J. Austral. Math. Soc. (*Series A*) 39 (1985), 270–281

COUNTING 2-CIRCULANT GRAPHS

GEK-LING CHIA and CHONG-KEANG LIM

(Received 15 October 1983)

Communicated by W. D. Wallis

Abstract

Alspach and Sutcliffe call a graph $X(S, q, F)$ 2-circulant if it consists of two isomorphic copies of circulant graphs $X(p, S)$ and $X(p, qS)$ on p vertices with "cross-edges" joining one another in a prescribed manner. In this paper, we enumerate the nonisomorphic classes of 2-circulant graphs $X(S, q, F)$ such that $|S| = m$ and $|F| = k$. We also determine a necessary and sufficient condition for a 2-circulant graph to be a GRR. The nonisomorphic classes of GRR on $2p$ vertices are also enumerated.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 05 C 25, 05 C 30, 05 C 99.

1. Introduction

We consider only finite undirected graphs with no loops or multiple edges. Definitions not given here may be found in [10]. Let Z_n be the ring of integers and Z_n^* the multiplicative group of units in Z_n. Let S be a subset of Z_n^* with $S = -S$. The *circulant graph* $X = X(n, S)$ with *symbol* S is the graph with vertex set u_0, $u_1, \ldots, u_{n-1}$ and an edge joining u_i and u_j if and only if $j - i \in S$. Let p denote a prime number. Turner [12] shows that two circulant graphs $X(p, S)$ and $X(p, S')$ are isomorphic if and only if $S' = qS$ for some q in Z_p^*. He also gave an enumerative polynomial for this class of circulant graphs. The automorphism group $A(X)$ of a circulant graph $X = X(p, S)$ was determined explicitly by Alspach [1]. If $\varnothing \subset S \subset Z_p^*$, then $A(X)$ has order $|E(S)|p$ where $E(S)$ is the largest subgroup of Z_p^* for which S can be written as a union of cosets of $E(S)$. If $\beta^*(p, m, d)$ denotes the number of nonisomorphic circulant graphs $X = X(p, S)$

with degree $|S| = m$ and automorphism group of order dp, then

$$\beta^*(p, m, d) = \frac{d}{m} \sum_{d|d_i} \mu\left(\frac{d_i}{d}\right) \binom{\frac{p-1}{d_i} - 1}{\frac{m}{d_i} - 1}$$

where $\mu(n)$ is the classical Möbius function (see [5] Chapter 5).

In [2] Alspach and Sutcliffe call a graph $X = X(S, q, F)$ *2-circulant* if (i) $V(X) = V(X_1) \cup V(X_2)$ where $X_1 = X(p, S)$ and $X_2 = X(p, qS)$ are two isomorphic circulant graphs with $V(X_j) = \{u_{j,0}, u_{j,1}, \ldots, u_{j,p-1}\}, j = 1, 2$, (ii) $E(X) = E(X_1) \cup E(X_2) \cup \{(u_{1,i}, u_{2,j}) | j - i \in F\}$, (iii) q is chosen such that $q^2 \in E(S)$ and (iv) (a) if $qS = S$ then F is any subset of Z_p, (b) if $qS \neq S$ then $j \in F$ implies that $-qj \in F$. A 2-circulant $X(S, q, F)$ is said to be of *Type-I* if it has a representation $X(S', q', F') \cong X(S, q, F)$ with $q' = 1$; otherwise it is said to be of *Type-II*. In this paper we enumerate separately, the nonisomorphic classes of Type-I and Type-II 2-circulants such that $|S| = m$ and $|F| = k$. Our method is similar to the one used in [4].

It is not difficult to see that a GRR on $2p$ vertices is a Type-I 2-circulant. In the final section, we determine a necessary and sufficient condition for a Type-I 2-circulant graph to be a GRR (Theorem 4.3). We then proceed to enumerate the nonisomorphic classes of GRR on $2p$ vertices.

2. Type-I 2-circulants

In this section we shall count the number of Type-I 2-circulant graphs. Theorem 8 of [2] asserts that $X(S, q, F)$ with $|F| \neq 0$ is of Type-I if and only if $qS = S$. Now this is possible if and only if $q \in E(S)$. So we may assume without loss of generality that $q = 1$ whenever $X(S, q, F)$ is Type-I.

