The Cayley Graphs of Prime-square Order which are Cayley Invariant

Zheng Yu Gu

Department of Mathematics
Yunnan Normal University,
Kunming, 650092, People's Republic of China

Cai Heng Li

Department of Mathematics
University of Western Australia
Nedlands, WA 6907, Australia

Abstract

For a finite group G and a self-inverse subset S of G which does not contain the identity of G, let $\mathrm{Cay}(G,S)$ denote the Cayley graph of G with respect to S. If, for all subsets S, T of G of size m, $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ implies $S^\alpha = T$ for some $\alpha \in \mathrm{Aut}(G)$, then G is said to have the m-CI property. In this paper we completely determine the positive integers m for which a cyclic group of prime-square order has the m-CI property.

1 Introduction

Let G be a finite group and set $G^\# = G \setminus \{1\}$. Let S be a self-inverse subset of $G^\#$, that is, $S = S^{-1} := \{s^{-1} \mid s \in S\}$. The *Cayley graph* $\mathrm{Cay}(G,S)$ of G with respect to S is the graph Γ with vertex set $V\Gamma = G$ and edge set $E\Gamma = \{\{a,b\} \mid a, b \in G, a^{-1}b \in S\}$.

For a finite group G, an element α of $\mathrm{Aut}(G)$ induces an isomorphism from $\mathrm{Cay}(G,S)$ to $\mathrm{Cay}(G,S^\alpha)$. However, it is of course possible that there exist a group G and subsets S and T of $G^\#$ such that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ but S is not conjugate under $\mathrm{Aut}(G)$ to T. A Cayley graph $\mathrm{Cay}(G,S)$ is called a *CI-graph* (CI stands for *Cayley Invariant*) of G if, for any subset T of $G^\#$, $S^\alpha = T$ for some $\alpha \in \mathrm{Aut}(G)$ whenever $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$. One long-standing open problem about Cayley graphs is to determine the groups G (or the types of Cayley graphs for a given group G) for which all Cayley graphs of G are CI-graphs. This is the so-called isomorphism problem of Cayley graphs, and has been widely studied (see, for example, [1, 2, 13, 14]).

Australasian Journal of Combinatorics 17(1998), pp.169–174

A group G is said to have the *m-CI property* if all Cayley graphs of G of valency m are CI-graphs. Recently Praeger, Xu and the second author in [12] proposed to characterize finite groups with the m-CI property, and made a general investigation on the structure of Sylow subgroups of groups with the m-CI property for certain values of m. In particular, it was proved in [12, Theorem 1.3] that the 2-CI property implies the 1-CI property. However, it was proved in [10] that the 3-CI property does not necessarily imply the 2-CI property. Further, it was proved that a finite nonabelian simple group G has the 2-CI property if and only if $G = \mathrm{A}_5$ or $\mathrm{PSL}(2,8)$ (see [11, Theorem 1.3]), and G has the 3-CI property if and only if $G = \mathrm{A}_5$ (see [10]). For directed Cayley graphs, the so-called m-DCI property was defined similarly in [12], and some further results have been obtained in [7, 8, 9]. It seems very hard to obtain a "good" characterisation of arbitrary groups with the m-CI property. In this paper we focus on the groups of prime-square order.

From the definition it easily follows that a subset S of $G^{\#}$ is a CI-subset of G if and only if $G^{\#} \setminus S$ is a CI-subset. Thus, for any positive integer $m < |G|$, G has the m-CI property if and only if G has the $(|G^{\#}| - m)$-CI property. So we shall always assume that $m \leq \frac{|G|-1}{2}$. The main result of this paper is the following theorem.

