www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 3 No. 1 (2014), pp. 1-6.

www.ui.ac.ir

ON THE SYMMETRIES OF SOME CLASSES OF RECURSIVE CIRCULANT GRAPHS

S. MORTEZA MIRAFZAL

Communicated by Jamshid Moori

Abstract. A recursive-circulant $G(n;d)$ is defined to be a circulant graph with n vertices and jumps of powers of d. $G(n;d)$ is vertex-transitive, and has some strong hamiltonian properties. $G(n;d)$ has a recursive structure when $n = cd^m$, $1 \leq c < d$ [*Theoret. Comput. Sci.* **244** (2000) 35-62]. In this paper, we will find the automorphism group of some classes of recursive-circulant graphs. In particular, we will find that the automorphism group of $G(2^m;4)$ is isomorphic with the group $D_{2\cdot 2^m}$, the dihedral group of order 2^{m+1}.

1. Introduction

An interconnection network can be represented as an undirected graph where a processor is represented as a vertex and a communication channel between processors as an edge between corresponding vertices. Measures of the desirable properties for interconnection networks include degree, connectivity, diameter, fault tolerance, and symmetry [1]. The main aim of this paper is to study the symmetries of a class of graphs that are useful in some aspects for designing some interconnection networks. In this paper, a graph $G = (V, E)$ is considered as an undirected graph where $V = V(G)$ is the vertex-set and $E = E(G)$ is the edge-set. For all the terminology and notation not defined here, we follow [3, 6, 11]. The hypercube Q_n of dimension n is the graph with vertex-set $\{(x_1, x_2, \ldots, x_n)|x_i \in \{0, 1\}\}$, two vertices $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are adjacent if and only if $x_i = y_i$ for all but one i. The graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are called isomorphic if there is a bijection $\alpha : V_1 \longrightarrow V_2$ such that $\{a, b\} \in E_1$ if and only if $\{\alpha(a), \alpha(b)\} \in E_2$ for all $a, b \in V_1$. In such a case the bijection α is called an

MSC(2010): Primary: 05C25; Secondary: 94C15.

Keywords: Cayley graph, recursive-circulant, automorphism group, dihedral group.

Received: 25 May 2013, Accepted: 28 November 2013.

isomorphism. An automorphism of a graph Γ is an isomorphism of Γ with itself. The set of automorphisms of Γ, with the operation of composition of functions, is a group, called the automorphism group of Γ and denoted by $Aut(\Gamma)$. In most situations, it is difficult to determine the automorphism group of a graph and this has been the subject of many research papers. Some of the recent works appear in the references [4, 5, 7, 8, 9, 12]. A permutation of a set is a bijection of it with itself. The group of all permutations of a set V is denoted by $Sym(V)$, or just $Sym(n)$ when $\mid V \mid = n$. A permutation group G on V is a subgroup of $Sym(V)$. In this case we say that G acts on V. If Γ is a graph with vertex-set V, then we can view each automorphism as a permutation of V, so $Aut(\Gamma)$ is a permutation group. Let G act on V. We say that G is transitive (or G act transitively on V) if there is just one orbit. This means that given any two elements u and v of V, there is an element β of G such that $\beta(u) = v$.

The graph Γ is called vertex transitive if $Aut(\Gamma)$ acts transitively on $V(\Gamma)$. For $v \in V(\Gamma)$ and $G = Aut(\Gamma)$, the stabilizer subgroup G_v is the subgroup of G containing all automorphisms which fix v. In the vertex transitive case all stabilizer subgroups G_v are conjugate in G, and consequently isomorphic. In this case the index of G_v in G is given by the equation, $|G : G_v| = \frac{|G|}{|G_v|} = |V(\Gamma)|$. Let G be any abstract finite group with identity 1, and suppose that Ω is a set of generators of G, with the properties :

(i) $x \in \Omega \Longrightarrow x^{-1} \in \Omega; (ii) 1 \notin \Omega$. The Cayley graph $\Gamma = Cay(G, \Omega)$ is the graph whose vertex-set and edge-set are defined as follows: $V(\Gamma) = G; E(\Gamma) = \{\{g, h\} \mid g^{-1}h \in \Omega\}$.

