New constructions of self-complementary Cayley graphs

Lei Wang

Beijing International Center
for Mathematical Research
Peking University
Beijing, 100871, P. R. China.

wanglei-2468@163.com

Cai Heng Li

Department of Mathematics
South University of Science and Technology
Shenzhen, Guangdong 518055, P. R. China

lich@sustc.edu.cn

Yin Liu

Department of Mathematics
Yunnan Normal University
Kunming, Yunnan 650500, P. R. China

liuyinjiayou@sina.com

Ci Xuan Wu

School of Statistics and Mathematics
Yunnan University of Finance and Economics
Kunming, Yunnan 650221, P. R. China

wucixuan@gmail.com

Submitted: Dec 20, 2016; Accepted: Jul 17, 2017; Published: Jul 28, 2017
Mathematics Subject Classifications: Primary 05C25; Secondary 05E18

Abstract

Self-complementary Cayley graphs are useful in the study of Ramsey numbers, but they are relatively very rare and hard to construct. In this paper, we construct several families of new self-complementary Cayley graphs of order p^4 where p is a prime and congruent to 1 modulo 8.

Keywords: self-complementary graph; Cayley graph; lexicographic product; fixed-point-free automorphism.

1 Introduction

Throughout this paper, all graphs are assumed to be undirected and simple. A graph $\Gamma = (V, E)$ consists of a vertex set V and an edge set E which is a subset of the set $\{\{u, v\} \mid u, v \in V, u \neq v\}$. 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 $u \neq v$, and $\{u, v\}$ is not an edge of Γ. A graph Γ is called vertex-transitive if $\mathsf{Aut}\Gamma$ is transitive on V, Γ is called self-complementary if it is isomorphic to its complement graph, and an isomorphism from Γ to $\overline{\Gamma}$ is called a complementary isomorphism of Γ.

The graphs that are both self-complementary and vertex-transitive are said to be self-complementary vertex-transitive graphs. One of the motivations of studying self-complementary vertex-transitive graphs is to investigate Ramsey numbers. For a positive integer m, we wish to construct a graph Γ with vertex set V such that neither Γ nor $\overline{\Gamma}$ contains a complete subgraph $\mathbf{K}_m$ and $|V|$ is as big as possible. By intuition, the distribution of pairs of elements of V between Γ and $\overline{\Gamma}$ should be "balanced" so that Γ and $\overline{\Gamma}$ should not be very different. In the extreme case, $\Gamma \cong \overline{\Gamma}$. Furthermore, since any induced subgraph of Γ is not isomorphic to $\mathbf{K}_m$, the edges of Γ should be distributed "homogeneously". In the ideal case, Γ is vertex-transitive. Because of this, self-complementary vertex-transitive graphs have been effectively used as models to find good lower bounds of Ramsey numbers (see [4, 5, 9, 24] for references).

The research of self-complementary vertex-transitive graphs has a long history (see the excellent survey of Beezer [2]). In 1962, Sachs [25] constructed the first families of self-complementary circulants (that is, where the automorphism group contains a transitive cyclic subgroup), and since then this class of graphs has been extensively studied (refer to [6, 20, 22, 26]). In 1990s, the orders of general self-complementary vertex-transitive graphs were completely determined by Muzychuck [21], and we also refer to the earlier work in [1, 7] for the orders of self-complementary circulants. More constructions and characterisations of self-complementary vertex-transitive graphs can be found in [12, 15, 18, 19]. In 2001, Li and Praeger [13] constructed the first family of self-complementary vertex-transitive graphs which are not Cayley graphs. After 2001, the study of self-complementary vertex-transitive graphs has been significantly developed by Li and Praeger [14] and their joint work with Guralnick and Saxl [10] for the vertex-primitive case. More recently, self-complementary vertex-transitive graphs of order pq where p, q are primes are classified [16], and self-complementary metacirculants are studied in [17], which form a subclass of self-complementary vertex-transitive graphs.

To the best of our knowledge, examples of self-complementary vertex-transitive graphs seem relatively rare and hard to construct. In this paper, we present serval families of self-complementary Cayley graphs of non-abelian and non-metacyclic p-groups of order p^4. Our main result in some sense complements the work of the second author (with other collaborators) who has constructed a family of self-complementary Cayley graphs of nonabelian metacyclic p-groups (forthcoming).

Theorem 1. *Let G be a non-abelian and non-metacyclic p-group of order p^4, where $p \equiv 1 \pmod{8}$ is a prime. Then there exist self-complementary Cayley graphs of G.*

This paper is organized as follows. After this introduction, we give some preliminary results on both graph theory and group theory in Section 2, and subsequently construct some new examples of self-complementary Cayley graphs in Section 3 and in Section 4, respectively. Finally, we summarize the constructions in Section 5.

2 Preliminaries

In this section, we define some notation and quote some preliminary results which will be used later.