Main Theorem *Let G be a group of order p^2 where p is a prime, and let m be a positive integer with $1 \leq m \leq \frac{p^2-1}{2}$. Then G has the m-CI property if and only if either G is elementary abelian, or one of the following holds:*

(1) $p = 2, 3$,

(2) *m is odd,*

(3) *$[\frac{m}{p}]$ is odd,*

(4) $m \leq p - 1$,

(5) *$m = kp$ or $kp + (p-1)$ for some even positive integer k.*

2 Preliminaries

This section quotes some preliminary results which will be used in the proof of the Main Theorem. First we have a criterion for a Cayley graph to be a CI-graph:

Lemma 2.1 (Alspach and Parsons [1, Theorem 1], or Babai [2, Lemma 3.1]) *Let Γ be a Cayley graph of a finite group G and let A be the automorphism group of Γ. Let G_R denote the subgroup of A consisting of right multiplications $g: x \to xg$ by elements $g \in G$. Then Γ is a CI-graph of G if and only if, for any $\tau \in \mathrm{Sym}(G)$ with $G_R^{\tau} \leq A$, there exists $\alpha \in A$ such that $G_R^{\alpha} = G_R^{\tau}$.*

In the following, we shall use G itself to denote the group G_R of right multiplications induced by element of G. The normalizer of G in $\mathrm{Aut}\,\mathrm{Cay}(G,S)$ is often useful for characterizing $\mathrm{Cay}(G,S)$.

Lemma 2.2 ([5, Lemma 2.1]) *Let G be a finite group and S a subset of $G^{\#}$, let $A = \mathrm{Aut}\,\mathrm{Cay}(G,S)$ and $\mathrm{Aut}(G,S) = \{\alpha \in \mathrm{Aut}(G) \mid S^{\alpha} = S\}$. Then $\mathrm{N}_A(G) = G \rtimes \mathrm{Aut}(G,S)$, a semidirect product of G by $\mathrm{Aut}(G,S)$.*

This property is specially useful for groups of prime-power order due to the following conclusion.

Lemma 2.3 ([15, p. 88]) *Let H be a proper subgroup of a p-group G where p is a prime. Then $\mathrm{N}_G(H) > H$.*

The final simple lemma gives some properties about subsets of a cyclic group.

Lemma 2.4 ([8, Lemma 2.1]) *Let $G = \langle z \rangle$ be a cyclic group of order n, and assume that $i, m \in \{1, 2, \ldots, n-2\}$. Suppose that $\{z, z^2, \ldots, z^m\} = \{z^i, z^{2i}, \ldots, z^{mi}\}$. Then $i = 1$.*

The terminology and notation used in this paper are standard (see, for example, [3, 15]). In particular, for a group and an element $g \in G$, denote by $|G|$ and $o(g)$ the orders of G and g, respectively. For a graph $\Gamma = (V, E)$, its *complement* $\overline{\Gamma} = (V, \overline{E})$ is the graph with vertex set V such that $\{a, b\} \in \overline{E}$ if and only if $\{a, b\} \notin E$. The *lexicographic product* $\Gamma_1[\Gamma_2]$ of two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ is the graph with vertex set $V_1 \times V_2$ such that $\{(a_1, a_2), (b_1, b_2)\}$ is an edge if and only if either $\{a_1, b_1\} \in E_1$ or $a_1 = b_1$ and $\{a_2, b_2\} \in E_2$. For a positive integer n, K_n denotes the complete graph on n vertices.

3 Proof of the Main Theorem

In this section we prove the Main Theorem. For convenience, if $\mathrm{Cay}(G,S)$ is a CI-graph of G then we call the subset S a *CI-subset.* For a group G and a pair of subsets S, T of $G^{\#}$, if $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ but S is not conjugate under $\mathrm{Aut}(G)$ to T, then we call $\{S, T\}$ an *NCI-pair* of G.

Proof of the Main Theorem: It is known that a group of prime-square order is either elementary abelian or cyclic. Assume that G is elementary abelian. Then by the result of Godsil [6], G has the m-CI property for all values of m. Thus in the following we assume that G is a cyclic group of order p^2 where p is a prime.