Let $2I(p, m, k)$ denote the number of nonisomorphic Type-I 2-circulant graphs $X(S, 1, F)$ with $|S| = m$ (even) and $|F| = k$. We note that $2I(p, m, k) = 2I(p, m, p - k) = 2I(p, p - m - 1, p - k)$ for any $k \geqslant 0$ and $m > 0$. We note further that if $k = 0$ or $k = 1$, then $2I(p, m, k)$ is the number of circulant graphs $X(p, S)$ with $|S| = m$. In view of these we may assume that $2 \leqslant |F| \leqslant (p - 1)/2$ and $0 < m \leqslant (p - 1)/2$.

THEOREM 2.1 [2, Theorem 10]. *Two Type-*I *2-circulant graphs $X(S, 1, F)$ and $X(S, 1, F')$ with $\varnothing \subset F, F' \subset Z_p$ are isomorphic if and only if there exists $\alpha \in E(S)$ such that $F' = \alpha F + c$ for some $c \in Z_p$.*

Let $X = X(S, 1, F)$ and $\mathscr{F}(k)$ be the collection of all subsets of Z_p each of cardinality $k > 0$. Suppose $k < p$ and let $F \in \mathscr{F}(k)$. By Theorem 2.1, $X(S, 1, F + c) \cong X(S, 1, F + d)$ for any $c, d \in Z_p$. Now since $F + c \neq F + d$ if $c \neq d$, each $F \in \mathscr{F}(k)$ induces a family containing p elements and so there are $n = (1/p)\binom{p}{k}$ families in $\mathscr{F}(k)$. Let these families be $\mathscr{F}_1, \ldots, \mathscr{F}_n$. Two families $\mathscr{F}_i$ and $\mathscr{F}_j$ are said to be *equivalent* under $E(S)$, written $\mathscr{F}_i \sim \mathscr{F}_j$ if there exist $\alpha \in E(S)$, $F \in \mathscr{F}_i$ and $F' \in \mathscr{F}_j$ such that $\alpha F = F' + c$ for some $c \in Z_p$. Evidently $\sim$ is an equivalence relation and that if $\mathscr{F}_i \sim \mathscr{F}_j$, then $X(S, 1, F) \cong X(S, 1, F')$ for any $F \in \mathscr{F}_i$ and $F' \in \mathscr{F}_j$. By Theorem 2.1 the action of $E(S)$ will partition $\mathscr{F}_1, \ldots, \mathscr{F}_n$ into equivalence classes. We shall determine the number of these equivalence classes.

Let E_i be the subgroup of Z_p^* with $|E_i| = d_i$. Then $\mathscr{F}$ is said to be *invariant* under E_i, if for every $F \in \mathscr{F}$, we have $\alpha F = F + c$ for any $\alpha \in E_i$ and some $c \in Z_p$.

LEMMA 2.2. *$\mathscr{F}$ is invariant under $E_i \neq 1$ if and only if there exists $F \in \mathscr{F}$ such that $F = \bigcup_\alpha \alpha E_i$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_i$.*

PROOF. The sufficiency is clear. If $\mathscr{F}$ is invariant under E_i, then for every $F \in \mathscr{F}$, we have $aF = F + c$ for some $c \in Z_p$ and any $a \in E_i$. In particular we choose F such that $c = 0$. Since $aF = F$ if and only if $a \in E_i$, it follows that either $F = \bigcup_\alpha \alpha E_i$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_i$.

LEMMA 2.3. *Let $A_1 = \bigcup_\alpha \alpha E_i$, $A_2 = \bigcup_\beta \beta E_i$ where $E_i \neq 1$. If $A_1 \neq A_2$, then $A_1 \neq A_2 + c$ for any $c \in Z_p$.*

PROOF. We need only note that for $E_i \neq 1$ and $j = 1, 2$, $\sum_{r \in A_j} r \equiv 0 \pmod p$ and that $c|A_2| \not\equiv 0 \pmod p$ unless $c = 0$ or $|A_2| = p$. But these are ruled out by the fact that $A_1 \neq A_2$.

Combining Lemmas 2.2 and 2.3, we have

LEMMA 2.4. *The number of families which are invariant under some non-trivial subgroup E_i of $E(S)$ is given by*

$$\Psi(E_i; F) = \begin{cases} \dbinom{(p-1)/d_i}{|F|/d_i} & \text{if } d_i \text{ divides } |F|, \\ \dbinom{(p-1)/d_i}{(|F|-1)/d_i} & \text{if } d_i \text{ divides } |F| - 1, \\ 0 & \text{otherwise}. \end{cases}$$

https://doi.org/10.1017/S1446788700022527 Published online by Cambridge University Press

Since the identity subgroup $E_0 = 1$ of $E(S)$ leaves all families invariant, $\Psi(1; F) = (1/p)\binom{p}{|E|}$.

