Can. J. Math., Vol. XXXIV, No. 2, 1982, pp. 307–318

A CONSTRUCTION FOR VERTEX-TRANSITIVE GRAPHS

BRIAN ALSPACH AND T. D. PARSONS

1. Introduction. A useful general strategy for the construction of interesting families of vertex-transitive graphs is to begin with some family of transitive permutation groups and to construct for each group Γ in the family all graphs G whose vertex-set is the orbit V of Γ and for which $\Gamma \leqq \mathrm{Aut}\ (G)$, where Aut (G) denotes the automorphism group of G. For example, if we consider the family of cyclic groups $\langle (0\ 1\ \ldots\ n-1) \rangle$ generated by cycles $(0\ 1\ \ldots\ n-1)$ of length n, then the corresponding graphs are the n-vertex circulant graphs.

In this paper we consider transitive permutation groups of degree mn generated by a "rotation" ρ which is a product of m disjoint cycles of length n and by a "twisted translation" τ such that $\tau\rho\tau^{-1} = \rho^{\alpha}$ for some α. The abstract groups isomorphic to the groups $\Gamma = \langle \rho, \tau \rangle$ are the semi-direct products of two cyclic groups. We call the corresponding graphs *metacirculants*.

We note that similar constructions apply to vertex-transitive digraphs, though we shall restrict our attention here to graphs.

2. A family of transitive permutation groups. Let $Z_m = \{0, 1, \ldots, m-1\}$ and $Z_n = \{0, 1, \ldots, n-1\}$ be the rings of integers modulo m and n, respectively, where $m \geqq 1$ and $n \geqq 2$. Let $Z_r{}^*$ denote the group of units of the ring Z_r. Let

$$V = \{v_j{}^i : i \in Z_m \quad \text{and} \quad j \in Z_n\}$$

where superscripts and subscripts are always reduced modulo m and modulo n, respectively.

Let $\alpha \in Z_n{}^*$ and define two permutations ρ and τ on V by

$$\rho(v_j{}^i) = v_{j+1}^i$$

and

$$\tau(v_j{}^i) = v_{\alpha j}^{i+1}.$$

Received April 16, 1980. The authors wish to thank the Canadian Mathematical Society, the Natural Sciences and Engineering Research Council of Canada, and Simon Fraser University for their support of the Summer Research Workshop in Algebraic Combinatorics during July 1979, at which this research was carried out.

It is easy to see that ρ and τ generate a transitive subgroup $\langle \rho, \tau \rangle$ of the symmetric group on V.

Notice that ρ has a cycle decomposition as

$$\rho = (v_0{}^0 v_1{}^0 \ldots v_{n-1}^0)(v_0{}^1 v_1{}^1 \ldots v_{n-1}^1) \ldots (v_0{}^{m-1} v_1{}^{m-1} \ldots v_{n-1}^{m-1})$$

so that $\langle \rho \rangle$ is cyclic of order n and has the m orbits $V^0, V^1, \ldots, V^{m-1}$ where $V^i = \{v_0{}^i, v_1{}^i, \ldots, v_{n-1}^i\}$ for $i = 0, 1, \ldots, m-1$.

Now let a be the order of α in $Z_n{}^*$ and let $b = \operatorname{lcm}(a, m)$. Then

$$\tau^b(v_j{}^i) = v_{\alpha^b j}^{i+b} = v_j{}^i$$

since $b \equiv 0 \pmod m$ and $\alpha^b \equiv 1 \pmod n$. Hence, $\tau^b = 1$ and the order of τ divides b. On the other hand, if $\tau^c = 1$, then

$$v_1{}^0 = \tau^c(v_1{}^0) = v_{\alpha^c}^c$$

so that $c \equiv 0 \pmod m$ and $\alpha^c \equiv 1 \pmod n$. This implies that b divides c. Thus, τ has order b and the cyclic subgroup $\langle \tau \rangle$ has order b.

It is easy to verify that $\langle \rho \rangle \cap \langle \tau \rangle = \{1\}$ and that $\tau \rho \tau^{-1} = \rho^\alpha$. The group $\langle \rho, \tau \rangle$ has the presentation

$$\langle \rho, \tau : \quad \rho^n = 1 = \tau^b, \tau \rho \tau^{-1} = \rho^\alpha \rangle$$

and so has a rather simple structure. Indeed, $\langle \rho \rangle$ is a normal subgroup of $\langle \rho, \tau \rangle$ and $\rho \to \rho^\alpha$ is an automorphism of $\langle \rho \rangle$ so that $\langle \rho, \tau \rangle$ is a semi-direct product of $\langle \rho \rangle$ by $\langle \tau \rangle$. If $\alpha - 1 \in Z_n{}^*$, it is not hard to see that $\langle \rho, \tau \rangle$ is a metacyclic group.

Now suppose that we wish to construct all those graphs G having vertex-set $V(G) = V$ and for which $\langle \rho, \tau \rangle \leqq \operatorname{Aut}(G)$. Let $\mu = \lfloor m/2 \rfloor$ and abbreviate "is adjacent to" by $\sim$. An arbitrary unordered pair of distinct vertices of G can be written as an ordered pair $(v_j{}^i, v_h{}^{i+r})$ for some r such that $0 \leqq r \leqq \mu$. In fact, the ordering will be unique unless $r = 0$ or m is even and $r = m/2 = \mu$. If $\langle \rho, \tau \rangle \leqq \operatorname{Aut}(G)$, we have $v_j{}^i \sim v_h{}^{i+r}$ if and only if $v_0{}^0 \sim v_s{}^r$ where $s = \alpha^{-i}(h - j)$. Therefore, to construct G it suffices to specify the sets

$$S_r = \{s \in Z_n : v_0{}^0 \sim v_s{}^r\} \quad \text{for } 0 \leqq r \leqq \mu$$

and to determine what conditions these sets S_r must satisfy in order that $\langle \rho, \tau \rangle \leqq \operatorname{Aut}(G)$.

