then

$$p^d - 1 = p^{2^k m} - 1 = (p^{2^k} - 1)((p^{2^k})^{m-1} + \cdots + p^{2^k} + 1)$$

and $(p^{2^k})^{m-1} + \cdots + p^{2^k} + 1$ is odd. Thus, we have $2^f \mid (p^{2^k} - 1)$. Since 2^f is a primitive divisor of $p^d - 1$, we have that $m = 1$ and $d = 2^k$.

Suppose first that $k = 1$. Then $p^d - 1 = p^2 - 1 = (p-1)(p+1)$. If $p \equiv 3 \pmod 4$, then 4 is a primitive divisor of $p^d - 1$ as in Construction 5.1 with $r = 1$. If $p \equiv 1 \pmod 4$ and $2^f < (p^2 - 1)_2$, then $2^f \mid p - 1$, which contradicts the fact that 2^f is a primitive divisor of $p^2 - 1$. Thus, $2^f = (p^2 - 1)_2$, as in Construction 5.1 with $r = 1$.

Now suppose that $k \geq 2$. Then

$$p^d - 1 = p^{2^k} - 1 = (p^{2^{k-1}} + 1)(p^{2^{k-1}} - 1)$$

and $p^{2^{k-1}} - 1$ is divisible by 4. This implies that $p^{2^{k-1}} + 1$ is not divisible by 4. If $2^f < (p^d - 1)_2$, then 2^f divides $p^{2^{k-1}} - 1$, which contradicts the fact that 2^f is a primitive divisor of $p^d - 1$. So, 2^f equals the 2-part $(p^d - 1)_2$. Moreover,

$$p^{2^k} - 1 = (p^{2^{k-1}} + 1)\cdots(p^2 + 1)(p^2 - 1)$$

and, as $(p^{2^i} + 1)_2 = 2$ for $i \geq 1$, we have $o(\sigma) = (p^{2^k} - 1)_2 = 2^{k-1}(p^2 - 1)_2$, as claimed in the lemma.

Case 2. Assume that Y is imprimitive. Then the cyclic group $\langle\sigma\rangle$ is reducible on V. By Maschke's theorem, the space V is a direct sum

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

such that $\langle\sigma\rangle$ fixes and is irreducible on each subspace V_i, where $1 \leq i \leq r$. Since σ fixes no nonzero vector of V, σ fixes no nonzero vector of the subspace V_i. Let σ_i be the linear transformation of V_i induced by σ. Then V_i and σ_i satisfy Case 1 and we conclude that

$$V_i = \mathbb{F}_p^{2^{e_i}}, \quad \text{where } e_i \geq 0,$$

such that $\sigma_i \in \mathrm{GL}(1, p^{2^{e_i}})$ is of order $2^{e_i-1}(p^2-1)_2$ if $e_i > 0$ and is of order at least 4 otherwise. Now the dimension

$$d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r}$$

and the complementing isomorphism σ can be expressed as

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_r).$$

This completes the proof. □

PROOF OF THEOREM 1.2. This proof follows from Construction 5.1 and Lemma 5.2. □

6. Self-complementary metacirculants

To state our construction, we need to prove an elementary number-theoretic lemma. For positive integers n and λ, the smallest positive integer m such that $\lambda^m \equiv 1 \pmod n$ is called the *order of λ modulo n* and is denoted by $o(\lambda \bmod n)$. As usual, $\phi(n)$ is the Euler phi-function, which is the number of positive integers that are less than n and coprime to n.

LEMMA 6.1. *Given $r \geqslant 2$ and a prime p such that $2^r \leqslant (p-1)_2$, for any p-powers p^e and p^f, there exists a positive integer λ such that $o(\lambda \bmod p^e) = 2^r$ and $o(\lambda \bmod p^f) = 2^r$.*

PROOF. By Euler's theorem, there exists an integer λ_0 such that

$$\lambda_0^{\phi(p^e)} \equiv 1 \pmod{p^e}.$$

As $\phi(p^e) = p^{e-1}(p-1)$, we have 2^r divides $\phi(p^e)$. Let $\lambda = \lambda_0^{\phi(p^e)/2^r}$. Then $\lambda^{2^r} \equiv 1 \pmod{p^e}$ and $o(\lambda \bmod p^e) = 2^r$.