For each $i \geqslant 0$ and d_i dividing $d = |E(S)|$, let $\mathscr{A}_i$ denote the collection of all $\mathscr{F}$ which are invariant under $E_i \leqslant E(S)$. Then $|\mathscr{A}_i| = \Psi(E_i; F)$.

LEMMA 2.5. *$\mathscr{A}_i \cap \mathscr{A}_j = \mathscr{A}_j$ if and only if d_i divides d_j.*

PROOF. Now d_i divides d_j implies that $E_i \leqslant E_j$ so that any $\mathscr{F}$ invariant under E_j is also invariant under E_i. Now if $\mathscr{A}_i = \mathscr{A}_j$, the result is true. So we may assume that $\mathscr{A}_j \subset \mathscr{A}_i$ and that there is no $\mathscr{A}_k$ with $\mathscr{A}_j \subset \mathscr{A}_k \subset \mathscr{A}_i$. Let $\mathscr{F} \in \mathscr{A}_j$. By Lemma 2.2, there exists $F \in \mathscr{F}$ such that either $F = \bigcup_\alpha \alpha E_j$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_j$. Since $\mathscr{A}_j \subset \mathscr{A}_i$, $\mathscr{F}$ is also invariant under E_i, and the same $F \in \mathscr{F}$ will have the property that $aF = F$ for all $a \in E_i$. Hence either $F = \bigcup_\alpha \alpha E_i$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_i$. Thus we have either $F = \bigcup_\alpha \alpha E_j = \bigcup_\alpha \alpha E_i$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_j = \bigcup_\alpha \alpha E_i$. By letting $b \in E_j \setminus E_i$, we check that d_i divides d_j.

Let $[a, b]$ denote the least common multiple of a and b. Using Lemma 2.5, we obtain the following lemma.

LEMMA 2.6. *$\mathscr{A}_i \cap \mathscr{A}_j = \mathscr{A}_k$ if and only if $d_k = [d_i, d_j]$.*

LEMMA 2.7. *$E(S)$ partitions $\mathscr{A}_i \setminus \bigcup_j \mathscr{A}_j$ into equivalence classes each containing exactly d/d_i families.*

PROOF. Since E_i is a subgroup of $E(S)$, we have

$$E(S) = E_i \cup g^k E_i \cup \cdots \cup g^{(n-1)k} E_i$$

where g is a primitive root of p and $k = (p-1)/d$. Since $\mathscr{F} \in \mathscr{A}_i \setminus \bigcup_j \mathscr{A}_j$ is invariant under E_i, there exists $F \in \mathscr{F}$ with $F = \bigcup_\alpha \alpha E_i$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_i$. Hence the action of $E(S)$ on $\mathscr{A}_i \setminus \bigcup_j \mathscr{A}_j$ is equivalent to the action of $\{1, g^k, \ldots, g^{(n-1)k}\}$ on $\mathscr{A}_i \setminus \bigcup_j \mathscr{A}_j$. Now $g^{ak}F \neq g^{bk}F$ whenever $0 \leqslant a \neq b \leqslant n-1$. Furthermore we assert that $g^{ak}F \neq g^{bk}F + c$ for any $c \in z_p$. This assertion is true for $E_i \neq 1$ as can be seen from Lemma 2.3. It remains to show that it is true for $E_i = 1$. Without loss of generality we show that $F \neq g^{ak}F + c$ for every $c \in Z_p$ and $a \neq 0$. Suppose the contrary; then $F = g^{ak}F + c$ for some $c \in Z_p$. But this implies that $F = g^{-ak}F + d$ for some $d \in Z_p$, and $\mathscr{F}$ is invariant under $\{1, g^{ak}, g^{-ak}\}$ which is a subgroup of $E(S)$. This contradicts $\mathscr{F} \in \mathscr{A}_0 \setminus \bigcup_j \mathscr{A}_j$.

Note that the above lemma does not hold if $|F| \leqslant 1$, or $|F| \geqslant p - 1$. However we have assumed earlier that $2 \leqslant |F| \leqslant (p-1)/2$. Let $2I^*(p, d, d_i, |F|)$ denote the number of equivalence classes in $\mathscr{A}_i \setminus \bigcup_j \mathscr{A}_j$. Then by Lemma 2.7, we have

$$\frac{d}{d_i} 2I^*(p, d, d_i, |F|) = |\mathscr{A}_i| - \left|\bigcup_j \mathscr{A}_j\right|.$$

Using Lemma 2.6 and applying the principle of inclusion and exclusion, we obtain

$$2I^*(p, d, d_i, |F|) = \frac{d_i}{d} \sum_{d_i | d_j} \mu\left(\frac{d_j}{d_i}\right) \Psi(E_j; F).$$