2.1 Self-complementary graphs

Let $\varGamma = (V, E)$ be a self-complementary graph, and let $\sigma \in \mathrm{Sym}(V)$ be a complementing isomorphism from $\varGamma$ to $\overline{\varGamma}$. Then σ interchanges $\varGamma$ and $\overline{\varGamma}$, and has order $o(\sigma) = 2^e b$ for $e \geqslant 1$, where b is an odd number. Observe that $\sigma = \sigma^b \cdot \sigma^{1-b}$, where σ^b is a complementing isomorphism of 2-power order and $\sigma^{1-b} \in \mathsf{Aut}\varGamma$. Thus we may assume a complementary isomorphism σ to be of 2-power order. If σ is of order 2, then σ interchanges some vertices u, v and fixes $\{u, v\}$, which is impossible. So 4 divides the order of σ.

Lemma 2. *A complementing isomorphism of a self-complementary graph has order divisible by* 4.

For a regular self-complementary graph of order n, a vertex has an equal number of neighbours and non-neighbours, and hence n must be an odd number. Furthermore, the graph has precisely half number of edges of the complete graph, and so $n(n-1)/4$ is an integer, and $n \equiv 1(\bmod 4)$.

Lemma 3. *The order of a regular self-complementary graph is congruent to* $1(\bmod 4)$.

We next introduce a classical method for constructing self-complementary graphs. For a finite group G, let $G^\#{:} = G \setminus \{1\}$, the set of all non-identity elements of G. For a subset $S \subseteq G^\#$ with $S = S^{-1}{:} = \{s^{-1} \mid s \in S\}$, the associated *Cayley graph* $\mathrm{Cay}(G, S)$ is the graph with vertex set $V = G$ and edge set $E = \{\{a, b\} \mid a, b \in G, ba^{-1} \in S\}$.

By the definition, the complement of the Cayley graph $\mathrm{Cay}(G, S)$ is $\mathrm{Cay}(G, G^\# \setminus S)$. Let $\varGamma = \mathrm{Cay}(G, S)$. Then each automorphism $\sigma \in \mathsf{Aut}(G)$ induces an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, S^\sigma)$. Hence, if there exist a subset $S \subset G^\#$ and an automorphism $\sigma \in \mathsf{Aut}(G)$ such that

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

then $\varGamma$ is self-complementary, and σ is a complementing isomorphism because

$$\varGamma = \mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S^\sigma) = \mathrm{Cay}(G, G^\# \setminus S) = \overline{\varGamma}.$$

We call such a subset S an *SC-subset* (short form for self-complementing subset), and such an automorphism σ a normal complementing isomorphism. For convenience, we shall refer such a self-complementary Cayley graph as an *SCI graph* of G (SCI stands for *Self-complementary Cayley Isomorphism*).

Another construction method of self-complementary vertex-transitive graphs is based on the so-called *lexicographic product* (sometimes called the *wreath product*). In general, for a graph $\varGamma_1$ with vertex set V_1 and a graph $\varGamma_2$ with vertex set V_2, the lexicographic product $\varGamma_1[\varGamma_2]$ 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 is adjacent to v_1 in Γ_1 or $u_1 = v_1$ and u_2 is adjacent in Γ_2 to v_2. The lexicographic product provides a method for constructing self-complementary graphs based on the following properties (see [2] for references).

Lemma 4. *If both Γ_1 and Γ_2 are self-complementary (vertex-transitive), then so is $\Gamma_1[\Gamma_2]$.*

2.2 Finite *p*-groups.

For a finite group G, the Frattini subgroup $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups. An element g of G is called a nongenerator of G if $G = \langle T, g\rangle$ implies $G = \langle T\rangle$ for any subset T of G.

Lemma 5. ([23, 5.2.12]) *If G is a finite, then $\Phi(G)$ equals the set of nongenerators of G.*

Let G be a finite p-group. Denote by G' the derived subgroup of G. Set $G^p = \langle g^p \mid g \in G\rangle$. The following lemma is called the Burnside Basis Theorem:

Lemma 6. ([23, 5.3.2]) *Let G be a finite p-group, where p is a prime. Then $\Phi(G) = G'G^p$. If $|G{:}\Phi(G)| = p^r$, then every generating set of G has a subset of r elements which also generates G. In particular, $G/\Phi(G) = \mathrm{C}_p^r$, which is elementary abelian of order p^r.*

Let G be a finite p-group. Denote by $c(G)$ the nilpotent class of G. The exponent of G is the largest order of the elements in G, denoted by $\exp(G)$. The group G is called p-abelian if $(xy)^p = x^py^p$ for any $x, y \in G$.

Lemma 7. ([3, Theorem 3.1]) *Let G be a finite p-group which is generated by two elements and whose derived subgroup G' is abelian. Then G is p-abelian if and only if $\exp(G') \leqslant p$ and $c(G) < p$.*

For an odd prime p and a positive integer m, we write p_+^{1+2m} for the extraspecial group of exponent p, and p_-^{1+2m} for the one of exponent p^2. A classification of the non-abelian groups of order p^4 for an odd prime p was given by Huppert [11, Chapter 3, Theorem 12.6 and Exercise 29]. Thus we have the following lemma.