First, $0 \notin S_0$ or else G would have loops. Since $\rho \in \operatorname{Aut}(G)$, we need $S_0 = -S_0$. Further, $s \in S_r$ if and only if $v_0{}^0 \sim v_s{}^r$ if and only if $\tau^m(v_0{}^0) \sim \tau^m(v_s{}^r)$ if and only if $v_0{}^0 \sim v_{\alpha^m s}^r$ if and only if $\alpha^m s \in S_r$. In case m is even (so that $\mu = m/2$), then $s \in S_\mu$ if and only if

$$v_0{}^0 \sim v_s{}^\mu$$

if and only if

$$\tau^\mu(v_0{}^0) \sim v_{\alpha^\mu s}^0 = \tau^\mu(v_s{}^\mu)$$

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

if and only if

$$\rho^{-\alpha^{\mu}s}(v_0^{\mu}) = v_{-\alpha^{\mu}s}^{\mu} \sim v_0^{0} = \rho^{-\alpha^{\mu}s}(v_{\alpha^{\mu}s}^{0})$$

if and only if

$$-\alpha^{\mu}s \in S_{\mu}.$$

Finally, if the remaining edges of G are given by

$$E(G) = \{\{v_j^{i}, v_h^{i+r}\}: 0 \leqq r \leqq \mu \quad \text{and} \quad \alpha^{-i}(h-j) \in S_r\},$$

it is then easy to see that $\langle \rho, \tau \rangle \leqq \text{Aut } (G)$.

3. Metacirculant graphs. We summarize the above four conditions for the basic definition to follow.

(1) $0 \notin S_0 = -S_0$
(2) $\alpha^m S_r = S_r \quad \text{for } 0 \leqq r \leqq \mu$
(3) If m is even, then $\alpha^{\mu} S_{\mu} = -S_{\mu}$
(4) $E(G) = \{\{v_j^{i}, v_h^{i+r}\}: 0 \leqq r \leqq \mu \quad \text{and} \quad h - j \in \alpha^{i} S_r\}$.

If $m \geqq 1, n \geqq 2, \alpha \in Z_n^*, \mu = \lfloor m/2 \rfloor$, and if $S_0, S_1, \ldots, S_{\mu}$ are subsets of Z_n satisfying conditions (1), (2), and (3), then we define the *metacirculant graph* $G = G(m, n, \alpha, S_0, \ldots, S_{\mu})$ to be the graph with $V(G) = V$ and with $E(G)$ given by (4). We shall also say that G is an (m, n)-metacirculant graph.

These are special cases of the "uniformly (m, n)-galactic graphs" studied by Marušič [**3**]. The $(2, p)$-metacirculants (where p is a prime) have been discussed in [**3**], and earlier in [**1**].

It is straightforward to check that G is a well-defined graph such that $\langle \rho, \tau \rangle \leqq \text{Aut } (G)$. By the above discussion we have the following result.

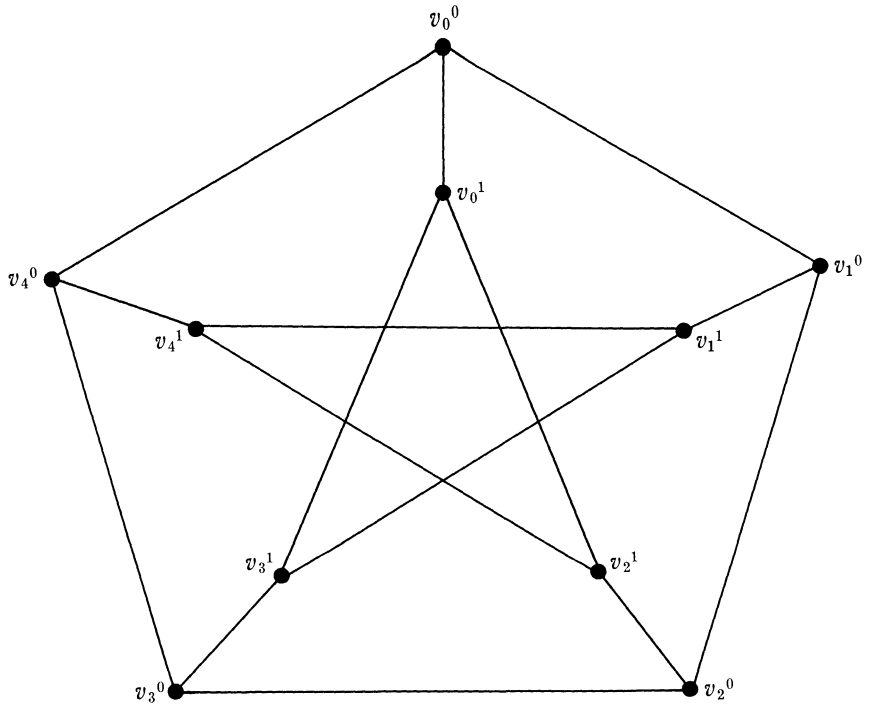
THEOREM 1. *The metacirculant $G = G(m, n, \alpha, S_0, \ldots, S_{\mu})$ is vertex-transitive with $\langle \rho, \tau \rangle \leqq \text{Aut } (G)$. Conversely, any graph G' with vertex-set V and $\langle \rho, \tau \rangle \leqq \text{Aut } (G')$ is an (m, n)-metracirculant.*

This approach to metacirculant graphs should be viewed as a constructive approach. First one chooses the number of blocks and the block sizes (m and n, respectively). Then one chooses $\alpha \in Z_n^*$ which can be viewed as how a block is "twisted" as it goes onto the next block. The sets $S_0, S_1, \ldots, S_{\mu}$ are then chosen so as to accommodate α^m. The edges are then put in to accommodate $\langle \rho, \tau \rangle$.