Suppose that none of conditions (1)–(5) listed in the theorem holds. (We shall construct various NCI-pairs for different cases.) Then $p \geq 5$ and $m = kp + j$ for some positive even integers k and j with $j \neq p - 1$. Thus $2 \leq j \leq p - 3$, and since $m \leq \frac{p^2-1}{2}$, we have that $2 \leq k \leq \frac{p-1}{2}$. We will prove that G does not have the m-CI property. Let $k_0 = \frac{k}{2}$ and $j_0 = \frac{j}{2}$. Then $1 \leq k_0 \leq \frac{p-1}{4}$ and $1 \leq j_0 \leq \frac{p-3}{2}$. Let $G = \langle a \rangle$, and let

$$\begin{cases} S_0 = \{a^p, a^{-p}, \ldots, a^{j_0 p}, a^{-j_0 p}\}, \\ T_0 = \{a^{2p}, a^{-2p}, \ldots, a^{2j_0 p}, a^{-2j_0 p}\}. \end{cases}$$

Since p is odd, there exists an automorphism τ of $\langle a^p \rangle$ such that $(a^p)^{\tau} = a^{2p}$. Now $S_0^{\tau} = T_0$, and so $\Gamma_1 := \mathrm{Cay}(\langle a^p \rangle, S_0) \cong \mathrm{Cay}(\langle a^p \rangle, T_0)$. If $a^p \in T_0$ then $a^{2hp} = a^p$ for some h with $1 \le h \le j_0$ or $-1 \ge h \ge -j_0$. Thus $a^{2hp-p} = 1$ and so $p \mid 2h-1$, which is a contradiction since $|h| \le j_0 \le \frac{p-3}{2}$. So $a^p \notin T_0$. Similarly, $a^{-p} \notin T_0$. Set

$$\begin{cases} S = \{a, a^{-1}, \ldots, a^{k_0}, a^{-k_0}\}\langle a^p\rangle \cup S_0, \\ T = \{a, a^{-1}, \ldots, a^{k_0}, a^{-k_0}\}\langle a^p\rangle \cup T_0. \end{cases}$$