Summing up $2I^*(p, d, d_i, |F|)$ for all d_i which divides d, we obtain

$$2I^*(p, d, |F|) = \sum_{d_i | d} 2I^*(p, d, d_i, |F|)$$

which is the number of equivalence classes in $\mathscr{F}(k)$ for a fixed S with $|E(S)| = d$. But there are altogether $\beta^*(p, m, d)$ non-equivalence S with $|E(S)| = d$, $0 < |S| \leqslant (p-1)/2$. Thus summing up $2I^*(p, d, |F|)\beta^*(p, m, d)$ for all d even (recall that d is a common divisor of m and $p - 1$), we get

$$2I(p, m, |F|) = \sum_{d \text{ even}} 2I^*(p, d, |F|)\beta^*(p, m, d).$$

THEOREM 2.8. *The number of Type-*I *2-circulant graphs $X = X(S, 1, F)$ with $|S| = m$ and $2 \leqslant |F| \leqslant (p-1)/2$ is given by*

$$2I(p, m, |F|) = \sum_{d} 2I^*(p, d, |F|)\beta^*(p, m, d)$$

where the summation ranges over all even common divisors d of m and $p - 1$.

EXAMPLE 1. Let $p = 13$, $m = 6$ and $k = 6$. Then the common divisors d of m and $p - 1$ are $1 < 2 < 3 < 6$.

(i) When $d = 6$,

$$2I^*(p, 6, 1, 6) = \tfrac{1}{6} \sum_{1 | d_j} \mu(d_j) \Psi(E_j; F) = 18,$$

$$2I^*(p, 6, 2, 6) = \tfrac{2}{6} \sum_{2 | d_j} \mu\left(\frac{d_j}{2}\right) \Psi(E_j; F) = 6,$$

$$2I^*(p, 6, 3, 6) = \tfrac{3}{6} \sum_{3 | d_j} \mu\left(\frac{d_j}{3}\right) \Psi(E_j; F) = 2,$$

$$2I^*(p, 6, 6, 6) = \tfrac{6}{6} \sum_{6 | d_j} \mu\left(\frac{d_j}{6}\right) \Psi(E_j; F) = 2.$$

https://doi.org/10.1017/S1446788700022527 Published online by Cambridge University Press

Thus

$$2I^*(p,6,6) = \sum_{d|6} 2I^*(p,6,d,6) = 28,$$

$$\beta^*(p,m,6) = \tfrac{6}{m} \sum_{6|d_j} \mu\left(\frac{d_j}{6}\right) \begin{pmatrix} \dfrac{p-1}{d_j} - 1 \\ \dfrac{m}{d_j} - 1 \end{pmatrix} = 1.$$

(ii) When $d = 2$,

$$2I^*(p,2,1,6) = \tfrac{1}{2} \sum_{1|d_j} \mu(d_j) \Psi(E_j; F) = 56,$$

$$2I^*(p,2,2,6) = \tfrac{2}{2} \sum_{2|d_j} \mu\left(\frac{d_j}{2}\right) \Psi(E_j; F) = 18,$$

$$2I^*(p,2,6) = 74,$$

$$\beta^*(p,m,2) = \tfrac{2}{m} \sum_{2|d_j} \mu\left(\frac{d_j}{2}\right) \begin{pmatrix} \dfrac{p-1}{d_j} - 1 \\ \dfrac{m}{d_j} - 1 \end{pmatrix} = 3.$$

Hence

$$2I(p,m,6) = \sum_{d} 2I^*(p,d,6)\beta^*(p,m,d) = 250.$$

For the case $H = Z_p^*$, we note that $E(S) = Z_p^*$ and that the expression $2I^*(p, d, d_i, |F|)$ also works for $d = p - 1$. Hence $2I^*(p, p-1, |F|) = \sum_{d|p-1} 2I^*(p, p-1, d, |F|)$. However there is only one circulant graph $X(p, S)$ with $S = Z_p^*$. Thus $2I(p, p-1, |F|) = 2I^*(p, p-1, |F|)$ and we have the following formula which counts the number of weak starred polygons of degree $|F|$ on $2p$ vertices. (See [6] for the definition of weak starred polygons.)

THEOREM 2.9. $2I(p,0,|F|) = 2I(p, p-1, |F|) = \sum_{d|p-1} 2I^*(p, p-1, d, |F|)$.