Example 1. The metacirculant $G(2, 5, 2, \{1, 4\}, \{0\})$ is the Petersen graph.

Recall that if Γ is a group and $1 \notin \Delta = \Delta^{-1} \subseteq \Gamma$, then the Cayley graph $K(\Gamma, \Delta)$ has vertex-set Γ and edge-set $\{\{x, x\delta\}: x \in \Gamma \text{ and } \delta \in \Delta\}$. For any Cayley graph $K(\Gamma, \Delta)$, the automorphism group Aut $K(\Gamma, \Delta)$

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press



contains the left regular representation of Γ, thus $K(\Gamma, \Delta)$ is vertex-transitive. In fact, this property is characteristic for Cayley graphs, since by a theorem of Sabidussi [**4**] a graph is Cayley if and only if its automorphism group contains a regular subgroup.

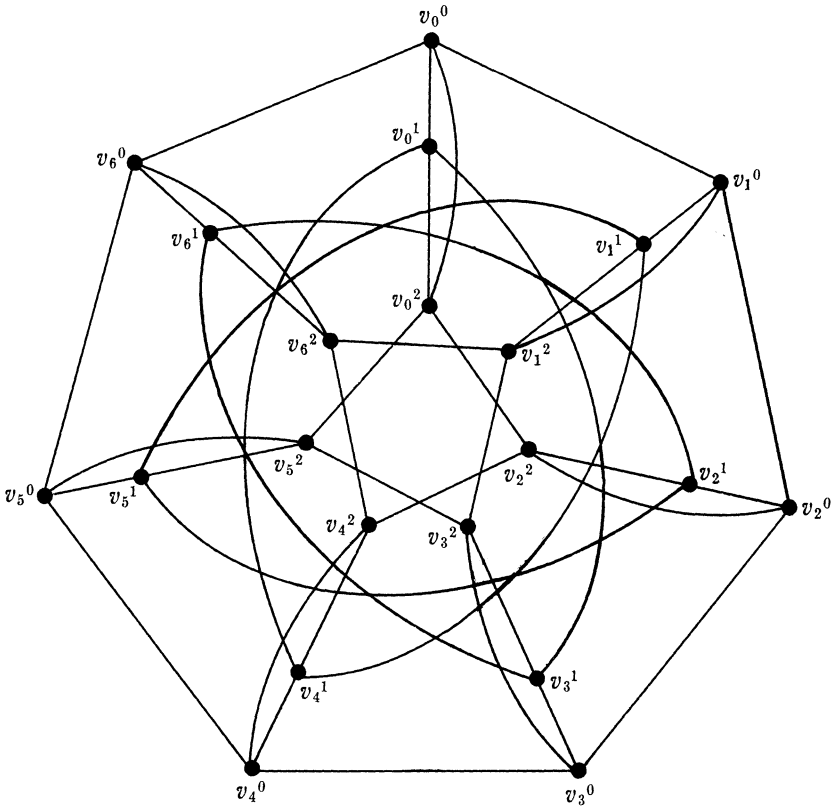
Suppose Γ is a semi-direct product of a cyclic group of order n by a cyclic group of order m. Then Aut $K(\Gamma, \Delta)$ contains a regular subgroup isomorphic to Γ, and this subgroup must be a semi-direct product of a cyclic subgroup $\langle \rho \rangle$ of order n by a cyclic subgroup $\langle \tau \rangle$ of order m. Now $\tau\rho\tau^{-1} = \rho^\alpha$ for some integer α relatively prime to n, and thus $\langle \tau \rangle$ acts as a permutation group on the m orbits of $\langle \rho \rangle$. Since $\langle \rho, \tau \rangle$ is regular, and hence transitive on the vertices of $K(\Gamma, \Delta)$, τ must permute the orbits of $\langle \rho \rangle$ in a cycle of length m. Therefore we can label the vertices of $K(\Gamma, \Delta)$ as v_j^i, $i \in Z_m$ and $j \in Z_n$, so that

$$\rho = (v_0^0 v_1^0 \ldots v_{n-1}^0) \ldots (v_0^{m-1} v_1^{m-1} \ldots v_{n-1}^{m-1}) \quad \text{and} \quad \tau(v_j^i) = v_{\alpha j}^{i+1}.$$

Theorem 1 then implies that $K(\Gamma, \Delta)$ is an (m, n)-metacirculant.

THEOREM 2. *Every Cayley graph $K(\Gamma, \Delta)$, for a group Γ which is a semi-direct product of a cyclic group of order n by a cyclic group of order m, is an (m, n)-metacirculant graph.*

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press



Example 2. The metacirculant $G(3, 7, 3, \{1, 6\}, \{0\})$ is the Cayley graph $K(\Gamma, \Delta)$ for

$$\Gamma = \langle a, b : a^3 = 1 = b^7, aba^{-1} = b^2 \rangle \quad \text{and} \quad \Delta = \{a, b, a^{-1}, b^{-1}\}.$$

Not every vertex-transitive graph is a Cayley graph. Sabidussi [**5**] has characterized vertex-transitive graphs in a way which shows their close relation to Cayley graphs. However, it is usually not easy to compute whether given vertex-transitive graphs are Cayley graphs.