The connectivity of a graph Γ is the minimum number of vertices whose removal leaves the remaining graph disconnected or trivial.

The dihedral group D_{2n} is a group of order $2n, n > 2$, generated by two elements α, β such that $o(\alpha) = n$, $o(\beta) = 2$ and $\alpha\beta = \beta\alpha^{-1}$.

A recursive circulant $G(n; d)$ is a Cayley graph over an abelian group, in more precise words, the Cayley graph on the cyclic group $\mathbb{Z}_n$, where $n = cd^m$, $1 \leq c < d$, with the generating set $S = \{1, n-1, d, n-d, \ldots, d^m, n-d^m\}$, if $c \neq 1$ and $S = \{1, n-1, d, n-d, \ldots, d^{m-1}, n-d^{m-1}\}$, if $c = 1$. Several interesting properties of these graphs have been studied in the literature [2, 10]. For example, it has been proved in [10] that the connectivity of $G(2^m; 4)$ is m, which is the best possible. Hypercubes are one of the most popular interconnection networks being used. Note that the number of vertices of $G(2^m; 4)$ is 2^m, which is equal to that of Q_m, but the diameter of $G(2^m; 4)$ is $\lceil \frac{3m-1}{4} \rceil$, which is less than that of the Hypercube Q_m [2].

The following figure shows the graphs $G(12; 4)$ and $G(16; 4)$.

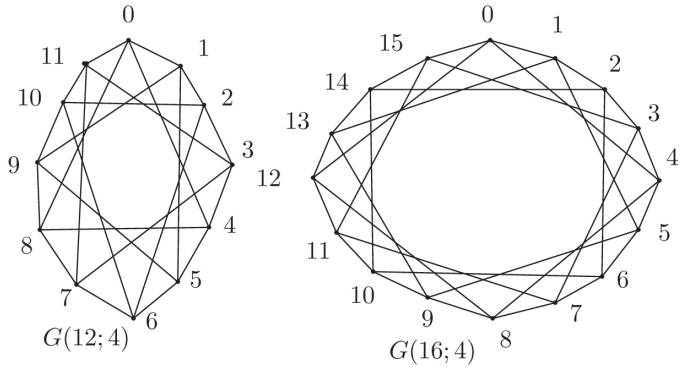

Fig 1. The graphs $G(12;4)$ and $G(16;4)$

2. **Main results**

Lemma 2.1. *Let $n = cd^m$, where c, d, m are positive integers, $d \geq 4$, $2 \leq c < d$. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ be the cyclic group of order n and $S = \{1, n-1, d, n-d, \ldots, d^m, n-d^m\} \subset \mathbb{Z}_n$. Let $x, y, s_1, s_2 \in S$, $x + y \not\equiv 0 \pmod{n}$ and $x \neq y$. If $x + y \equiv s_1 + s_2 \pmod{n}$, then $\{x, y\} = \{s_1, s_2\}$.*

Proof. We know that if $\alpha \equiv \beta \pmod{l}$, then $-\alpha \equiv -\beta \pmod{l}$, thus it is sufficient to prove the lemma for the following two cases;

(1) $x = d^i,\ y = d^j$ and (2) $x = d^i,\ y = n - d^j$, where we have $0 \leq i, j \leq m$ and $i \neq j$ in both cases.

In the first step we show that if $d^i + d^j = d^k + d^l + t(cd^m)$, where t is an integer, then $\min\{i, j\} = \min\{k, l\}$, where $\min\{u, v\}$ is the minimum of the integers u, v. Let $e = \min\{i, j\}$ and $h = \min\{k, l\}$. If $e < h$, then $e \neq m$, and thus, $d^{i-e} + d^{j-e} = d^{k-e} + d^{l-e} + t(cd^{m-e})$. It follows that $d|1$ which is a contradiction since $d \geq 4$. By a similar argument, it follows that $h < e$ is again impossible, and thus we must have $e = h$. Let $i = e = h = k$, so that $d^i = d^k$, which implies that $d^j = d^l + t(cd^m)$. Now $j \neq l$ is again impossible and thus, $\{i, j\} = \{k, l\}$. Therefore, the assertion of Lemma 2.1. in the case that $d^i + d^j \equiv d^k + d^l \pmod{n}$ is proved.