3. Type-II 2-circulants

In this section we shall count Type-II 2-circulant graphs $X(S, q, F)$ with $|S| = m$ and $|F| = k$. We proceed by determining the conditions on q which make $X(S, q, F)$ Type-II 2-circulant.

https://doi.org/10.1017/S1446788700022527 Published online by Cambridge University Press

PROPOSITION 3.1. *A 2-circulant graph* $X = X(S, q, F)$ *with* $\varnothing \subset F \subset Z_p$ *is Type-*II *if and only if* $q = g^{k/2}a$ *for some* $a \in E(S)$, *where g is a primitive root of p and* $k = (p-1)/|E(S)|$.

PROOF. Now $Z_p^* = E(S) \cup gE(S) \cup \cdots \cup g^{k-1}E(S)$. If X is Type-II 2-circulant, then $qS \neq S$ and so $q \notin E(S)$ and $q = g^{\alpha}a$ for some $a \in E(S)$ and $0 < \alpha \leqslant k-1$. Now since $q^2 = g^{2\alpha}a^2 \in E(S)$ we must have $g^{2\alpha} \in E(S)$. But this is possible only if $2\alpha \equiv 0 \pmod{k}$ or $\alpha = k/2$.

On the other hand if $q = g^{k/2}a$, then $qS \neq S$. Since $\varnothing \subset F \subset Z_p$, X is a Type-II 2-circulant graph according to Theorem 8 of [2].

COROLLARY 3.2 [2, Theorem 9]. *If* $X = X(S, q, F)$ *is a Type-*II *2-circulant graph, then* $p \equiv 1 \pmod 4$.

PROOF. Since X is Type-II 2-circulant, Proposition 3.1 asserts that $k/2 = (p-1)/2d$ is an integer. Since d is even, the result follows.

COROLLARY 3.3. *If* $X = X(S, q, F)$ *is of Type-*II *2-circulant, then* $2|E(S)|$ *divides* $p-1$.

PROOF. If $X = X(S, q, F)$ is Type-II 2-circulant, then by Proposition 3.1, $k = (p-1)/|E(S)|$ is an even integer. Hence the result follows.

THEOREM 3.4 [2, Theorem 10]. *Two Type-*II *2-circulant graphs* $X(S, q, F)$ *and* $X(S, q', F')$ *are isomorphic if and only if there exists* $\alpha \in E(S)$ *with* $\alpha F = F'$.

Let $\#(a)$ denote the order of $a \in E(S)$.

LEMMA 3.5. *If* $X = X(S, q, F)$ *is Type-*II *2-circulant, then* $\#(q^2)$ *is even.*

PROOF. Since $q = g^{k/2}a = g^{k/2}g^{rk}$, $0 \leqslant r \leqslant d-1$, we have $q^2 = g^{(2r+1)k}$. Since d is even, it follows that $q^{2n} = g^{n(2r+1)k} = 1$ only if n is even. Hence $\#(q^2)$ is even.

LEMMA 3.6. *Let* $\#(q^2) = d_i$. *Then for any* $j \in F$, $jE_v \subseteq F$ *where* $d_v = 2d_i$.

PROOF. It suffices to show that $1 \in F$ implies $E_v \subseteq F$. Let $1 \in F$. Then by condition (iv)(b), $-q \in F$. Continuing we have $(-1)^r q^r \in F$ where $0 \leqslant r \leqslant 2d_i - 2$. Then $\{1, q^2, \ldots, q^{2d_i-2}\} \cup -q\{1, q^2, \ldots, q^{2d_i-2}\} \subseteq F$. Since d_i is even by Lemma

https://doi.org/10.1017/S1446788700022527 Published online by Cambridge University Press

3.5, it follows that $-q\{1, q^2, \ldots, q^{2d_i-2}\} = q\{1, q^2, \ldots, q^{2d_i-2}\}$. Since $\#(q^2) = d_i$, we see that $q^2 = g^{k_i}$ and so $q = g^{k_i/2} = g^{k_v}$. Thus $\{1, q^2, \ldots, q^{2d_i-2}\} \cup q\{1, q^2, \ldots, q^{2d_i-2}\} = E_v$ and the lemma follows.

Thus we see that if $|F| \neq 1$, then F depends on the choice of q, and for this reason we may sometimes write $F = F(q)$. Since $d_v = 2d_i = 2\#(q^2)$ and $F = \bigcup_\alpha \alpha E_v$ or $F \setminus \{0\} = \bigcup_\alpha \alpha E_v$, we have the following corollary.