Without loss of generality, assume that $f < e$. Then $\lambda^{2^r} \equiv 1 \pmod{p^f}$. Thus, the order $o(\lambda \bmod p^f)) = 2^s$ for some integer $s \leqslant r$, that is,

$$\lambda^{2^s} = 1 + mp^f \quad \text{for some integer } m.$$

Suppose that $s < r$. The 2^{r-s}th power λ^{2^s} has the form

$$\begin{aligned}\lambda^{2^r} &= (\lambda^{2^s})^{2^{r-s}} = (1 + mp^f)^{2^{r-s}} \\ &= 1 + \binom{2^{r-s}}{1} mp^f + \binom{2^{r-s}}{2} (mp^f)^2 + \cdots + (mp^f)^{2^{r-s}}.\end{aligned}$$

Let $t = \mathrm{Min}\,\{2f, e\}$. Then

$$1 \equiv \lambda^{2^r} \equiv 1 + \binom{2^{r-s}}{1} mp^f \pmod{p^t}.$$

https://doi.org/10.1017/S1446788720000488 Published online by Cambridge University Press

This implies that $f = t = e$, which is a contradiction. Thus, $s = r$, completing the proof. □

Let R be a metacyclic p-group, where p is a prime congruent to 1 modulo 4. Then R has a presentation, refer to [12]:

$$R = \langle a, b \mid b^{p^d} = 1, a^{p^t} = b^{p^m}, aba^{-1} = b^{1+p^f} \rangle.$$

Let $e = t + d - m$. The order $o(a) = p^{t+d-m} = p^e$. Let $c = b^{p^f}$. Then the commutator subgroup

$$R' = \langle c \rangle \cong \mathbb{Z}_{p^{d-f}}.$$

Let σ be an automorphism of $\langle b \rangle$, and τ be an automorphism of $\langle a \rangle$ such that σ, τ are of order 2^r, and $4 \leqslant 2^r \leqslant (p-1)_2$. By Lemma 6.1, there exists a positive integer λ such that

$$b^\sigma = b^\lambda, \quad a^\tau = a^\lambda.$$

Let $S_1 \subset \langle b \rangle$ be an SC-subset with respect to σ; namely, S_1 and σ satisfy $S_1^\sigma = \langle b \rangle^\# \setminus S_1$. Then, for any elements $x = b^{j_1}$ and $y = b^{j_2}$,

$$b^{j_2 - j_1} = yx^{-1} \in S_1 \Longleftrightarrow b^{(j_2-j_1)\lambda} = y^\lambda x^{-\lambda} = y^\sigma (x^\sigma)^{-1} \notin S_1.$$

Let $\overline{R} = R/\langle c \rangle = \langle \overline{b}, \overline{a} \rangle \cong \mathbb{Z}_{p^f} \times \mathbb{Z}_{p^e}$. Then the pair (σ, τ) induces an automorphism $\overline{\rho}$ of $\overline{R}$ as follows:

$$(\overline{b}^i \overline{a}^j)^{\overline{\rho}} = \overline{b}^{i\lambda} \overline{a}^{j\lambda} = (\overline{b}^i \overline{a}^j)^\lambda, \quad \text{where } 0 \leqslant i \leqslant p^f - 1 \text{ and } 0 \leqslant j \leqslant p^e - 1.$$

Let $\overline{S}_2 \subset \langle \overline{b}, \overline{a} \rangle$ be an SC-subset with respect to $\overline{\rho}$, which means that $\overline{S}_2^{\overline{\rho}} = \langle \overline{b}, \overline{a} \rangle^\# \setminus \overline{S}_2$. Then the Cayley graph

$$\Sigma = \mathsf{Cay}(\langle \overline{b}, \overline{a} \rangle, \overline{S}_2)$$

is self-complementary with complementing isomorphism $\overline{\rho}$.

Let $I = \{(i, j) \mid \overline{b}^i \overline{a}^j \in \overline{S}_2, 0 \leqslant i \leqslant p^f - 1, 0 \leqslant j \leqslant p^e - 1\}$ and let

$$S_2 = \bigcup_{(i,j) \in I} b^i a^j \langle c \rangle,$$
$$\Gamma_2 = \mathsf{Cay}(R, S_2).$$

We notice that, since $b^{p^f} = c$, elements of R can be written as

$$b^i a^j c^k, \text{ where } 0 \leqslant i \leqslant p^f - 1,\ 0 \leqslant j \leqslant p^e - 1, \text{ and } 0 \leqslant k \leqslant p^{d-f} - 1.$$

By the definition, we have the following conclusion.

Lemma 6.2. *The Cayley graph* $\Gamma_2 = \Sigma[\overline{\mathsf{K}}_{p^f}]$ *and, for any elements* $x = b^{i_1} a^{j_1} c^{k_1}$ *and* $y = b^{i_2} a^{j_2} c^{k_2}$, *where* $0 \leqslant i_1 \neq i_2 \leqslant p^f - 1$, $0 \leqslant j_1, j_2 \leqslant p^e - 1$, *and* $0 \leqslant k_1, k_2 \leqslant p^{d-f} - 1$,

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^\lambda \overline{x}^{-\lambda} = \overline{y}^{\overline{\rho}} (\overline{x}^{\overline{\rho}})^{-1} \notin \overline{S}_2.$$

Now we are ready to present our construction of self-complementary Cayley graphs of the metacyclic group R.