Let $\overline{G} := G/\langle a^p\rangle$, $\overline{S} := S\langle a^p\rangle/\langle a^p\rangle \setminus \{1\}$ and $\overline{T} := T\langle a^p\rangle/\langle a^p\rangle \setminus \{1\}$. Then $\overline{S} = \{\overline{a}, \ldots, \overline{a}^k\} = \overline{T}$. Let $\Gamma_2 = \mathrm{Cay}(\overline{G}, \overline{S})$ $(= \mathrm{Cay}(\overline{G}, \overline{T}))$. Then $\mathrm{Cay}(G,S) \cong \Gamma_2[\Gamma_1] \cong \mathrm{Cay}(G,T)$. Suppose that G has the m-CI property. Then there exists $\alpha \in \mathrm{Aut}(G)$ mapping S to T. Since $a \in S$ we have $a^\alpha \in T$, and since $o(a^\alpha) = o(a) = p^2$, we have $a^\alpha \in \{a, a^{-1}, \ldots, a^{k_0}, a^{-k_0}\}\langle a^p\rangle$. Thus $a^\alpha = a^{i+hp}$ for some integers i, h where $1 \le i \le k_0$ or $-1 \ge i \ge -k_0$. Let $\overline{\alpha}$ be the automorphism of $\overline{G}$ induced by α. Then $\{\overline{a}^i, \overline{a}^{-i}, \ldots, \overline{a}^{k_0 i}, \overline{a}^{-k_0 i}\} = \overline{S}^{\overline{\alpha}} = \overline{T} = \{\overline{a}, \overline{a}^{-1}, \ldots, \overline{a}^{k_0}, \overline{a}^{-k_0}\}$. Let ε be equal to 1 or -1 such that εi is positive. Then $1 \le \varepsilon i \le k_0$. We claim that $\{\overline{a}^{\varepsilon i}, \overline{a}^{2\varepsilon i}, \ldots, \overline{a}^{k_0 \varepsilon i}\} = \{\overline{a}, \overline{a}^2, \ldots, \overline{a}^{k_0}\}$. Suppose to the contrary that $\{\overline{a}^{\varepsilon i}, \overline{a}^{2\varepsilon i} \ldots, \overline{a}^{k_0\varepsilon i}\} \cap \{\overline{a}^{-1}, \ldots, \overline{a}^{-k_0}\} \ne \emptyset$. Then there exists an integer l with $1 < l \le k_0$ such that $1 \le (l-1)\varepsilon i \le k_0$ and $l\varepsilon i > k_0$. Since $\varepsilon i \le k_0$ and $k_0 \le \frac{p-1}{4}$, we have $l\varepsilon i = \varepsilon i + (l-1)\varepsilon i \le 2k_0 \le \frac{p-1}{2}$. It follows that $a^{l\varepsilon i} \in \{\overline{a}^{-1}, \ldots, \overline{a}^{-k_0}\}$. Thus we have that $p - k_0 \le l\varepsilon i < p-1$, and so $\varepsilon i = l\varepsilon i - (l-1)\varepsilon i \ge (p-k_0) - k_0$. Since $\varepsilon i \le k_0 \le \frac{p-1}{4}$, we have $p \le \varepsilon i + 2k_0 \le \frac{3(p-1)}{4}$, which is a contradiction. Therefore, $\{\overline{a}^{\varepsilon i}, \overline{a}^{2\varepsilon i}, \ldots, \overline{a}^{k_0\varepsilon i}\} = \{\overline{a}, \overline{a}^2, \ldots, \overline{a}^{k_0}\}$ and by Lemma 2.4, $\varepsilon i \equiv 1 \pmod{p}$. Since $1 \le \varepsilon i \le k_0 < p$, we have $\varepsilon i = 1$, and so $i = \varepsilon$. Consequently, $(a^p)^\alpha (a^{i+hp})^p = (a^{\varepsilon+hp})^p = a^{\varepsilon p}$. Therefore, since $a^{\varepsilon p} \notin T$, we have that $(a^p)^\alpha \in S^\alpha \setminus T$, which is a contradiction.

Conversely, we need to prove that G has the m-CI property for the cases (1)–(5) listed in the theorem. If $p = 2, 3$, then it follows from [4] that G has the m-CI property for $1 \le m \le 4$. Thus assume that $p \ge 5$. If m is odd, then G does not have self-inverse Cayley subsets of size m, so G vacuously has the m-CI property. Thus we may assume that one of cases (3)–(5) holds. We need to prove that S is a CI-subset. Let $\Gamma = \mathrm{Cay}(G,S)$ and $A = \mathrm{Aut}\,\Gamma$, and let A_1 be the stabilizer of 1 in A. If $p \nmid |A_1|$ then G is a Sylow p-subgroup of A. By Sylow's Theorem and Lemma 2.1, S is a CI-subset. Thus we may further assume that $p \mid |A_1|$.

First assume that $m < p$. If $\langle S\rangle = G$ then $p \nmid |A_1|$, which is a contradiction. Thus $\langle S\rangle < G$ and $\langle S\rangle = \langle a^p\rangle$. By a result of Turner [16], S is a CI-subset of $\langle a^p\rangle$. For any subset T of $G^\#$ such that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$, we have $\langle T\rangle = \langle a^p\rangle$ and $\mathrm{Cay}(\langle a^p\rangle, S) \cong \mathrm{Cay}(\langle a^p\rangle, T)$, and therefore, since S is a CI-subset of $\langle a^p\rangle$, there exists $\alpha \in \mathrm{Aut}(\langle a^p\rangle)$ satisfying $S^\alpha = T$. Further, there exists $\beta \in \mathrm{Aut}(G)$ such that the restriction of β to $\langle a^p\rangle$ is equal to α. Hence $S^\beta = T$ and so S is a CI-subset of G.