COROLLARY 3.7. *If* $X = X(S, q, F)$ *is Type-*II *2-circulant, then* $\varnothing \subset F \subset Z_p$ *and* $|F| \equiv 0 \pmod{2\#(q^2)}$ *or* $|F| \equiv 1 \pmod{2\#(q^2)}$.

Let $\mathscr{B}(|F(q)|)$ denote the collection of all $F(q)$ of a Type-II 2-circulant $X(S, q, F(q))$ with $|F(q)| > 1$. Then

$$|\mathscr{B}(|F(q)|)| = \begin{cases} \dbinom{(p-1)/2\#(q^2)}{|F|/2\#(q^2)} & \text{if } |F| \equiv 0 \left(\operatorname{mod} 2\#(q^2)\right), \\ \dbinom{(p-1)/2\#(q^2)}{(|F|-1)/2\#(q^2)} & \text{if } |F| \equiv 1 \left(\operatorname{mod} 2\#(q^2)\right), \\ 0 & \text{otherwise.} \end{cases}$$

Let (a, b) denote the greatest common divisor of a and b.

LEMMA 3.8. *The action of* $E(S)$ *partitions* $\mathscr{B}(|F(q)|)$ *into equivalence classes each containing exactly* $d/(2\#(q^2), d)$ *elements.*

PROOF. Let $2\#(q^2) = d_v = 2d_i$, and $(2\#(q^2), d) = d_t$. Then $E_v \cap E(S) = E_t$ and

$$E(S) = E_t \cup g^k E_t \cup \cdots \cup g^{(d/d_t-1)k} E_t,$$
$$E_v = E_t \cup g^{k_v} E_t \cup \cdots \cup g^{(d_v/d_t-1)k_v} E_t.$$

Since F or $F \setminus \{0\} = \bigcup_\alpha \alpha E_v = \bigcup_\beta \beta E_t$, we see that the action of $E(S)$ on $\mathscr{B}(|F(q)|)$ is equivalent to the action of $\{1, g^k, \ldots, g^{(d/d_t-1)k}\}$ on $\mathscr{B}(|F(q)|)$. Furthermore $g^{ak}F \neq g^{bk}F$ for any $0 \leqslant a \neq b \leqslant d/d_t - 1$ and this proves the lemma.

Let $2II^*(p, d, |F(q)|)$ denote the number of equivalence classes in $\mathscr{B}(|F(q)|)$ for a fixed S with $|E(S)| = d$. Then by Lemma 3.8

$$2II^*(p, d, |F(q)|) = \frac{(2\#(q^2), d)}{d} |\mathscr{B}(|F(q)|)|,$$

$|F(q)| > 1$. Furthermore, if $F(q) = \{0\}$, then $E(S)$ fixes $F(q)$ so that $2II^*(p, d, |F(q)|) = 1$. Since there are altogether $\beta^*(p, m, d)$ non-equivalent S

https://doi.org/10.1017/S1446788700022527 Published online by Cambridge University Press

with $|E(S)| = d$ and $|S| = m$, on summing $2II^*(p, d, |F(q)|)\beta^*(p, m, d)$ for all common divisors d of m and $p-1$ with $2d$ dividing $p-1$, we obtain $2II(p, m, |F(q)|)$, the number of Type-II 2-circulant graphs $X(S, q, F(q))$ with $|S| = m$.

THEOREM 3.9. *The number of Type-*II *2-circulant graphs* $X = X(S, q, F(q))$ *with* $|S| = m$ *is given by*

$$2II(p, m, |F(q)|) = \sum_d 2II^*(p, d, |F(q)|)\beta^*(p, m, d)$$

where the summation ranges over all even common divisors d of m and p $-$ 1 *with* $2d$ *dividing p* $-$ 1.

REMARK. If $S = \varnothing$, $S = Z_p^*$ or $F = \varnothing$, $F = Z_p$ then $X(S, q, F)$ is Type-I 2-circulant. Hence $2II(p, 0, k) = 0 = 2II(p, m, 0)$. Note that $2II(p, m, |F(q)|) = 2II(p, p-1-m, p-|F(q)|)$. Furthermore since $2II^*(p, d, |F(q)|) = 2II^*(p, d, p-|F(q)|)$ it follows that $2II(p, m, |F(q)|) = 2II(p, m, p-|F(q)|)$.

EXAMPLE 2. Let $p = 13$, $m = 6$ and $|F(q)| = 4$. Then the even common divisors d of m and $p-1$ are 2 and 6.

(i) When $d = 2$, $\#(q^2) = 2$ and so $2II^*(p, d, 4) = 3$ and $\beta^*(p, m, 2) = 2$.