Recently, Godsil [**2**] has determined those Kneser graphs $K(n, k)$ which are Cayley graphs. The Kneser graph $K(n, k)$ has as its vertices the k-element subsets of $\{1, 2, \ldots, n\}$, where $n \geqq 2k + 1$ and $k \geqq 2$, and has as its edges the unordered pairs of k-sets which are disjoint. In particular, Godsil showed that the "odd graphs" $O_{k+1} = K(2k + 1, k)$ are non-Cayley. The Petersen graph is $K(5, 2)$.

Among vertex-transitive graphs, it may be expected that the Cayley graphs enjoy special properties. For instance, there are only six known connected vertex-transitive graphs which are non-Hamiltonian, and these

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

graphs are not Cayley graphs. It may be that all connected Cayley graphs are Hamiltonian. If one wishes to study vertex-transitive graphs in general, then it is desirable to have some nice constructions for families of vertex-transitive non-Cayley graphs, such as the odd graphs.

As can be seen from Theorem 2 and Example 1, some metacirculants are Cayley graphs and others are not. We shall investigate which metacirculants are Cayley graphs.

4. Metacirculants which are Cayley graphs. We now seek conditions on the structure parameters of metacirculants which will result in these graphs being Cayley graphs. One such condition is that $\alpha = 1$.

THEOREM 3. *The Cayley graph* $K(Z_m \times Z_n, \Delta)$ *is isomorphic to the metacirculant* $G(m, n, 1, S_0, \ldots, S_\mu)$ *where* $S_r = \{j \in Z_n: (r, j) \in \Delta)\}$ *for* $0 \leqq r \leqq \mu$.

Proof. It is easy to see that the mapping $(i, j) \to v_j{}^i$ is an isomorphism.

The circulant graph Circ (n, S) is the Cayley graph $K(\mathbf{Z}_n, S)$ where $\mathbf{Z}_n$ is the additive group of integers modulo n. Every such circulant graph is trivially representable as a metacirculant $G(1, n, 1, S_0)$ with $S_0 = S$. By Theorem 3, if m and n are relatively prime, then Circ (mn, S) is representable as $G(m, n, 1, S_0, \ldots, S_\mu)$ with $S_r = \{j \pmod n: nr + mj \in S\}$ for $0 \leqq r \leqq \mu$. However, if gcd $(m, n) \neq 1$, then Circ (mn, S) may fail to be representable as any $G(m, n, \alpha, S_0, \ldots, S_\mu)$. This is the case for the 9-cycle C_9 = Circ $(9, \{1, 8\})$, which is not any $G(3, 3, \alpha, S_0, S_1)$.

Let $F(S_r) = \{\beta \in \mathbf{Z}_n{}^*: \beta S_r = S_r\}$ for $0 \leqq r \leqq \mu$ and let $F(G) = \bigcap_{r=0}^{\mu} F(S_r)$. Clearly, $F(S_0)$, $F(S_1)$, $\ldots$, $F(S_\mu)$ and $F(G)$ are subgroups of the multiplicative group $\mathbf{Z}_n{}^*$. If $\beta \in F(G)$ it is obvious that the mapping $v_j{}^i \to v_{\beta j}{}^i$ is an automorphism of G. In addition, the identity mapping $v_j{}^i \to v_j{}^i$ is an isomorphism of G onto $G(m, n, \alpha\beta, S_0, \ldots, S_\mu)$. Therefore, if $\alpha \in F(G)$ and so $\alpha^{-1} \in F(G)$, then $v_j{}^i \to v_j{}^i$ is an isomorphism of G onto $G(m, n, \alpha\alpha^{-1}, S_0, \ldots, S_\mu)$. But $\alpha\alpha^{-1} \equiv 1 \pmod n$ and we obtain a corollary to Theorem 3.

COROLLARY 4. *If* $\alpha \in F(G)$, *then the metacirculant graph* G *is a Cayley graph* $K(Z_m \times Z_n, \Delta)$. *In addition, if* gcd $(m, n) = 1$, *then* G *is a circulant graph.*

Let $E_\alpha = \{e \in \mathbf{Z}: \alpha^e \in F(G)\}$. Then $m \in E_\alpha$ by condition (2) earlier and $a \in E$ (recall that a is the order of α in $\mathbf{Z}_n{}^*$). We abbreviate "r divides s" by $r|s$. Now $a|\phi(n)$, where $\phi(n) = |Z_n{}^*|$ is the Euler phi function. Since $(E_\alpha, +)$ is a subgroup of the integers Z, we have $E_\alpha = \{dx: x \in \mathbf{Z}\}$ where d is the smallest positive element of E_α. Thus, d divides gcd (a, m) = gcd $(a, m, \phi(n))$. If gcd $(a, m) = 1$, which will certainly

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

hold if gcd $(m, \phi(n)) = 1$, then $d = 1$ so that $\alpha \in F(G)$. In this case, Corollary 4 gives the following two results.

COROLLARY 5. *If* gcd $(a, m) = 1$, *then* $G \cong K(Z_m \times Z_n, \Delta)$.