Lemma 8. *Let p be an odd prime and G a non-abelian and non-metacyclic group of order p^4. Then G is one of the following groups:*

(1) $G_1(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1\rangle$;

(2) $G_2(p) = \langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [b, c] = a^p, [a, b] = [a, c] = 1\rangle$;

(3) $G_3(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = a^p, [c, b] = 1\rangle$;

(4) $G_4(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = 1, [c, b] = a^{\nu p}\rangle$, *where ν is 1 or a non-quadratic residue modulo p;*

(5) $G_5(p) = \langle a, b \mid a^p = b^p = c^p = d^p = 1, [a, b] = c, [c, b] = d, [a, d] = [b, d] = [c, d] = [c, a] = 1\rangle$ *for $p > 3$;*
$G_5(3) = \langle a, b, c \mid a^9 = b^3 = c^3 = 1, [a, b] = 1, [a, c] = b, [b, c] = a^{-3}\rangle$;

(6) $G_6(p) = p_-^{1+2} \times \mathrm{C}_p$, *where* C_p *is cyclic of order* p*;*

(7) $G_7(p) = p_+^{1+2} \times \mathrm{C}_p$.

3 SCI graphs

In this section, we will construct self-complementary Cayley graphs via fixed-point-free automorphisms of groups of order p^4, where p is an odd prime. Lemma 9 below provides a generic method for constructing self-complementary Cayley graphs based on fixed-point-free automorphisms of groups. The following lemma is possibly known. As the authors find no proper references, a proof is given.

Lemma 9. *Let G be a finite group. Then there exist SCI graphs of G if and only if G has an automorphism σ of order a power of 2 such that σ^2 is fixed-point-free.*

Proof. Let $\Gamma = \mathrm{Cay}(G, S)$, where $S \subset G^{\#} = G \setminus \{1\}$. Assume first that Γ is an SCI graph. Notice that $S^\sigma = G^{\#} \setminus S$, we have $S \cap S^\sigma = \emptyset$, and hence the automorphism σ is fixed-point-free, namely, σ fixes no non-identity elements of G. Moreover, since $S = S^{-1}$, and σ cannot interchange any pair of vertices, we further obtain that σ^2 is fixed-point-free too, and as σ^2 fixes both S and $G^{\#} \setminus S$, we may assume that σ is a 2-element, that is, the order $o(\sigma) = 2^e$ for some e.

On the other hand, suppose that G has an automorphism σ of order 2^e such that σ^2 is fixed-point-free.

Let Δ be an orbit of $\langle \sigma^2 \rangle$ acting on $G^{\#}$. Let $\Delta^{-1} = \{h^{-1} \mid h \in \Delta\}$. Then, for any $g \in \Delta$, we have $\Delta = g^{\langle \sigma^2 \rangle}$, and $\Delta^{-1} = (g^{-1})^{\langle \sigma^2 \rangle}$, namely, Δ^{-1} is an orbit of $\langle \sigma^2 \rangle$ on $G^{\#}$. We claim that $\Delta^\sigma \cap \Delta^{-1} = \emptyset$. Assume otherwise. Then $g^{\sigma^{2l+1}} = (g^{\sigma^{2l}})^\sigma = g^{-1}$ for some $g \in \Delta$, and hence $g^{\sigma^{2(2l+1)}} = g$. Since σ is of order 2^e, we have $g^{\sigma^2} = g$, which contradicts the fact that σ^2 is fixed-point-free. Thus $\Delta^{-1} \cap \Delta^\sigma = \emptyset$, and $\langle \sigma \rangle$ acts on the set $\{\{g, g^{-1}\} \mid g \in G^{\#}\}$ with no fixed element.

Let $\Delta_1, \Delta_2, \ldots, \Delta_{2k}$ be the orbits of $\langle \sigma^2 \rangle$ acting on $\{\{g, g^{-1}\} \mid g \in G^{\#}\}$ such that

$$\Delta_{2i-1}^\sigma = \Delta_{2i} \text{ for } 1 \leqslant i \leqslant k.$$

Then $\Delta_{2i}^\sigma = \Delta_{2i-1}$. Let

$$S = \Delta_1 \cup \Delta_3 \cup \cdots \cup \Delta_{2k-1}.$$

Since $\Delta_j^{-1} = \Delta_j$, we have $S^{-1} = S$. Moreover,

$$G^{\#} \setminus S = \Delta_2 \cup \Delta_4 \cup \cdots \cup \Delta_{2k} \text{ and } S^\sigma = G^{\#} \setminus S.$$

It follows that the Cayley graph $\Gamma := \mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S^\sigma) = \mathrm{Cay}(G, G^{\#} \setminus S) = \overline{\Gamma}$. Therefore, $\mathrm{Cay}(G, S)$ is self-complementary and the complementing isomorphism is produced by the automorphism σ of G. ☐

For the sake of stating our main results, we derive an elementary number theoretic result. Let n, λ be coprime positive integers. The order of λ modulo n is the least positive integer m such that $\lambda^m \equiv 1 \pmod{n}$, denoted by $\mathrm{ord}_n(\lambda)$. As usual, the order of λ modulo n is a divisor of $\varphi(n)$. If $\mathrm{ord}_n(\lambda) = \varphi(n)$, then λ is called a primitive root modulo n.