(ii) When $d = 6$, then either $\#(q^2) = 2$ or $\#(q^2) = 6$. Since $2\#(q^2)$ must divide $|F(q)|$, only $\#(q^2) = 2$ is possible. So $2II^*(p, d, 4) = 1$ and $\beta^*(p, m, 6) = 1$.

Thus $2II(p, m, |F(q)|) = \Sigma_d 2II^*(p, m, d)\beta^*(p, m, d) = 10$.

4. GRR on $2p$ vertices

Let G be a finite group and H a subset of G with the properties (i) $1 \notin H$ and (ii) $h \in H$ implies $h^{-1} \in H$. Then the *Cayley graph* of G with respect to the *generating set* H is the graph $X_{G,H}$ with $V(X_{G,H}) = G$ and $E(X_{G,H}) = \{(g, gh) | h \in H\}$. Clearly $X_{G,H}$ is connected if and only if $\langle H \rangle = G$. A graph X is called a *graphical regular representation* (GRR) of a group G if the automorphism group $A(X)$ of X is regular, as a permutation group, and isomorphic to G. Sabidussi in [11] shows that if X is a GRR, then $X \cong \overline{K}_2$, or else X is connected and $X \cong X_{G,H}$ for some group G and some generating set H of G. In this section we shall apply the method developed in Section 2 to count the number of GRR on $2p$ vertices. A special case of our result is a partial solution (Corollary 4.7) to a problem (8b) raised in [9]: which groups have a cubic GRR?

We remark that the set of Type-I 2-circulant graphs coincides with the set of Cayley graphs $X_{D_p,J}$. (Here $D_p = \langle a, b | a^p = b^2 = 1, bab = a^{-1} \rangle$ denotes the dihedral group of order $2p$.) For if $X = X_{D_p,H}$, then X is of Type-I 2-circulant $X(S, 1, F)$ with $S = \{i | a^i \in H\}$ and $F = \{i | a^i b \in H\}$. Conversely if $X = X(S, 1, F)$, then X is a Cayley graph on the cyclic group Z_{2p}, or on the dihedral group D_p [2, Theorem 6]. Moreover if $X = X_{Z_{2p},H}$, then $X \cong X_{D_p,H'}$ for some generating set H' of D_p.

Let $\alpha \in Z_p^*$ and $c \in Z_p$ and define $\psi_{\alpha,c}$: $D_p \to D_p$ by $\psi_{\alpha,c}(a^i) = a^{\alpha i}$ and $\psi_{\alpha,c}(a^i b) = a^{\alpha i + c} b$. Then the automorphism group of D_p is $A(D_p) = \{\psi_{\alpha,c} | \alpha \in Z_p^*, c \in Z_p\}$ [6, Lemma 2]. Now any isomorphism ψ of $X_1 = X_{D_p,H}$ onto $X_2 = X_{D_p,H'}$ with $\psi(H) = H'$ corresponds to an isomorphism (α, c) of $X_1 = X(S, 1, F)$ onto $X_2 = X(S', 1, F')$ with $\alpha S = S'$ and $\alpha F = F' + c$. Thus ψ is of the form $\psi = \psi_{\alpha,c} \in A(D_p)$. This observation proves the following lemma.

LEMMA 4.1. *Let $X = X_{D_p,H}$. Then $\{\psi \in A(X) | \psi(1) = 1\} \leqslant A(D_p)$.*

Let $X = X_{G,H}$. Since $\{\psi \in A(G) | \psi(H) = H\} \leqslant \{\psi \in A(X) | \psi(1) = 1\}$ and that X is a GRR of G if and only if $\{\psi \in A(X) | \psi(1) = 1\} = \{1\}$, we have

COROLLARY 4.2. *$X_{D_p,H}$ is a GRR of D_p if and only if there exists no nontrivial group automorphism $\psi \in A(D_p)$ with $\psi(H) = H$.*

THEOREM 4.3. *Let $X = X(S, 1, F)$ where $0 < |S| \leqslant (p-1)/2$. Then X is a GRR of D_p if and only if $F \notin \mathscr{F}$ for any $\mathscr{F}$ which is invariant under some nontrivial subgroup of $E(S)$.*

PROOF. If $F \notin \mathscr{F}$ for any $\mathscr{F}$ which is invariant under some nontrivial subgroup of $E(S)$, then $F \in \mathscr{F}$ for some $\mathscr{F} \in \mathscr{A}_0$. This means that $\alpha F \neq F + c$ for any $c \in Z_p$ unless $\alpha = 1$ and $c = 0$. By Corollary 4.2 and the above discussion, this implies that X is a GRR of D_p.