COROLLARY 6. *If* gcd $(m, n) =$ gcd $(m, \phi(n)) = 1$, *then all* (m, n)-*metacirculant graphs are circulant graphs.*

We now improve upon the above simple observations. Assume that gcd $(a, m) > 1$ and let $p_1, \ldots, p_k$ be the distinct primes dividing both a and m. Let

$$a = p_1^{e_1} \ldots p_k^{e_k} a' \quad \text{and} \quad m = p_1^{f_1} \ldots p_k^{f_k} m'$$

where gcd $(a, m') = 1 =$ gcd (a', m). Let

$$A = \{i : 1 \leqq i \leqq k \quad \text{and} \quad e_i > f_i\} \quad \text{and}$$

$$u = a' \prod_{i \in A} p_i^{e_i} \quad \text{if } A \neq \emptyset$$

while $u = a'$ if $A = \emptyset$.

LEMMA 7. *Let* $w \in \mathbf{Z}$. *Then* $u|w$ *if and only if for every* $t \in \mathbf{Z}$ *we have* $m|wt$ *implies* $a|wt$.

Proof. Suppose that $w = uv$ for some v. If $m|wt$ and $i \notin A$, then $f_i \geqq e_i$ and $p_i^{f_i}|wt$ so that $p_i^{e_i}|wt$. Since

$$a' \prod_{i \in A} p_i^{e_i}|wt,$$

we certainly have that $a|wt$.

Conversely, suppose that $m|wt$ implies $a|wt$ for all integers t. Let $p_i^{\sigma_i}$, $\sigma_i \geqq 0$, be the highest power of p_i dividing w for $i = 1, 2, \ldots, k$. Choose

$$t = m' \prod_{i:\sigma_i < f_i} p_i^{f_i - \sigma_i}.$$

Then $m|wt$ so that $a|wt$. If $\sigma_i < f_i$, then $p_i^{f_i}$ is the highest power of p_i dividing wt. Now $a|wt$, so that $a'|w$ and $p_i^{e_i}|wt$ for $i = 1, 2, \ldots, k$. When $e_i > f_i$, then $\sigma_i \geqq f_i$ must hold and $p_i^{\sigma_i}$ is the highest power of p_i that divides both wt and w. Hence, $\sigma_i \geqq e_i$ for $i \in A$, so $u|w$.

Recall that a permutation group is semi-regular if the only permutation that has any fixed points is the identity permutation.

LEMMA 8. *With* u *as defined above, the group* $\langle \rho, \tau^u \rangle$ *is semi-regular and has order* $m'n \prod_{i \notin A} p_i^{f_i}$.

Proof. Recall that τ has order $b =$ lcm (a, m). We have

$$b = a'm' \prod_{i \in A} p_i^{e_i} \prod_{i \notin A} p_i^{f_i}$$

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

so that

$$b/u = m' \prod_{i \notin A} p_i^{f_i}.$$

From the discussion in Section 2, it follows that

$$\langle \rho, \tau^u \rangle = \{\rho^s \tau^{ut} : 0 \leqq s \leqq n-1 \quad \text{and} \quad 0 \leqq t \leqq b/u\}$$

has order $nb/u = m'n \prod_{i \notin A} p_i^{f_i}$. Suppose that $v_j^i = \rho^s \tau^{ut}(v_j^i)$. Then

$$v_j^i = \rho^s(v_{j\alpha^{ut}}^{i+ut}) = v_{j\alpha^{ut}+s}^{i+ut}.$$

Thus, $m|ut$. By Lemma 7, we have $a|ut$ so that

$$\alpha^{ut} \equiv 1 \pmod{n} \quad \text{and} \quad j \equiv j + s \pmod{n}.$$

This implies that $s \equiv 0 \pmod{n}$ and $\rho^s = 1$. Also, $m|ut$ and $a|ut$ imply that $b|ut$ so that $\tau^{ut} = 1$. We conclude that $\rho^s \tau^{ut} = 1$, and so 1 is the only element of $\langle \rho, \tau^u \rangle$ having a fixed point.

THEOREM 9. *Let* $G = G(m, n, \alpha, S_0, \ldots, S_\mu)$, *a be the order of* $\alpha \in \mathbf{Z}_n^*$, *and* $c = a/\gcd(a, m)$. *If* $\gcd(c, m) = 1$, *then G is a Cayley graph for the group* $\langle \rho, \tau^c \rangle$. *Furthermore, this group is abelian if* $\gcd(a, m) = 1$ *and it is cyclic if* $\gcd(a, m) = 1 = \gcd(m, n)$.

Proof. Letting $a = a' p_1^{e_1} \ldots p_k^{e_k}$ and $m = m' p_1^{f_1} \ldots p_k^{f_k}$ as done before, we have that $\gcd(c, m) = 1$ if and only if $f_i \geqq e_i$, $i = 1, \ldots, k$, if and only if $A = \emptyset$ and $u = a' = c$. By Lemma 8, if $\gcd(c, m) = 1$, then $\langle \rho, \tau^c \rangle$ is semi-regular of order mn. Thus its order and degree are equal so that $\langle \rho, \tau^c \rangle$ is a regular permutation group contained in Aut (G). Therefore G is a Cayley graph. If $\gcd(a, m) = 1$, then $c = a$ so the group is $\langle \rho, \tau^a \rangle$ and it is abelian because $\tau^a \rho \tau^{-a} = \rho^{\alpha^a} = \rho$. Furthermore, if $\gcd(m, n) = 1$, then $\langle \rho, \tau^a \rangle = \langle \rho \tau^a \rangle$ is cyclic and G is a circulant graph.