Now assume that either $[\frac{m}{p}]$ is odd, or $m = kp$ or $kp + (p-1)$ for some even positive integer k. Let $G = \langle a\rangle$ $(\cong \mathbb{Z}_{p^2})$, and let S be a self-inverse subset of $G^\#$ of size m. Our goal is to show that S is a CI-subset. Let $\Gamma = \mathrm{Cay}(G,S)$ and $A = \mathrm{Aut}\,\Gamma$, and let A_1 be the stabilizer of 1 in A. If $p \nmid |A_1|$ then G is a Sylow p-subgroup of A. By Sylow's Theorem and Lemma 2.1, S is a CI-subset.

Since $p \mid |A_1|$, a Sylow p-subgroup of A has order at least p^3. By Sylow's Theorem, there exists a Sylow p-subgroup P of A which contains G as a subgroup.

By Lemma 2.3, $\mathbf{N}_A(G) \geq \mathbf{N}_P(G) > G$. First we study the structure of S. From Lemma 2.2 it follows that there exists $\alpha \in \mathrm{Aut}(G)$ of order p such that $S^\alpha = S$. It is easy to see that $a^\alpha = a^{1+jp}$ for some $1 \leq j \leq p-1$. Thus for any integer k, $(a^k)^\alpha = a^{k+kjp}$, so $(a^k)^\alpha = a^k$ if and only if $p \big| k$, which is equivalent to $a^k \in \langle a^p \rangle$. Therefore, α fixes every element of S of order p and fixes no elements of S of order p^2. Moreover, if $a^k \in S$ and $(a^k)^\alpha \neq a^k$ then $a^k\langle a^p\rangle = a^k\langle a^{kjp}\rangle = \{a^k, a^{k+kjp}, \ldots, a^{k+(p-1)kjp}\} = \{a^k, (a^k)^\alpha, \ldots, (a^k)^{\alpha^{p-1}}\} = (a^k)^{\langle\alpha\rangle} \subset S$. Since $S = S^{-1}$, we also have $a^{-k}\langle a^p\rangle \subset S$. Since α is of order p, every nontrivial $\langle\alpha\rangle$-orbit (on S) has size p, and since G has exactly $p-1$ elements of order p, it follows that $[\frac{m}{p}]$ is even and there is a subset Q of $G \setminus \langle a^p\rangle$ of size k such that if $m = kp$ then $S = Q\langle a^p\rangle$, and if $m = kp + (p-1)$ then $S = Q\langle a^p\rangle \cup \langle a^p\rangle^\#$.