Now let $d^i + d^j = d^k - d^l + t(cd^m)$, where $k \neq l$ and $i \neq j$. If we let $\min\{i, j\} = i$, then by a similar argument it follows that $i = k$ or $i = l$. In the first step let $i = k$, so that $d^j = -d^l + t(cd^m)$. Now since $j < l$ and $l < j$ are impossible so we must have $j = l$ so that we have $2d^j = t(cd^m)$. For $c \neq 2$, this is impossible and for $c = 2$ it follows that $j = m$, so we have $n - d^m = d^m = d^j = d^l$. Thus, if $d^i + d^j \equiv d^k + n - d^l \pmod{n = 2d^m}$, then $\{d^i, d^j\} = \{d^k, n - d^l\}$.

If we now let $i = l$, then $2d^i = d^k - d^j + t(cd^m)$. Let $c \neq 2$. It then follows that $k \neq j$, so $i = \min\{k, j\}$ and thus, $i = k$. Therefore, $d^i = -d^j + t(cd^m)$ so that, $i = j$, which is a contradiction.

If we now let $i = l$ and $c = 2$, then we have $2d^i = d^k - d^j + t(2d^m)$. If $k = j$, then $i = m$, so $m = i = l$ and thus, $n - d^l = d^l = d^i$ and $d^k = d^j$. If $k \neq j$, then $i = \min\{k, j\}$, so that $i = k$ and thus, $d^i = -d^j + t(2d^m)$. This implies that $d^i + d^j \equiv 0 \pmod{n = cd^m}$, which is a contradiction. Now it has been proved that, if $c \neq 2$, then $d^i + d^j \equiv d^k + n - d^l \pmod{n = cd^m}$ is impossible and if $c = 2$, then $d^i + d^j \equiv d^k + n - d^l \pmod{n = 2d^m}$ implies that $\{d^i, d^j\} = \{d^k, n - d^l\}$.

By a similar argument, we can show that if $d^i + d^j \equiv n - d^k + n - d^l \pmod{n = cd^m}$, then for $i = \min\{i, j\}$ and $k = \min\{k, l\}$ we must have $i = k$ and thus, $2d^i + d^j \equiv -d^l \pmod{n = cd^m}$. Since $i \neq m$ (if $i = m$, then $j = m = i$, which is a contradiction), then we must have $i = l$, so $3d^i \equiv -d^j \pmod{n = cd^m}$. Now since $d \neq 3$, we must have $i = j$, which is a contradiction. It follows that since $i \neq j$, then $d^i + d^j \equiv n - d^k + n - d^l \pmod{n = cd^m}$ is impossible.

(2) By a similar argument, it follows that if $d^i + n - d^j \equiv s_1 + s_2 \pmod{n = cd^m}$, where $i \neq j$ and $s_1, s_2 \in S$, then $\{d^i, n - d^j\} = \{s_1, s_2\}$. □

The following lemma shows that a similar result holds for the case $c = 1$.

Lemma 2.2. *Let $n = d^m$, where d, m are positive integers, $d \geq 4$. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ be the cyclic group of order n and $S = \{1, n-1, d, n-d, \ldots, d^{m-1}, n-d^{m-1}\} \subset \mathbb{Z}_n$. Let $x, y, s_1, s_2 \in S$, $x + y \not\equiv 0 \pmod{n}$ and $x \neq y$. If $x + y \equiv s_1 + s_2 \pmod{n}$, then $\{x, y\} = \{s_1, s_2\}$.*

The above results are not true for $d = 2$ or $d = 3$. For example, letting $n = 2^m$ and $m > 2$, then in $\mathbb{Z}_n$ we have, $2^{m-1} + n - 2^{m-2} \equiv 2^{m-3} + 2^{m-3} \pmod{n}$, but $\{2^{m-1}, n - 2^{m-2}\} \neq \{2^{m-3}, 2^{m-3}\}$. Also, for $n = 2 \cdot 3^m$, in $\mathbb{Z}_n$ we have $3^m + n - 3^{m-1} \equiv 3^{m-1} + 3^{m-1} \pmod{n}$, but $\{3^m, n - 3^{m-1}\} \neq \{3^{m-1}, 3^{m-1}\}$.