5. Metacirculants of order qp. In Theorem 9 we have given sufficient conditions for the metacirculant $G(m, n, \alpha, S_0, \ldots, S_\mu)$ to be a Cayley graph. We now seek necessary conditions. We specialize m and n to be distinct primes q and p with $q < p$. In this case, we can determine the structure of the Sylow p-subgroups of Aut (G).

LEMMA 10. *The Sylow p-subgroups of* Aut (G) *have order* $p^e > p$ *if and only if* $e = q$ *if and only if for each* r, $0 < r \leqq \mu$, *we have* $S_r = \emptyset$ *or* $S_r = \mathbf{Z}_p$.

Proof. Assume that for each r, $0 < r \leqq \mu$, that $S_r = \emptyset$ or $S_r = \mathbf{Z}_p$. It is clear that Aut (G) contains the p-group P of order p^q that is the direct product $\prod_{i=1}^{q} \langle \rho_i \rangle$ where ρ_i is the p-cycle

$$\rho_i = (v_0^i v_1^i \ldots v_{p-1}^i).$$

But Aut (G) is a subgroup of the symmetric group of degree qp, and the

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

Sylow p-subgroups of this symmetric group have order p^q. Thus, P is a Sylow p-subgroup of Aut (G) and we have $e = q$.

Assume that $e = q$. Then since $q > 1$, we know that the Sylow p-subgroups of Aut (G) have the order $p^e > p$.

Finally, assume that the Sylow p-subgroups of Aut (G) have order $p^e > p$. Let P be a Sylow p-subgroup containing the automorphism ρ. It is then clear that the orbits of P are $V^0, V^1, \ldots, V^{q-1}$. Consider P_0, the stabilizer of $v_0{}^0$ under P. Since P restricted to any orbit is cyclic of order p, P_0 fixes every vertex in V^0. Suppose that for some $r \neq 0$, both $S_r \neq \emptyset$ and $S_r \neq Z_p$. Then P_0 must fix every vertex of V^r since P restricted to V^r is a p-group. In the same way, P_0 must fix every vertex of V^{2r}, which implies then P_0 fixes every vertex of V^{3r}. Continuing in this way we obtain P_0 is trivial. This implies that $|P| = p$, which is a contradiction. From this contradiction, we conclude that for every $r \neq 0$ we have $S_r = \emptyset$ or $S_r = \mathbf{Z}_p$.

Notice that if $|P| > p$, then by Lemma 10 the metacirculant G is a wreath product of an order q circulant over an order p circulant, and so G is isomorphic to a circulant graph of order qp.

LEMMA 11. *Let H be a multiplicative cyclic group of order n and $x \in H$ be an element of order e. Then there exists a generator g of H such that $g^{n/e} = x$.*

Proof. (L. Babai). Let $H = \langle h \rangle$. Then $\langle x \rangle = \langle h^{n/e} \rangle$ is the unique subgroup of order e so that $x = h^{nt/e}$ for some t relatively prime to e. Let $n^* = n/\gcd(n, e^n)$ so that $\gcd(e, n)^* = 1$. By the Chinese Remainder Theorem, there is an integer r such that $r \equiv t \pmod{e}$ and $r \equiv 1 \pmod{n^*}$. Then $\gcd(r, n) = 1$ so that $g = h^r$ generates H and

$$g^{n/e} = h^{rn/e} = h^{(t+ke)n/e} = h^{tn/e} = x.$$

THEOREM 12. *Let $G = G(q, p, \alpha, S_0, \ldots, S_\mu)$ where $q < p$ are primes. Suppose that $q^2 | a$ and for some r, $0 < r \leqq \mu$, $0 < |S_r| < p$. Then G is a Cayley graph if and only if $\alpha S_0 = S_0$ and there exists a cyclic permutation $\hat{\sigma} = (i_0 i_1 \ldots i_{q-1})$ of $\mathbf{Z}_q = \{0, 1, \ldots, q-1\}$ and a sequence $a_0, a_1, \ldots, a_{q-1}$ in $\mathbf{Z}_p$ having the properties*$_\gamma$

(i) *If $0 < r \leqq \mu$, $0 \leqq k \leqq q-1$, and $\hat{\sigma}(k+r) \equiv \hat{\sigma}(k) + t \pmod{q}$ for some t such that $0 < t \leqq \mu$, then*

$$S_r = \alpha^{\hat{\sigma}(k)-k} S_t + \alpha^{-k}(a_k - a_{k+r}) \pmod{p}.$$

(ii) *If $0 < r \leqq \mu$, $0 \leqq k \leqq q-1$, and $\hat{\sigma}(k) \equiv \hat{\sigma}(k+r) + t \pmod{q}$ for some t such that $0 < t \leqq \mu$, then*

$$S_r = -\alpha^{\hat{\sigma}(k+r)-k} S_t + \alpha^{-k}(a_k - a_{k+r}) \pmod{p}.$$

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

(iii) *For some* $\gamma \in Z_p$, *where either* $\gamma = 1$ *or* $\gamma = \alpha^{a/q}$, *we have*

$$\gamma^q a_{i_0} + \gamma^{q-1} a_{i_1} + \ldots + \gamma a_{i_{q-1}} \equiv 0 \pmod{p}.$$

(*In conditions* (i), (ii) *the subscript on* a_{k+r} *is reduced modulo* q.)