Let T be a subset of $G^\#$ such that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$. It follows from the arguments in the previous paragraph that if $m = kp$ then $T = Q'\langle a^p\rangle$, and if $m = kp + (p-1)$ then $T = Q'\langle a^p\rangle \cup \langle a^p\rangle^\#$, where Q' is a subset of $G \setminus \langle a^p\rangle$ of size k. We want to prove that S is conjugate under $\mathrm{Aut}(G)$ to T. Let $\overline{G} = G/\langle a^p\rangle$ and $\overline{S} = S\langle a^p\rangle/\langle a^p\rangle \setminus \{1\}$, and let $\overline{\Gamma} = \mathrm{Cay}(\overline{G}, \overline{S})$. It follows from the definition that if $m = kp$ then $\Gamma \cong \overline{\Gamma}[\overline{K}_p]$; if $m = kp + (p-1)$ then $\Gamma \cong \overline{\Gamma}[K_p]$. Thus A preserves the unique nontrivial imprimitive system $\{x\langle a^p\rangle \mid x \in G\}$ of $V\Gamma$ consisting of p blocks of size p. Similarly, setting $\Gamma' = \mathrm{Cay}(G,T)$, also $\mathrm{Aut}\,\Gamma'$ has the unique imprimitive system $\{x\langle a^p\rangle \mid x \in G\}$. Therefore, if ρ is an isomorphism from $\mathrm{Cay}(G,S)$ to $\mathrm{Cay}(G,T)$, then $\{x\langle a^p\rangle \mid x \in G\}^\rho = \{x\langle a^p\rangle \mid x \in G\}$. Hence ρ induces an isomorphism from $\mathrm{Cay}(\overline{G},\overline{S})$ to $\mathrm{Cay}(\overline{G},\overline{T})$ where $\overline{T} = T\langle a^p\rangle/\langle a^p\rangle \setminus \{1\}$. Since $V\overline{\Gamma}$ is of size p, $\overline{G}$ is a Sylow p-subgroup of $\mathrm{Aut}\,\overline{\Gamma}$. All subgroups of $\mathrm{Aut}\,\overline{\Gamma}$ which act regularly on $V\overline{\Gamma}$ are cyclic groups of order p and hence are conjugate by Sylow's Theorem. So by Lemma 2.1, $\overline{S}$ is a CI-subset of $\overline{G}$. Hence there exists $\tau \in \mathrm{Aut}(\overline{G})$ such that $\overline{S}^\tau = \overline{T}$, so $\overline{a}^\tau = \overline{a}^r$ for some integer $r \in \{1, 2, \ldots, p-1\}$. Write $\overline{S} = \{\overline{a}^{i_1}, \overline{a}^{i_2}, \ldots, \overline{a}^{i_k}\}$, and then $\overline{T} = \overline{S}^\tau = \{\overline{a}^{i_1 r}, \overline{a}^{i_2 r}, \ldots, \overline{a}^{i_k r}\}$. Therefore, $S = a^{i_1}\langle a^p\rangle \cup a^{i_2}\langle a^p\rangle \cup \ldots \cup a^{i_k}\langle a^p\rangle$ and $T = a^{i_1 r}\langle a^p\rangle \cup a^{i_2 r}\langle a^p\rangle \cup \ldots \cup a^{i_k r}\langle a^p\rangle$. Since r is coprime to p, $a \to a^r$ induces an automorphism σ of G. Now $S^\sigma = T$, so S is a CI-subset of G. Therefore, G has the m-CI property. □

References

[1] B. Alspach and T. D. Parsons, Isomorphism of circulant graphs and digraphs, *Disc. Math.* **25**(1979), 97-108.

[2] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29**(1977), 329-336.

[3] N. Biggs, *Algebraic Graph Theory*, (Cambridge Uni. Press, New York, 1974).

[4] C. Delorme, O. Favaron and M. Mahéo, Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups, *European J. Combin.* **13**(1992), 59-61.

[5] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1**(1981), 243-256.

[6] C. D. Godsil, On Cayley graphs isomorphisms, *Ars Combin.* **15**(1983), 231-246.

[7] C. H. Li, The finite groups with the 2-DCI property, *Comm. Algebra* **24(5)** (1996), 1749-1757.

[8] C. H. Li, Finite abelian groups with the m-DCI property, *Ars Combin.* (to appear).

[9] C. H. Li, The cyclic groups with the m-DCI property, *European J. Combin.* (to appear).

[10] C. H. Li, Finite groups with Cayley invariant property, *Bull. Austral. Math. Soc.* (to appear).

[11] C. H. Li and C. E. Praeger, The finite simple groups with at most two fusion classes of every order, *Comm. Algebra* **24(11)**(1996), 3681-3704.

[12] C. H. Li, C. E. Praeger and M. Y. Xu, On finite groups with the Cayley isomorphism property, submitted.

[13] M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Combin. Theory, Ser.A* **72**(1995), 118-134.

[14] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, *European J. Combin.* **8**(1987), 35-43.

[15] M. Suzuki, *Group Theory I*, (Springer-Verlag, New York, 1986).

[16] J. Turner, Point-symmetric graphs with a prime number of points, *J. Combin. Theory* **3** (1967), 136-145.

(Received 18/2/97)