Lemma 10. *Let p, λ be coprime positive integers, where p is an odd prime. Assume $\mathrm{ord}_{p^n}(\lambda) = p^{n-1}(p-1)$. Then $\mathrm{ord}_{p^m}(\lambda) = p^{m-1}(p-1)$ where $1 \leqslant m < n$.*

Proof. By Euler's Theorem, $\lambda^{p^{m-1}(p-1)} \equiv 1 \pmod{p^m}$. Assume $\mathrm{ord}_{p^m}(\lambda) = \mu$, where μ is a proper divisor of $p^{m-1}(p-1)$. Calculation shows that $\lambda^{\mu p^{n-m}} \equiv 1 \pmod{p^n}$, which contradicts the hypothesis. Thus the statement follows. □

Lemma 11. *Let $G = G_1(p)$, $G_5(p)$ or $G_7(p)$ be the group defined in Lemma 8. If $p \equiv 1 \pmod{8}$, then G has two fixed-point-free automorphisms σ and σ^2 of 2-power orders.*

Proof. Assume first that $G = G_1(p)$. By Lemma 8, we have

$$G_1(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a,b] = c, [c,a] = [c,b] = 1 \rangle.$$

Now pick a positive integer λ_1 such that $\mathrm{ord}_{p^2}(\lambda_1) = p(p-1)$. By Lemma 10, we have $\mathrm{ord}_p(\lambda_1) = p - 1$. Let σ be such that

$$a^\sigma = a^{\lambda_1^p}, \ \ b^\sigma = b^{\lambda_1} \ \text{and} \ \ c^\sigma = c^{\lambda_1^2}.$$

It is simple to show that σ is an automorphism of G of order $p-1$. Assume that $p \equiv 1 \pmod{8}$. Write $p - 1 = 2^e m$ with m an odd number and $e \geqslant 3$. Then

$$a^{\sigma^m} = a^{\lambda_1^{mp}}, \ b^{\sigma^m} = b^{\lambda_1^m} \ \text{and} \ c^{\sigma^m} = c^{\lambda_1^{2m}}.$$

Suppose, if possible, that there exists some $1 \neq x \in G$ such that $x^{\sigma^m} = x$. By definition of $G_1(p)$, we have $x = a^{i_1} b^{i_2} c^{i_3}$, where $0 \leqslant i_1 \leqslant p^2 - 1$, and $0 \leqslant i_2, i_3 \leqslant p - 1$. If $i_1 = 0$ and $i_2 = 0$, then $x = c^{i_3}$ where $i_3 \neq 0$. Thus

$$(c^{i_3})^{\lambda_1^{2m}} = x^{\sigma^m} = x = c^{i_3}.$$

It follows that $\lambda_1^{2m} \equiv 1 \pmod{p}$, which is a contradiction. Thus, either $i_1 \neq 0$ or $i_2 \neq 0$. Observe that $G' = \langle c \rangle$. Let $\overline{G} = G/G'$. For any $z \in G$, we denote by $\overline{z}$ the image of z in $\overline{G}$. Write $\overline{G} = \langle \overline{a}, \overline{b} \rangle$. Then $\overline{x} = \overline{a}^{i_1} \overline{b}^{i_2} \neq 1$. Since G' is a characteristic subgroup of G, σ^m induces an automorphism τ of $\overline{G}$, namely,

$$(\overline{a}^i \overline{b}^j)^\tau = \overline{a^i b^j}^\tau = \overline{(a^i b^j)^{\sigma^m}} = \overline{(a^i)^{\lambda_1^{mp}}} \ \overline{(b^j)^{\lambda_1^m}} = (\overline{a}^i)^{\lambda_1^{mp}} (\overline{b}^j)^{\lambda_1^m},$$

where i, j are integers. Then we have

$$(\overline{a}^{i_1})^{\lambda_1^{mp}} (\overline{b}^{i_2})^{\lambda_1^m} = \overline{x}^\tau = \overline{x^{\sigma^m}} = \overline{x} = \overline{a}^{i_1} \overline{b}^{i_2}.$$

This implies that $\lambda_1^{mp} \equiv 1 \pmod{p^2}$, again a contradiction. Thus σ^m is a fixed-point-free automorphism of order 2^e. Similarly, σ^{2m} is also fixed-point-free and of order 2^{e-1}.

Assume now that $G = G_5(p)$. By Lemma 8, we have

$$G_5(p) = \langle a, b \mid a^p = b^p = 1, [a, b] = c, [c, b] = d, [a, c] = [a, d] = [b, d] = 1 \rangle.$$

Let $\mathrm{ord}_p(\lambda_2) = p - 1$. Let σ be such that

$$a^\sigma = a^{\lambda_2},\ b^\sigma = b^{\lambda_2},\ c^\sigma = c^{\lambda_2^2} d^{\frac{\lambda_2^2(\lambda_2 - 1)}{2}} \text{ and } d^\sigma = d^{\lambda_2^3}.$$

It is easy to verify that σ is an automorphism of G of order $p-1$. Assume $p \equiv 1 \pmod 8$. Write $p - 1 = 2^e m$ with m an odd number and $e \geqslant 3$. By the definition of σ, we have

$$a^{\sigma^m} = a^{\lambda_2^m},\ b^{\sigma^m} = b^{\lambda_2^m},\ c^{\sigma^m} = c^{\lambda_2^{2m}} d^\ell \text{ and } d^{\sigma^m} = d^{\lambda_2^{3m}},$$

where ℓ is an integer. Arguing similarly as above, we can obtain that σ^m and σ^{2m} are fixed-point-free automorphisms of order 2^e and 2^{e-1}, respectively.