Theorem 2.3. *Let $n = cd^m$, where c, d, m are positive integers, $d \geq 4$, $1 \leq c < d$. Let $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ be the cyclic group of order n and $S = \{1, n-1, d, n-d, \ldots, d^m, n-d^m\} \subset \mathbb{Z}_n$, for $c \neq 1$, and $S = \{1, n-1, d, n-d, \ldots, d^{m-1}, n-d^{m-1}\} \subset \mathbb{Z}_n$, for $c = 1$. If $\Gamma = Cay(\mathbb{Z}_n, S)$, then $Aut(\Gamma) \cong D_{2n}$, where D_{2n} is the dihedral group of order $2n$.*

Proof. We prove the theorem for the case $c \neq 1$ because the proof is similar for $c = 1$. Let $G = Aut(\Gamma)$. We show that G_0, the stabilizer of the vertex 0 (the identity element of the group $\mathbb{Z}_n$), is the cyclic group of order 2. Let $f \in G_0$. In the first step we show that f is an automorphism of the group $\mathbb{Z}_n$. Let $v, w \in S$, $v \neq w$ and $v + w \neq 0$. Since $v + w - v = w \in S$, then $\{v + w, v\} \in E(\Gamma)$ so that $\{v + w, w\} \in E(\Gamma)$. Thus $\{f(v + w), f(v)\} \in E(\Gamma)$ and $\{f(v + w), f(w)\} \in E(\Gamma)$ so that $f(v+w) = f(v)+s_1$ and $f(v+w) = f(w)+s_2$, where $s_1, s_2 \in S$. Note that if $u \in S$, then $\{0, u\} \in E(\Gamma)$, so that $\{f(0), f(u)\} = \{0, f(u)\} \in E(\Gamma)$. Now since $N(0) = S$ ($N(x)$ is the set of vertices that are adjacent to vertex x), then $f(u) \in S$ so that $f(S) = S$. We now have $f(v) + s_1 = f(w) + s_2$ and thus, $f(v) - f(w) = s_2 - s_1$. On the other hand, f is a permutation of $\mathbb{Z}_n$ and $v \neq w$ so that, $f(v) \neq f(w)$. Thus, by Lemma 2.1. we must have $\{f(v), -f(w)\} = \{s_2, -s_1\}$. If $f(v) = -s_1$, then we have $f(v + w) = f(v) + s_1 = 0 = f(0)$, and thus $v + w = 0$, which is a contradiction. So $f(v) = s_2$ and we have $f(v + w) = f(w) + s_2 = f(v) + f(w)$.

We now show that if $u \in S$, then $f(2u) = 2f(u)$. Let $2u \neq 0$. Then $f(2u) \neq 0$. Since $2u - u = u \in S$, then $\{2u, u\} \in E(\Gamma)$ so that $\{f(2u), f(u)\} \in E(\Gamma)$. Thus $f(2u) = f(u) + y$, where $y \in S = f(S)$ and therefore there is an $x \in S$ such that $y = f(x)$ and we have $f(2u) = f(u) + f(x)$. We assert that $f(x) = f(u)$. If $f(x) \neq f(u)$, then since $f^{-1} \in G_0$, and by what is proved hitherto $2u = f^{-1}(f(2u)) = f^{-1}(f(u) + f(x)) = f^{-1}(f(u)) + f^{-1}(f(x)) = u + x$. Thus, $x = u$ from which we conclude that $f(x) = f(u)$ which is a contradiction. Therefore, if $u \in S$ and $2u \neq 0$, then $f(2u) = 2f(u)$.