Proof. Suppose that the hypotheses of Theorem 12 hold. Using Lemma 11, we can let $\mathbf{Z}_p^* = \langle \lambda \rangle$ and $\alpha = \lambda^{(p-1)/a}$. Now assume that G is a Cayley graph, so that Aut (G) contains a regular subgroup Γ of order qp. By Lemma 10, The Sylow p-subgroups of Aut (G) have order p. Replacing Γ by one of its conjugates in Aut (G), if necessary, we lose no generality in assuming that $\langle \rho \rangle \leqq \Gamma$. Then there exists $\sigma \in$ Aut (G) such that $\Gamma = \langle \rho, \sigma \rangle$ and $\sigma^q = 1 = \rho^p$ and $\sigma\rho\sigma^{-1} = \rho^\gamma$ where $\gamma^q \equiv 1 \pmod{p}$. If $\gamma \not\equiv 1 \pmod{p}$, by replacing σ with an appropriate σ^j, we may assume that $\gamma = \lambda^{(p-1)/q}$ so that $\Gamma = \langle \rho, \sigma \rangle$ where $\sigma^q = 1 = \rho^p$, $\sigma\rho\sigma^{-1} = \rho^\gamma$ and either $\gamma = 1$ or $\gamma = \lambda^{(p-1)/q}$. If $\gamma = 1$, then $\gamma \in F(G)$. Otherwise,

$$\gamma = \lambda^{(p-1)/q} = (\lambda^{(p-1)/a})^{a/q} = \alpha^{a/q} = \alpha^{qs}$$

for some integer s because $q^2 | a$. Since $\alpha^q \in F(G)$, we have that $\gamma \in F(G)$. In either case, $\gamma \in F(G)$ so that $\gamma S_r = S_r$ for $0 \leqq r \leqq \mu$.

Now $\Gamma = \langle \rho, \sigma \rangle$ is transitive and imprimitive on $V(G)$ with blocks $V^0, V^1, \ldots, V^{q-1}$ so that $\langle \sigma \rangle$ acts transitively on the blocks. We may define a cyclic permutation $\hat{\sigma}$ on Z_q by $\sigma(V^i) = V^{\hat{\sigma}(i)}$. Define $a_i \in Z_p$ by $\sigma(v_0{}^i) = v_{\gamma a_i}{}^{\hat{\sigma}(i)}$. Then we claim

$$(A)\ \sigma(v_j{}^i) = v_{\gamma(j+a_i)}^{\hat{\sigma}(i)} \quad \text{for all } i \in Z \quad \text{and} \quad j \in Z_p.$$

To see this, note that

$$(\sigma(v_0{}^0)\sigma(v_1{}^0) \ldots \sigma(v_{p-1}^0)) \ldots (\sigma(v_0{}^{q-1})\sigma(v_1{}^{q-1}) \ldots \sigma(v_{p-1}^{q-1}))$$
$$= \sigma\rho\sigma^{-1} = \rho^\gamma = (v_0{}^0 v_\gamma{}^0 \ldots v_{(p-1)\gamma}^0) \ldots (v_0{}^{q-1} v_\gamma{}^{q-1} \ldots v_{(p-1)\gamma}^{q-1}),$$

and together with the definition of $\hat{\sigma}$ this implies (A).

Let $\hat{\sigma} = (i_0 i_1 \ldots i_{q-1})$ where $i_0 = 0$, $i_1 = \hat{\sigma}(0)$, and so on. From (A) we obtain

$$\sigma^j(v_0{}^0) = v_{\gamma^j a_0 + \gamma^{j-1} a_{i_1} + \ldots + \gamma a_{i_{j-1}}}^{\hat{\sigma}^j(0)}.$$

Since $\sigma^q = 1$, this yields

$$\gamma^q a_{i_0} + \gamma^{q-1} a_{i_1} + \ldots + \gamma a_{i_{q-1}} \equiv 0 \pmod{p}.$$

We now obtain conditions on $S_0, \ldots, S_\mu$ by using the fact that (A) determines $\sigma \in$ Aut (G). Recall that $\gamma \in F(G)$. We have $\gamma j \in \alpha^k S_0$ if and only if $v_0{}^k \sim v_j{}^k$ if and only if

$$v_{\gamma a_k}{}^{\hat{\sigma}(k)} = \sigma(v_0{}^k) \sim \sigma(v_j{}^k) = v_{\gamma(j+a_k)}^{\hat{\sigma}(k)}$$

if and only if

$$\gamma j \in \alpha^{\hat{\sigma}(k)} S_0.$$

Therefore, $\alpha^k S_0 = \alpha^{\hat{\sigma}(k)} S_0$ which implies that $S_0 = \alpha^{\hat{\sigma}(0)} S_0$. Now $\hat{\sigma}(0) \in \{1, 2, \ldots, q-1\}$ modulo q and since both α^q and $\alpha^{\hat{\sigma}(0)}$ are in $F(S_0)$, we have $\alpha \in F(S_0)$, so that $\alpha S_0 = S_0$.

Now let $0 < r \leqq \mu$. Similarly to the above we obtain $\gamma j \in \alpha^k S_r$ if and only if

$$v_{\gamma a_k}^{\hat{\sigma}(k)} \sim v_{\gamma(j+a_{k+r})}^{\hat{\sigma}(k+r)}.$$

There are two cases to consider.