Assume finally that $G = G_7(p)$. Let $H = \langle a, b \mid a^p = b^p = 1, [a, b] = c, c^a = c^b = c \rangle$. By Lemma 8, we have that $G = H \times \langle d \rangle \cong p_+^{1+2} \times \mathrm{C}_p$.

Let $\mathrm{ord}_p(\lambda_3) = p - 1$. Let σ be such that

$$a^\sigma = a^{\lambda_3},\ \ b^\sigma = b^{\lambda_3},\ \ c^\sigma = c^{\lambda_3^2} \ \text{ and } \ d^\sigma = d^{\lambda_3}.$$

It is straightforward to check that σ is an automorphism of G of order $p - 1$. Assume that $p \equiv 1 \pmod 8$. Let $p - 1 = 2^e m$, where m is an odd number and $e \geqslant 3$. Then

$$a^{\sigma^m} = a^{\lambda_3^m},\ \ b^{\sigma^m} = b^{\lambda_3^m},\ \ c^{\sigma^m} = c^{\lambda_3^{2m}} \ \text{ and } \ d^{\sigma^m} = d^{\lambda_3^m}.$$

Arguing as for the group $G_1(p)$, we obtain that σ^m and σ^{2m} are fixed-point-free automorphisms of order 2^e and 2^{e-1}, respectively. This completes the proof of Lemma 11. □

Lemma 12. *Let $G = G_2(p)$ be the group defined in Lemma 8. If $p \equiv 1 \pmod 4$, then G has two fixed-point-free automorphisms σ and σ^2 of 2-power orders.*

Proof. By Lemma 8, we have

$$G_2(p) = \langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [b, c] = a^p, [a, b] = [a, c] = 1 \rangle.$$

Now take a positive integer λ such that $\mathrm{ord}_{p^2}(\lambda) = p(p - 1)$. By Lemma 10, we have $\mathrm{ord}_p(\lambda) = p - 1$. Let σ be such that

$$a^\sigma = a^{-\lambda^p},\ b^\sigma = c^\lambda \text{ and } c^\sigma = b.$$

It is easy to show that σ is an automorphism of G of order $2(p-1)$. Assume $p \equiv 1 \pmod 4$. Write $p - 1 = 2^e m$ with m an odd number and $e \geqslant 2$. Then

$$a^{\sigma^m} = a^{-\lambda^{pm}},\ b^{\sigma^m} = c^{\lambda^{\frac{m+1}{2}}} \text{ and } c^{\sigma^m} = b^{\lambda^{\frac{m-1}{2}}}.$$

Arguing similarly as in Lemma 11, σ^m and σ^{2m} are fixed-point-free automorphisms of order 2^{e+1} and 2^e, respectively. □

Combining Lemma 9 with Lemmas 11-12, we obtain an important conclusion in the next proposition.

Proposition 13. *Let G be a p-group of order p^4, where p is an odd prime. Then one of the following holds:*

(i) *if $p \equiv 1 \,(\mathsf{mod}\ 4)$, then there exist SCI graphs of G when $G = G_2(p)$;*

(ii) *if $p \equiv 1 \,(\mathsf{mod}\ 8)$, then there exist SCI graphs of G when $G = G_1(p)$, $G_5(p)$ or $G_7(p)$.*

4 Non-SCI graphs

In this section, we construct self-complementary Cayley graphs of the groups $G_3(p)$, $G_4(p)$ and $G_6(p)$. For such groups, we have the following lemma.

Lemma 14. *Let $G = G_3(p)$, $G_4(p)$ or $G_6(p)$ be the group defined in Lemma 8. Then the square of each automorphism of G is not fixed-point-free.*

Proof. By Lemma 8, we have

$$G_3(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = a^p, [c, b] = 1\rangle,$$
$$G_4(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = 1, [c, b] = a^{\nu p}\rangle.$$

Let $G = G_3(p)$ or $G_4(p)$. In either case, $\Phi(G) = \langle a^p, c\rangle$ and $\mathbf{Z}(G) = \langle a^p\rangle$. For any $\sigma \in \mathsf{Aut}(G)$, if $p = 3$, then σ^2 centralises $\mathbf{Z}(G)$, and hence σ^2 is not fixed-point-free. Thus we may assume $p > 3$. By Lemma 7, G is p-abelian.

Assume first that $G = G_3(p)$. By the previous paragraph, we may assume

$$a^\sigma = a^{k_1}b^{k_2}c^{k_3},\ b^\sigma = a^{pl_1}b^{l_2}c^{l_3} \text{ and } c^\sigma = c^k a^{pl},$$

where $1 \leqslant k_1 \leqslant p^2 - 1$, $(k_1, p) = 1$, and $0 \leqslant k_i, l_j, k, l \leqslant p - 1$ for $i = 2$ or 3, and $j = 1, 2$ or 3. In particular, $(a^p)^\sigma = (a^{k_1}b^{k_2}c^{k_3})^p = a^{pk_1}$ since G is p-abelian.