Now let $2u = 0$, (for $n = 2d^m$ and $u = d^m$). If $f(u) = u$, then $2f(u) = 2u = 0 = f(0) = f(2u)$. If $f(u) = y \neq u$, then $2f(u) = 2y \neq 0$ so that $f^{-1}(2y) = 2f^{-1}(y) = 2u$ and thus, $f(2u) = f(f^{-1}(2y)) = 2y = 2f(u)$. Note that if $n = 2d^m$, then $u = d^m$ is the unique element of S such that $2u = 0$.

We now show that if $x \in S$, then $f(-x) = -f(x)$. Let $2x \neq 0$. Then $x \neq -x$, so $f(x) \neq f(-x)$ and thus, if $t = f(x) + f(-x) \neq 0$, then by what is proved hitherto, we have $f^{-1}(t) = f^{-1}(f(x) + f(-x)) = f^{-1}(f(x)) + f^{-1}(f(-x)) = x - x = 0 = f^{-1}(0)$. Thus $t = 0$ which is a contradiction and therefore we must have $f(x) + f(-x) = 0$ so that $f(-x) = -f(x)$. If $2x = 0$, then $x = -x$ and we have $f(2x) = f(0) = 2f(x) = 0$. thus $f(x) = -f(x) = -f(-x)$ which implies that $f(-x) = -f(x)$. Therefore if $v, w \in S$ and $v + w = 0$, then $w = -v$ so that we have $f(v+w) = f(0) = 0 = f(v) - f(v) = f(v) + f(-v) = f(v) + f(w)$.

We have proven that if $v, w \in S$, then $f(v + w) = f(v) + f(w)$. We now wish to extend this, by induction on k, to the assertion $f(k1 + v) = kf(1) + f(v)$, where 1 and v are in S and k is a positive integer.

Note that the assertion is true for $k = 1$. Assume the assertion is true for $l < k$. Let $y = k1 + v$. If $1 + v = 0$, then $0 = f(0) = f(1 + v) = f(1) + f(v)$ and $y = (k - 1)1$. Thus by the induction assumption we have $f(y) = f(k1 + v) = f((k - 1)1) = (k - 1)f(1) = (k - 1)f(1) + f(1) + f(v) = kf(1) + f(v)$.

Now let $1 + v \neq 0$ and $v \neq 1$. Note that $\{k1 + v, k1\}, \{k1 + v, (k - 1)1 + v\} \in E(\Gamma)$ and thus, $\{f(k1 + v), f(k1)\}, \{f(k1 + v), f((k - 1)1 + v)\} \in E(\Gamma)$. Therefore $f(k1 + v) = f(k1) + f(u)$ and $f(k1 + v) = f((k - 1)1 + v) + f(w)$, where $u, w \in S$. Then $f(k1) + f(u) = f((k - 1)1 + v) + f(w)$. By the induction hypothesis, we have $f(k1) = f((k - 1)1 + 1) = (k - 1)f(1) + f(1) = kf(1)$ and thus, $f(1) + f(u) = f(v) + f(w)$ so, $1 + u = v + w$. We then have $1 - v = w - u$ and thus, by Lemma 2.1 we have $\{1, -v\} = \{w, -u\}$. If $1 = -u$, then $f(u) = -f(1)$ so that we have $f(k1 + v) = f(k1) + f(u) = kf(1) - f(1) = f(k - 1)$ and therefore, $k1 + v = (k - 1)1$. This implies $1 + v = 0$ which is a contradiction. Therefore, we must have $1 = w$ implying that $v = u$. Now we have $f(k1 + v) = f(k1) + f(u) = f(k1) + f(v) = kf(1) + f(v)$.

Now let $v = 1$. Since $\{(k + 1)1, k1\} \in E(\Gamma)$, then $\{f((k + 1)1), f(k1)\} \in E(\Gamma)$ and thus $f((k + 1)1) = f(k1) + f(u)$, where $u \in S$. If $u \neq 1$, then $f(k1) + f(u) = f(k1 + u)$ and thus we have $f((k + 1)1) = f(k1 + u)$. This implies $(k + 1)1 = k1 + u$ so that $u = 1$ which is a contradiction. Therefore, $u = 1$ and we have $f((k + 1)1) = f(k1) + f(u) = (k + 1)f(1)$. We now have proved that $f(k1 + v) = kf(1) + f(v)$ for any positive integer k and any $v \in S$.