CONSTRUCTION 6.3. Using the notation defined above, let

$$S = S_1 \cup (S_2 \setminus \langle b\rangle)$$

and $\Gamma = \mathsf{Cay}(R, S)$. Define a permutation ρ of the set R:

$$\rho : \ b^i a^j c^k \mapsto b^{i\lambda} a^{j\lambda} c^{k\lambda}, \ \text{ where } 0 \leqslant i \leqslant p^f - 1,\ 0 \leqslant j \leqslant p^e - 1, \text{ and } 0 \leqslant k \leqslant p^{d-f} - 1.$$

We remark that with suitable choices of S_1 and $\overline{S}_2$, the graph Γ produced in this construction is not a lexicographic graph product of smaller graphs.

We note that the map ρ only fixes the identity of R, but ρ is not an automorphism of the group R. The next lemma shows ρ maps Γ to its complement $\overline{\Gamma}$.

LEMMA 6.4. *The Cayley graph Γ defined in Construction 6.3 is self-complementary and ρ is a complementing isomorphism.*

PROOF. Pick two vertices $x = b^{i_1}a^{j_1}c_1$ and $y = b^{i_2}a^{j_2}c_2$, where $0 \leqslant i_1, i_2 \leqslant p^f - 1$, $0 \leqslant j_1, j_2 \leqslant p^e - 1$, and $c_1, c_2 \in \langle c\rangle$. Then

$$\begin{aligned} yx^{-1} &= (b^{i_2}a^{j_2}c_2)(b^{i_1}a^{j_1}c_1)^{-1} \\ &= b^{i_2-i_1}a^{j_2-j_1}c', \\ y^\rho(x^\rho)^{-1} &= (b^{i_2\lambda}a^{j_2\lambda}c_2^\lambda)(b^{i_1\lambda}a^{j_1\lambda}c_1^\lambda)^{-1} \\ &= b^{(i_2-i_1)\lambda}a^{(j_2-j_1)\lambda}c''. \end{aligned}$$

First, assume that $j_2 = j_1$. Then

$$\begin{aligned} &yx^{-1} = b^{i_2-i_1}c' \in b^{i_2-i_1}\langle c\rangle, \\ &y^\rho(x^\rho)^{-1} = b^{(i_2-i_1)\lambda}c'' \in b^{(i_2-i_1)\lambda}\langle c\rangle = y^\sigma(x^\sigma)^{-1}\langle c\rangle. \end{aligned}$$

Both yx^{-1} and $y^\rho(x^\rho)^{-1} \in \langle b\rangle$. By the definition of σ, we have $yx^{-1} \in S_1$ if and only if $y^\sigma(x^\sigma)^{-1} \in \langle b\rangle^\# \setminus S_1$, and $y^\sigma(x^\sigma)^{-1} \in \langle b\rangle^\# \setminus S_1$ if and only if $y^\rho(x^\rho)^{-1} \in R^\# \setminus S_1$.

Assume now that $j_2 \neq j_1$. Then $\overline{y}\,\overline{x}^{-1} = \overline{b}^{i_2-i_1}\overline{a}^{j_2-j_1}$ and $\overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} = \overline{b}^{(i_2-i_1)\lambda}\overline{a}^{(j_2-j_1)\lambda}$. Neither of them is in $\langle b\rangle$. Thus, by the definition of S_2 and $\overline{S}_2$,

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} \in \langle \overline{b}, \overline{a}, \rangle^\# \setminus \overline{S}_2 \Longleftrightarrow y^\rho(x^\rho)^{-1} \in R^\# \setminus S_2.$$

Therefore, x, y are adjacent in Γ if and only if x^ρ, y^ρ are not adjacent in Γ and so ρ is a isomorphism between Γ and $\overline{\Gamma}$. In particular, $\Gamma \cong \overline{\Gamma}$ and ρ is a complementing isomorphism. □

PROOF OF THEOREM 1.4. Let p be a prime that is congruent to 1 modulo 4 and let R be a metacyclic p-group. If R is abelian, then $R = \langle a\rangle \times \langle b\rangle$ and it follows from Lemmas 3.1 and 3.4 that there exist Cayley graphs of R that are self-complementary. If R is nonabelian, then Lemma 6.4 shows that R has Cayley graphs that are self-complementary. □

References

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

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

[3] J. G. Berkovic, 'Finite metacyclic groups', *Sakharth. SSR Mecn. Akad. Moambe* **68** (1972), 529–532.