By $[c^\sigma, a^\sigma] = (a^p)^\sigma$, we calculate that $[c^k, a^{k_1}] = a^{pk_1}$, and so $a^{pkk_1} = a^{pk_1}$. Thus $pkk_1 \equiv pk_1 \,(\mathsf{mod}\ p^2)$. Since $(k_1, p) = 1$, we obtain $k = 1$. Let $r = c^{t_1}a^{pt_2}$ where $1 \leqslant t_1, t_2 \leqslant p - 1$. Then $r^\sigma = c^{t_1}a^{p(k_1t_2+lt_1)}$. If $k_1 = 1$, then $(a^p)^\sigma = a^p$. Otherwise, let $t_2 = \frac{l}{1-k_1}t_1$, and then $r^\sigma = r$. It follows that G has no fixed-point-free automorphism.

Assume next that $G = G_4(p)$. For any $\sigma \in \mathsf{Aut}(G)$, we may assume

$$a^\sigma = a^{\bar{k}_1}c^{\bar{k}_2},\ b^\sigma = a^{p\bar{l}_1}b^{\bar{l}_2}c^{\bar{l}_3} \text{ and } c^\sigma = a^{p\bar{l}}c^{\bar{k}},$$

where $1 \leqslant \bar{k}_1 \leqslant p^2 - 1$, $(\bar{k}_1, p) = 1$, and $0 \leqslant \bar{k}_i, \bar{l}_j, \bar{k}, \bar{l} \leqslant p - 1$, $(\bar{k}, p) = 1$ for $i = 2$ or 3 and $j = 1, 2$ or 3. By $[c^\sigma, b^\sigma] = (a^{vp})^\sigma$, we compute that $a^{vp\bar{k}\bar{l}_2} = a^{vp\bar{k}_1}$, and thus $\bar{k}_1 \equiv \bar{k}\ \bar{l}_2 \,(\mathsf{mod}\ p)$. By $[a^\sigma, b^\sigma] = c^\sigma$, we obtain $c^{\bar{k}_1\bar{l}_2} = c^{\bar{k}}$, and so $\bar{k} \equiv \bar{k}_1\bar{l}_2 \,(\mathsf{mod}\ p)$. Since $(\bar{k}_1, p) = 1$, we conclude that $\bar{l}_2 \equiv \pm 1 \,(\mathsf{mod}\ p)$.

Let $\overline{G} = G/\Phi(G)$. For any $x \in G$, we denote by $\overline{x}$ the image of x in $\overline{G}$. Since G' is a characteristic subgroup of G, σ induces an automorphism $\overline{\sigma}$ of $\overline{G}$, that is,

$$(\overline{a}^i\overline{b}^j)^{\overline{\sigma}} = \overline{a^ib^j}^{\overline{\sigma}} = \overline{(a^ib^j)^\sigma} = \overline{a^{i\bar{k}_1}}\ \overline{b^{j\bar{l}_2}} = \overline{a}^{i\bar{k}_1}\overline{b}^{j\bar{l}_2},$$

where i, j are integers. This implies that $\bar{b}^{\overline{\sigma}} = \bar{b}^{\bar{l}_2}$, and so $\bar{b}^{\overline{\sigma}^2} = \bar{b}$. In other words, $\overline{\sigma}^2$ is not fixed-point-free. By [8, p.335, Lemma 1.3], σ^2 is not a fixed-point-free automorphism of G. Since σ is arbitrary, the statement holds.

Assume finally that $G = G_6(p)$. Arguing similarly as above, G has no fixed-point-free automorphism. This completes the proof of Lemma 14. □

We remark that when $G = G_3(p)$ or $G_6(p)$, G has no fixed-point-free automorphisms, and when $G = G_4(p)$, the square of each automorphism of G is not fixed-point-free. If there exist self-complementary Cayley graphs of G, then the complementing isomorphism can not be produced by special automorphisms of the group G, see Lemma 9.

In order to state the following construction, we need the next lemma.

Lemma 15. *Let $G = p_+^{1+2} \cong \mathrm{C}_p^2{:}\mathrm{C}_p$, where p is an odd prime. If $p \equiv 1 \,(\mathsf{mod}\ 8)$, then G has two fixed-point-free automorphisms σ and σ^2 of 2-power orders.*

Proof. Now we may write G as follows:

$$G = \langle a, b, c \mid a^p = b^p = c^p = 1, [a, b] = c, [a, c] = [b, c] = 1 \rangle.$$

Assume that $p - 1 = 2^e m$, where m is an odd number, and $e \geqslant 3$. Let λ be a positive integer such that $\mathrm{ord}_p(\lambda) = 2^e$. Let σ be such that

$$a^\sigma = a^\lambda,\ b^\sigma = b^\lambda \text{ and } c^\sigma = c^{\lambda^2}.$$

It is clear that σ and σ^2 are two fixed-point-free automorphisms of 2-power orders. □

Let $p \equiv 1 \,(\mathsf{mod}\ 8)$ be a prime. Write $p - 1 = 2^e m$ with $e \geqslant 3$, and m an odd number. Let

$$G = G_3(p) = \langle a, b \mid a^{p^2} = b^p = c^p = 1, [a, b] = c, [c, a] = a^p, [c, b] = 1 \rangle.$$

Clearly, $\mathbf{Z}(G) = \langle a^p \rangle \cong \mathrm{C}_p$. Set $H = \langle a^p, b, c \rangle \cong \mathrm{C}_p^3$.