In particular, we have $f(m1) = mf(1)$ for any positive integer m and $1 \in S$. The set $\{1\}$ is a generating set for the cyclic group $\mathbb{Z}_n$ and therefore, if $a, b \in \mathbb{Z}_n$ and $a = l.1$, $b = k1$, then $f(a + b) = f(l.1 + k1) = f((l + k)1) = (l + k)f(1) = lf(1) + kf(1) = f(l.1) + f(k1) = f(a) + f(b)$. We now have proved that the graph automorphism f which fixes the vertex $v = 0$ is, in fact an automorphism of the group $\mathbb{Z}_n$.

We know that $f(S) = S$ so that $f(1) \in S$. On the other hand, the element 1 is a generating element of the cyclic group $\mathbb{Z}_n$ and thus $f(1)$ is a generating element of the cyclic group $\mathbb{Z}_n$. However, the elements of S that can generate the group $\mathbb{Z}_n$ are $1, -1 = n - 1$. It follows that $|G_0| = 2$.

The graph $\Gamma = Cay(\mathbb{Z}_n, S)$ is vertex-transitive because it is a Cayley graph. Thus, $|G| = 2n$ by the orbit-stabilizer theorem. The group $G = Aut(\Gamma)$ contains a subgroup isomorphic to the group $\mathbb{Z}_n$, say $T = \{f_x | f_x : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, f_x(v) = x + v \quad x, v \in \mathbb{Z}_n\}$. It is an easy task to show that $G = \langle f_1, g\rangle$ where $1 \neq g \in G_0$. It is trivial that $\langle f_1, g\rangle \cong D_{2n}$. □

We now pose the following question:

Question. Is Theorem 2.3 also true for the cases $d = 2$ and $d = 3$?

Conclusion remarks

In this paper, we have found the automorphism groups of almost all classes of recursive circulant graphs but, the problem is still open for two classes of these graphs.

Acknowledgments

The author is thankful to the anonymous referees for valuable comments and suggestions.

References

[1] S. B. Akers and B. Krishnamurthy, A group-theoretic model for symmetric interconnection networks, *IEEE Trans. Comput.*, **38** no. 4 (1989) 555-566.

[2] C. H. Tsai, Jimmy J. M. Tan and L. H. Hsu, The super-connected property of recursive circulant graphs, *Inform. Process. Lett.*, **91** (2004) 293-298.

[3] N. L. Biggs, *Algebraic Graph Theory*, (Second edition), Cambridge University Press, Cambridge, 1993.

[4] Y. Q. Feng, Automorphism groups of Cayley graphs on symmetric groups with generating transposition, *J. Combin. Theory Ser. B*, **96** (2006) 67-72.

[5] A. Ganesan, Automorphisms of Cayley graphs generated by transposition sets, Preprint is at http://arxiv.org/abs/1303.5974v2

[6] C. Godsil and G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, **207**, Springer-Verlag, New York, 2001.

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

[8] S. M. Mirafzal, On the automorphism groups of regular hyper-stars and folded hyper-stars, Ars Combinatoria (in press).

[9] S. M. Mirafzal, Some other algebraic properties of folded hypercubes, Ars Combinatoria (in press).

[10] J. H. Park and K. Y. Chwa, Fundamental study recursive circulants and their embedding among hypercubes, *Theoret. Comput. Sci.*, **244** (2000) 35-62.

[11] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., **148**, Springer-Verlag, New York, 1995.

[12] J. X. Zhou, The automorphism group of the alternating group graph, *Appl. Math. Lett.*, **24** no. 2 (2011) 229-231.

S. Morteza Mirafzal

Department of Mathematics, Lorestan University, Khoramabad, Iran

Email: morteza_mirafzal@yahoo.com smortezamirafzal@yahoo.com mirafzal.m@lu.ac.ir