[4] N. Biggs, *Algebraic Graph Theory*, 2nd edn, Cambridge Mathematical Library (Cambridge University Press, Cambridge, 1993). ISBN: 0-521-45897-8.

[5] V. Chvátal, P. Erdös and Z. Hedrlín, 'Ramsey's theorem and self-complementary graphs', *Discrete Math.* **3** (1972), 301–304.

[6] C. R. J. Clapham, 'A class of self-complementary graphs and lower bounds of some Ramsey numbers', *J. Graph Theory* **3** (1979), 287–289.

[7] R. Figueroa and R. E. Giudici, 'Group generation of self-complementary graphs', in: *Combinatorics and Graph Theory (Hefei, 1992)* (World Scientific, River Edge, NJ, 1993), 131–140.

[8] D. Fronček, A. Rosa and J. Širáň, 'The existence of selfcomplementary circulant graphs', *European J. Combin.* **17** (1996), 625–628.

[9] D. Gorenstein and I. N. Herstein, 'Finite groups admitting a fixed-point-free automorphism of order 4', *Amer. J. Math.* **83** (1961), 71–78.

[10] F. Gulden and P. Tomasta, 'New lower bounds of some diagonal Ramsey numbers', *J. Graph Theory* **7** (1983), 149–151.

[11] R. 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), 4857–4872.

[12] C. E. Hempel, 'Metacyclic groups', *Comm. Algebra* **28**(8) (2000), 3865–3897.

[13] E. I. Huhro, 'Finite groups that admit a 2-automorphism without fixed point', *Mat. Zametki* **23**(5) (1978), 651–657.

[14] R. Jajcay and C. H. Li, 'Constructions of self-complementary circulants with no multiplicative isomorphisms', *European J. Combin.* **22** (2001), 1093–1100.

[15] C. H. Li and C. E. Praeger, 'Self-complementary vertex-transitive graphs need not be Cayley graphs', *Bull. Lond. Math. Soc.* **33**(6) (2001), 653–661.

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

[17] C. H. Li and C. E. Praeger, 'Finite permutation groups with a transitive cyclic subgroup', *J. Algebra* **349** (2012), 117–127.

[18] C. H. Li and G. Rao, 'Self-complementary vertex-transitive graphs of order a product of two primes', *Bull. Aust. Math. Soc.* **89**(2) (2014), 322–330.

[19] C. H. Li, G. Rao and S. J. Song, 'On finite self-complementary metacirculants', *J. Algebraic Combin.* **40** (2014), 1135–1144.

[20] C. H. Li, S. H. Sun and J. Xu, 'Self-complementary circulants of prime-power order', *SIAM J. Discrete Math.* **28** (2014), 8–17.

[21] V. Liskovets and R. Pschel, 'Non-Cayley-isomorphic self-complementary circulant graphs', *J. Graph Theory* **34** (2000) 128–141.

[22] R. Mathon, 'On self-complementary strongly regular graphs', *Discrete Math.* **69** (1988), 263–281.

[23] M. Muzychuck, 'On Sylow subgraphs of vertex-transitive self-complementary graphs', *Bull. Lond. Math. Soc.* **31**(5) (1999), 531–533.

[24] S. B. Rao, 'On regular and strongly regular selfcomplementary graphs', *Discrete Math.* **54** (1985), 73–82.

[25] V. Rödl and E. Šiňajová, 'Note on Ramsey numbers and self-complementary graphs', *Math. Slovaca* **45** (1995), 155–159.

[26] H. Sachs, 'Über selbstcomplementäre graphen', *Publ. Math. Debrecen* **9** (1962), 270–288.

[27] D. A. Suprunenko, 'Selfcomplementary graphs', *Cybernetics* **21** (1985), 559–567.

[28] B. Zelinka, ‘Self-complementary vertex-transitive undirected graphs’, *Math. Slovaca* **29** (1979), 91–95.
[29] H. Zhang, ‘Self-complementary symmetric graphs’, *J. Graph Theory* **16** (1992), 1–5.

CAI HENG LI, Southern University of Science and Technology,
Shenzhen, China
e-mail: lich@sustc.edu.cn

GUANG RAO, The Chinese University of Hong Kong, Shenzhen, China
e-mail: raoguang@cuhk.edu.cn

SHU JIAO SONG, Yantai University,
Yantai, China
e-mail: shujiao.song@ytu.edu.com

https://doi.org/10.1017/S1446788720000488 Published online by Cambridge University Press