Pick a positive integer λ such that $\mathrm{ord}_p(\lambda) = 2^e$. Then we choose $\sigma \in \mathsf{Aut}(H)$ such that

$$(a^p)^\sigma = (a^p)^\lambda,\ \ b^\sigma = b^\lambda \ \text{ and } \ c^\sigma = c^{\lambda^2}.$$

Obviously, σ is a fixed-point-free automorphism of order 2^e. So is σ^2 of order 2^{e-1} as $e \geqslant 3$. By Lemma 9, there exists $S_1 \subset H$ such that S_1 is an SC-subset with respect to σ. Then $S_1^\sigma = H^\# \setminus S_1$, and so for any elements $x = a^{pi_1} b^{j_1} c^{k_1}$ and $y = a^{pi_2} b^{j_2} c^{k_2}$,

$$\begin{aligned} &a^{p(i_2 - i_1)} b^{j_2 - j_1} c^{k_2 - k_1} = y x^{-1} \in S_1 \\ \Leftrightarrow &a^{\lambda p(i_2 - i_1)} b^{\lambda(j_2 - j_1)} c^{\lambda^2 (k_2 - k_1)} = y^\sigma (x^\sigma)^{-1} \notin S_1. \end{aligned}$$

Let $\tau \in \mathsf{Aut}(\langle a \rangle)$ be such that $a^\tau = a^\lambda$, where λ is as above. Let $\overline{G} = G/\mathbf{Z}(G) = \langle \overline{a}, \overline{b}, \overline{c} \rangle = \mathrm{C}_p^2{:}\mathrm{C}_p$. By Lemma 15, the pair (σ, τ) induces a fixed-point-free automorphism $\overline{\rho}$ of $\overline{G}$. So does $\overline{\rho}^2$ for $e \geqslant 3$.

Again by Lemma 9, we may let $\overline{S}_2 \subset \overline{G}^{\#}$ be an SC-subset with respect to $\overline{\rho}$. Then $\overline{S}_2^{\overline{\rho}} = \overline{G}^{\#} \setminus \overline{S}_2$, and Cayley graph

$$\Sigma = \mathrm{Cay}(\overline{G}, \overline{S}_2)$$

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

Let $I = \{(i,j,k) \mid \overline{a}^i \overline{b}^j \overline{c}^k \in \overline{S}_2, 0 \leqslant i,j,k \leqslant p-1\}$. Set

$$\begin{array}{rcl} S_2 & = & \cup_{(i,j,k)\in I} a^i b^j c^k \langle a^p \rangle, \\ \Gamma_2 & = & \mathrm{Cay}(G, S_2). \end{array}$$

Let $a^p = d$. We observe that each element of G can be written as

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

By the definition, we have the conclusion in the next lemma.

Lemma 16. *The Cayley graph $\Gamma_2 = \Sigma[\overline{\mathbf{K_p}}]$, and for any elements $x = a^{i_1} b^{j_1} c^{k_1} d^{l_1}$ and $y = a^{i_2} b^{j_2} c^{k_2} d^{l_2}$ with $(i_1, j_1, k_1) \neq (i_2, j_2, k_2)$, we have*

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

With this preparation, we are ready to present our construction of self-complementary Cayley graphs of the group $G_3(p)$.

Construction 17. With the notation above, let

$$\begin{array}{rcl} S & = & S_1 \cup (S_2 \setminus H) \text{ and} \\ \Gamma & = & \mathrm{Cay}(G, S). \end{array}$$

Define a permutation ρ of the set G as follows:

$$\rho: \ a^i b^j c^k d^l \mapsto a^{\lambda i} b^{\lambda j} c^{\lambda^2 k} d^{\lambda l'},$$

where $l' = l + \frac{ij[(\lambda^2-1)i+\lambda-1]}{2} + (\lambda^2 - 1)ik$ and $0 \leqslant i,j,k,l \leqslant p-1$.

We remark that the map ρ only fixes the identity of G, but by Lemma 14, ρ is not an automorphism of G. The next lemma shows that ρ maps Γ to its complement $\overline{\Gamma}$.

Lemma 18. *The Cayley graph Γ defined in Construction* 17 *is self-complementary, and ρ is a complementing isomorphism.*

Proof. Take two vertices $x = a^{i_1} b^{j_1} c^{k_1} d^{l_1}$ and $y = a^{i_2} b^{j_2} c^{k_2} d^{l_2}$, where $0 \leqslant i_t, j_t, l_t, k_t \leqslant p-1$ with $t = 1, 2$. By the definition of G, we have

$$yx^{-1} = a^{i_2} b^{j_2 - j_1} c^{k_2 - k_1} a^{-i_1} d^{l_2 - l_1}.$$

By the definition of ρ, we obtain

$$\begin{aligned}(x^\rho)^{-1} &= c^{-\lambda^2 k_1} b^{-\lambda j_1} a^{-\lambda i_1} d^{-\lambda(l_1+\frac{i_1 j_1[(\lambda^2-1)i_1+\lambda-1]}{2}+(\lambda^2-1)i_1 k_1)},\\ y^\rho &= a^{\lambda i_2} b^{\lambda j_2} c^{\lambda^2 k_2} d^{\lambda(l_2+\frac{i_2 j_2[(\lambda^2-1)i_2+\lambda-1]}{2}+(\lambda^2-1)i_2 k_2)}.\end{aligned}$$