In case 1, we have $\hat{\sigma}(k+r) \equiv \hat{\sigma}(k) + t \pmod{q}$ for some t satisfying $0 < t \leqq \mu$. The adjacency condition in the previous paragraph then holds if and only if

$$\gamma(j + a_{k+r}) - \gamma a_k \in \alpha^{\hat{\sigma}(k)} S_t$$

if and only if

$$j + a_{k+r} - a_k \in \alpha^{\hat{\sigma}(k)} S_t$$

if and only if

$$j \in \alpha^{\hat{\sigma}(k)} S_t + (a_k - a_{k+r}).$$

This shows that

$$S_r = \alpha^{\hat{\sigma}(k)-k} S_t + \alpha^{-k}(a_k - a_{k+r}).$$

In case 2, we have $\hat{\sigma}(k) \equiv \hat{\sigma}(k+r) + t \pmod{q}$ for some t satisfying $0 < t \leqq \mu$. Using an argument similar to that for case 1, we obtain that

$$S_r = -\alpha^{\hat{\sigma}(k+r)-k} S_t + \alpha^{-k}(a_k - a_{k+r}).$$

This completes the argument that if G is a Cayley graph, then $\alpha S_0 = S_0$ and conditions (i), (ii), (iii) hold. Suppose that, conversely, $\alpha S_0 = S_0$ and conditions (i), (ii), (iii) hold for some appropriate cyclic permutation $\hat{\sigma}$ of Z_q and sequence $a_0, a_1, \ldots, a_{q-1}$ in $\mathbf{Z}_p$. Let $\gamma = 1$ if $a_0 + a_1 + \ldots + a_{q-1} \equiv 0 \pmod{p}$. Otherwise, let $\gamma = \alpha^{a/q}$. Define $\sigma(v_j^i)$ by (A). Then $\sigma^q = 1$ by condition (iii) and the fact that $\hat{\sigma} = (i_0 i_1 \ldots i_{q-1})$ has length q. Furthermore, $\sigma \in \mathrm{Aut}\,(G)$ as can be seen by reversing the various "if and only if" statements used previously. Lastly, $\sigma\rho\sigma^{-1} = \rho^\gamma$ follows from (A). Thus $\langle \rho, \sigma \rangle$ is a regular subgroup of Aut (G), which implies that G is a Cayley graph.

This concludes the proof of Theorem 12.

COROLLARY 13. *Let $q^2 | p - 1$ and $q^2 | a$. Let $S_0, \ldots, S_\mu$ be such that $\alpha S_0 \neq S_0$ but $\alpha^q S_r = S_r$ for $0 \leqq r \leqq \mu$. Suppose for some r, $0 < r \leqq \mu$, that $0 < |S_r| < p$. Then $G(q, p, \alpha, S_0, \ldots, S)$ is not a Cayley graph.*

https://doi.org/10.4153/CJM-1982-020-8 Published online by Cambridge University Press

Proof. This follows immediately from Theorem 12.

Let q be a prime. By Dirichlet's famous theorem, there are infinitely many primes p in the arithmetic progression $1, 1 + q^2, 1 + 2q^2, \ldots$, that is, there are infinitely many primes $p > q$ such that q^2 divides $p - 1$. Choose such a prime p and let $p - 1 = q^k N$ where gcd $(q, N) = 1$. If λ generates $\mathbf{Z}_p^*$, then choose $\alpha = \lambda^N$, $S_0 = \langle \alpha^q \rangle \cup (-\langle \alpha^q \rangle)$, each S_r for $0 < r \leqq \mu = (q - 1)/2$ to be a union of cosets of $\langle \alpha^q \rangle$ in $\mathbf{Z}_p^*$ together possibly with the element 0 of $\mathbf{Z}_p$, and have at least one S_r, $r \geqq 1$, non-empty and not equal to $\mathbf{Z}_p$. Then $G(q, p, \alpha, S_0, \ldots, S_\mu)$ is not Cayley and it is easy to see how to construct many other such vertex-transitive non-Cayley graphs by using Theorem 12 similarly.

As a particular example, let $q = 3, p = 19, \alpha = 4, S_0 = \{1, 7, 8, 11, 12, 18\}$ and $S_1 = \{0\}$. The resulting (3, 19)-metacirculant is non-Cayley, has 57 vertices, and is regular of degree 8.

There are several problems about metacirculants that we wish to mention. In [3] it is shown that the line-graph of the Petersen graph is not a metacirculant, although its automorphism group has an element ρ which is a product of three disjoint 5-cycles. Marušič has also pointed out to us that the odd graph O_4 of order $35 = 5 \cdot 7$ is not a metacirculant, though it also has an automorphism which is a "rotation" ρ, the product of five 7-cycles. We do not know of any other vertex-transitive graphs with qp vertices which are not (q, p)-metacirculants, although it seems likely that some such graphs will exist. So the first problem is to characterize the vertex-transitive graphs of order qp, and in particular, those which are not metacirculants.

The second problem is to find necessary and sufficient conditions for $G(q, p, \alpha, S_0, \ldots, S_\mu)$ and $G(q, p, \alpha', S_0', \ldots, S_\mu')$ to be isomorphic. This was done for $q = 2$ in [1, 3].

A third problem is to determine which (m, n)-metacirculants are Hamiltonian.

References

1. B. Alspach and J. Sutcliffe, *Vertex-transitive graphs of order* $2p$, Annals N.Y. Acad. Sci. *319* (1979), 19–27.
2. C. Godsil, *More odd graph theory*, Discrete Math. *32* (1980), 205–207.
3. D. Marušič, *On vertex-symmetric digraphs*, Discrete Math. *36* (1981), 69–82.
4. G. Sabidussi, *On a class of fixed-point-free graphs*, Proc. Amer. Math. Soc. *9* (1958), 800–804.
5. ——— *Vertex-transitive graphs*, Monatsh. Math. *68* (1964), 426–438.

Simon Fraser University,
Burnaby, British Columbia;
Pennsylvania State University,
University Park, Pennsylvania