Conversely let X be a GRR of D_p. Since $|V(X)| = 2p$, $X \cong X_{D_p,H}$, $H = \{a^i, a^j b | i \in S, j \in F\}$. If $F \in \mathscr{F}$ for some $\mathscr{F} \in \mathscr{A}_i$ ($i \geqslant 1$), then for some $1 \neq \alpha \in E_i \subseteq E(S)$, we have $\alpha S = S$ and $\alpha F = F + c$ for some $c \in Z_p$. Since $X(S, 1, F) \cong X(S, 1, F + d)$ for any $d \in Z_p$, we can assume without loss of generality that F is such that $c = 0$ so that $\alpha S = S$ and $\alpha F = F$. But then this α corresponds to a nontrivial group automorphism $\psi_{\alpha,0}$ of D_p such that $\psi_{\alpha,0}(H) = H$. This however contradicts Corollary 4.2 that X is a GRR of D_p.

Applying Theorem 4.3 and the results in Section 2, we obtain the following result.

THEOREM 4.4. *The number of GRR $X(S, 1, F)$ with $0 < |S| \leqslant (p-1)/2$ is given by*

$$s(p, |S|, |F|) = \sum_{d \text{ even}} 2I^*(p, d, 1, |F|)\beta^*(p, |S|, d)$$

where the summation is extended over all even common divisors d of $|S|$ and $p-1$.

We note that

$s(p, m, k) = s(p, m, p-k)$ and $s(p, m, k) = s(p, p-m-1, p-k)$. We remark that Theorem 4.3 is also true for $S = Z_p^*$. Now there is only one circulant graph $X(p, S)$ with $S = Z_p^*$ and hence

$$s(p, p-1, |F|) = 2I^*(p, p-1, 1, |F|) = \frac{1}{p-1}\sum_{d_i}\mu(d_i)\Psi(E_i; F)$$

where the summation is over all divisors d_i of $p-1$ such that d_i divides $|F|$ or $|F|-1$. Thus we have the following result.

THEOREM 4.5. $s(p, 0, |F|) = (1/(p-1))\Sigma_{d_i}\mu(d_i)\Psi(E_i; F)$.

Note that if $|F| \leqslant 2$ or $|F| \geqslant p-2$, then $s(p, m, |F|) = 0$ for any $m \geqslant 0$. We are interested in the case when $m = 0$ and $|F| = 3$. We shall omit the proof since it is straight forward.

COROLLARY 4.6. *$s(p, 0, 3)$ is equal to $(p-7)/6$ if 3 divides $p-1$ and equal to $(p-5)/6$ otherwise.*

A group G is said to have a *cubic GRR* if there exists a GRR $X_{G,H}$ of G with $|H| = 3$.

COROLLARY 4.7. *D_p has a cubic GRR if and only if $p \geqslant 11$.*

References

[1] B. Alspach, 'Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree,' *J. Combin. Theory Ser. B.* **15** (1973), 12–17.

[2] B. Alspach and R. Sutcliffe, 'Vertex-transitive graphs of order $2p$,' *Ann. New York Acad. Sci.* **319** (1979), 18–27.

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

[4] G. L. Chia and C. K. Lim, 'A class of self-complementary vertex-transitive digraphs,' *J. Combin. Theory*, to appear.
[5] G. L. Chia, *A class of strongly vertex transitive digraphs*, (M. Sc. Thesis, University of Malaya, 1979).
[6] J. K. Doyle, 'Weak starred polygons and Cayley graphs,' *Nanta Math.* **11** (1978), 7–9.
[7] B. Elspas and J. Turner, 'Graphs with circulant adjecency matrices,' *J. Combin. Theory* **9** (1970), 297–307.
[8] C. D. Godsil, 'On Cayley graph isomorphisms,' Research Report No. 21, 1977, University of Melbourne.
[9] C. D. Godsil, 'Unsolved Problems,' Summer Research Workshop in Algebraic Combinatorics, July 1979, Simon Fraser University.
[10] F. Harary, *Graph theory* (Addison-Wesley, Reading, Menlo Park, London,1969).
[11] G. Sabidussi, 'On a class of fixed-point-free graphs,' *Proc. Amer. Math. Soc.* **9** (1958), 800–804.
[12] J. Turner, 'Point-symmetric graphs with a prime number of points,' *J. Combin. Theory* **3** (1967), 136–145.
[13] M. E. Watkins, 'On the action of non-Abelian groups on graphs,' *J. Combin. Theory* **11** (1971), 95–104.

Department of Mathematics
University of Malaya
Kuala Lumpur 22-11
Malaysia