Assume first that $i_1 = i_2$. Then, by the previous three equations,

$$\begin{aligned}yx^{-1} &= b^{j_2-j_1} c^{i_2(j_2-j_1)+k_2-k_1} d^{l_2-l_1-\frac{i_2(j_2-j_1)(i_2+1)}{2}-i_2(k_2-k_1)},\\ y^\rho(x^\rho)^{-1} &= b^{\lambda(j_2-j_1)} c^{\lambda^2[i_2(j_2-j_1)+k_2-k_1]} d^{\lambda[l_2-l_1-\frac{i_2(j_2-j_1)(i_2+1)}{2}-i_2(k_2-k_1)]}.\end{aligned}$$

By the above two equations, we obtain that both yx^{-1} and $y^\rho(x^\rho)^{-1}$ belong to H. Recall that $S_1 \subset H$ is an SC-subset with respect to σ. By the definition of ρ, S_1 is also an SC-subset with respect to ρ. It follows that yx^{-1} belongs to S_1 if and only if $y^\rho(x^\rho)^{-1}$ does not belong to S_1.

Assume now that $i_1 \neq i_2$. It is easy to show that neither yx^{-1} nor $y^\rho(x^\rho)^{-1}$ belongs to H. Calculation shows that

$$\begin{aligned}\overline{y}\ \overline{x}^{-1} &= \overline{a}^{i_2-i_1}\overline{b}^{j_2-j_1}\overline{c}^{i_1(j_2-j_1)+k_2-k_1}, \text{ and}\\ \overline{y}^\rho(\overline{x}^\rho)^{-1} &= \overline{a}^{\lambda(i_2-i_1)}\overline{b}^{\lambda(j_2-j_1)}\overline{c}^{\lambda^2[i_1(j_2-j_1)+k_2-k_1]}.\end{aligned}$$

Lemma 16 along with the above two equations imply that

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

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

Notice that, with the same method, a similar construction will also work for the groups $G_4(p)$ and $G_6(p)$.

5 Proof of Theorem 1

Combining Proposition 13 and Lemma 18 along with Construction 17, we obtain an important conclusion in the next proposition.

Proposition 19. *Let G be a p-group of order p^4, where p is an odd prime. Then one of the following holds:*

(i) *if $p \equiv 1 \pmod 4$, then there exist self-complementary Cayley graphs of G when $G = G_2(p)$;*

(ii) *if $p \equiv 1 \pmod 8$, then there exist self-complementary Cayley graphs of G when $G = G_i(p)$ for $i = 1$ or $3 \leqslant i \leqslant 7$.*

We remark that the groups $G_1(p)$, $G_2(p)$, $G_5(p)$ and $G_7(p)$ have fixed-point-free automorphisms by Lemmas 11-12. Therefore, the self-complementary Cayley graphs appearing in Proposition 19 can be produced by fixed-point-free automorphisms of the groups.

The assertion of Theorem 1 follows from Lemma 8 and Proposition 19.

References

[1] B. Alspach, J. Morris, 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] W. Brisley, I. D. Macdonald, Two classes of metabelian p-groups, *Math. Z.* **112** (1969) 5-12.

[4] V. Chvátal, P. Erdős, Z. Hedrlín, Ramsey's theorem and self-complementary graphs, *Disc. Math.* **3** (1972) 301-304.

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

[6] R. Figueroa, R. E. Giudici, Group generation of self-complementary graphs, *Combinatorics and graph theory*, Hefei. (1992) 131-140.

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

[8] D. Gorenstein, Finite Groups, 2nd ed, Chelsea, New York, 1980.

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

[10] R. Guralnick, C. H. Li, C. E. Praeger, J. Saxl, On orbital partitions and exceptionality of primitive permutation groups, *Trans. Amer. Math. Soc.* **356** (2004) 4857-4872.

[11] B. Huppert, Eudiche Gruppen I, Springer-Verlag, 1967.

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

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

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

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

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

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

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

[19] V. Liskovets, R. Pöschel, Non-Cayley-isomorphic self-complementary circulant graphs, *J. Graph Theory.* **34** (2000) 128-141.

[20] R. Mathon, On self-complementary strongly regular graphs, *Disc. Math.* **69** (1988) 263-281.

[21] M. Muzychuck, On Sylow subgraphs of vertex-transitive self-complmentary graphs, *Bull. London Math. Soc.* **31(5)** (1999) 531-533.

[22] S. B. Rao, On Regular and strongly regular selfcomplementary graphs, *Disc. Math.* **54** (1985) 73-82.

[23] D. J. Robinson, A Course in the Theory of Groups, second ed. Springer, New York, 1996.

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

[25] H. Sachs, Über selbstcomplementäre graphen, *Publ. Math. Debrecen.* **9** (1962) 270-288.

[26] B. Zelinka, Self-complementary vertex-transitive undirected graphs, *Math. Slovaca.* **29** (1979) 91-95.