University of Ljubljana
Institute of Mathematics, Physics and Mechanics
Department of Mathematics
Jadranska 19, 1111 Ljubljana, Slovenia

Preprint series, Vol. 41 (2003), 909

ON THE NUMBER OF CLOSED WALKS IN VERTEX-TRANSITIVE GRAPHS

Robert Jajcay Aleksander Malnič
Dragan Marušič

ISSN 1318-4865

December 10, 2003

Ljubljana, December 10, 2003

ON THE NUMBER OF CLOSED WALKS IN VERTEX-TRANSITIVE GRAPHS

ROBERT JAJCAY[1]
Department of Mathematics
Indiana State University
Terre Haute, IN 47809
U.S.A.
jajcay@cayley.indstate.edu

ALEKSANDER MALNIČ [1]
IMFM, Oddelek za matematiko
Univerza v Ljubljani
Jadranska 19, 1111 Ljubljana
Slovenija
aleksander.malnic@uni-lj.si

DRAGAN MARUŠIČ [1]
IMFM, Oddelek za matematiko
Univerza v Ljubljani
Jadranska 19, 1111 Ljubljana
Slovenija
dragan.marusic@uni-lj.si

Abstract

The results of J. Širáň and the first author (Australasian J. Combin. **10** (1994)) are generalized, and new formulas for the number of closed walks of length p^r or pq, where p and q are primes, valid for all vertex-transitive graphs are found. Based on these formulas, several simple tests for vertex-transitivity are presented, as well as lower bounds on the orders of the smallest vertex- and arc-transitive groups of automorphisms for vertex-transitive graphs of given valence.

1 Introduction

All graphs considered in this paper are finite, simple, and undirected. An *automorphism* of a graph Γ is a permutation of the vertex set $V(\Gamma)$ that preserves the edges, and Γ is *vertex-transitive* if the full automorphism group Aut Γ acts transitively on vertices. More generally, we say that a group

[1]Supported in part by the COBASE program of the "National Academy of Sciences", and by "Ministrstvo za šolstvo, znanost in šport Slovenije", grant SLO-US-2002/12.

$G \leq \mathrm{Aut}\Gamma$ acts *t-arc-transitively*, $t \geq 0$, on Γ if it acts transitively on the set of all t-arcs of Γ, where a *t-arc* is a sequence $(v_0, \ldots, v_t)$ of $t+1$ vertices of Γ such that for each $i \in \{0, \ldots, t-1\}$ the vertices v_i and v_{i+1} are adjacent, and for each $i \in \{1, \ldots, t-1\}$, $v_{i-1} \neq v_{i+1}$. In particular, Γ is *t-arc-transitive* provided $\mathrm{Aut}\Gamma$ acts t-arc-transitively.

The study of vertex-transitive graphs is an area of interplay between graph theory and the theory of permutation groups. This area of research has many applications ranging from topological graph theory to constructing reliable and cost-efficient interconnection networks [5, 6].

For a given finite graph Γ, it is decidedly hard to determine whether Γ is vertex-transitive, and the ultimate answer comes usually only after a substantial part of the full automorphism group of Γ has been determined. Similarly, even if Γ is known to be vertex-transitive, any further questions about the "automorphism" properties of Γ (for example, whether Aut Γ contains a regular subgroup, that is, whether Γ is a Cayley graph) require good knowledge of the action of Aut Γ. Thus, any graph theoretic characteristics allowing for a simplification of these problems based on some "easily" computable characteristics of Γ are important, and have been the topic of a considerable number of articles with most of the results focusing on properties determined by the order and/or the valence of the graph under consideration [2, 10, 12, 13, 15].

The aim of this paper is to study the impact of another graph-theoretic property, namely, the number of closed walks and oriented cycles, on the automorphism group of the graph. This approach appeared for the first time in [3], and was further developed in a series of articles [7, 8, 9].

A *closed walk of length n* in a graph Γ is any sequence $(v_0, \ldots, v_{n-1})$ of n vertices of Γ that satisfies the property that for each $i \in \{0, \ldots, n-2\}$ the vertices v_i and v_{i+1} as well as the vertices v_{n-1} and v_0 are adjacent. A closed walk is an *oriented cycle of length n* if all the vertices $v_0, \ldots, v_{n-1}$ are distinct, and, in each case, we say that the walk or the cycle is *based* at v_0. In [8], the following result concerning the number of closed walks and the number of generators of a specified order has been proved for all Cayley graphs.

Proposition 1.1 ([8]) *Let $\Gamma = Cay(G, X)$ be a finite Cayley graph and p, q be two distinct primes.*

Then the number of closed walks of length p^r, $r \geq 1$, based at any fixed vertex of Γ, is congruent (mod p) to the number of elements in X for which

$x^{p^r} = 1$.

If $n = pq$ and j_n denotes the number of elements $x \in X$ for which $x^n = 1$, then the number of closed walks of length n, based at any fixed vertex of Γ, is congruent (mod p) to $j_n + sq$, where s is a nonnegative integer.

We generalize the above proposition in two ways.

First, in Section 2 we show that a similar statement holds for the number of oriented cycles of any Cayley graph (Theorem 2.1). This result can be used as a quick test to exclude that a graph is Cayley (Corollary 2.2).

Second, in Section 3 we study a connection between lexicographic product of a given vertex-transitive graph with a totally disconnected graph and certain Cayley graphs associated with the automorphism group of the vertex-transitive graph in question (Propositions 3.1 and 3.4).

This allows us, in Section 4, to generalize Proposition 1.1 to the number of closed walks in all vertex-transitive graphs (Theorem 4.2). In addition, Theorem 4.6 gives us lower bounds on the order of the vertex stabilizers of t-arc transitive graphs, $t \geq 1$, relating these orders to the valence and girth of the graphs.

Finally, in Section 5, we present several examples and applications of the above mentioned results.

2 Oriented cycles in Cayley graphs

Cayley graphs comprise one of the most important classes of vertex transitive graphs: If G is any (finite) group and X is any unit-free symmetric subset of G, that is, $1 \notin X$ and $x^{-1} \in X$ whenever $x \in X$, then the (right) *Cayley graph* $Cay(G, X)$ has G as its vertex set, and two vertices $a, b \in G$ are adjacent if and only if $a^{-1}b \in X$. Note that $Cay(G, X)$ is connected if and only if X generates all of G. The group G acts regularly (as a subgroup of the group of automorphisms) on the vertex set of $Cay(G, X)$ by left multiplication. Hence, every Cayley graph is vertex-transitive, and a vertex-transitive graph is a Cayley graph if and only if it admits a regular automorphism subgroup of its full automorphism group.

The following theorem is a natural restatement of Proposition 1.1 for cycles. The proof we present here is just a modification of the original proof in [3], and its main idea can be traced back to the proof of Cauchy's theorem

on the existence of elements of prime order in a finite group (see, for instance, [1]).

We use $\mathcal{W}_\Gamma^b(n)$ to denote the *set of closed walks of length n based at a fixed vertex b of a graph Γ*, and $\mathcal{C}_\Gamma^b(n)$ to denote *the set of oriented cycles of length n rooted at b*. Further, let $\omega_X(n)$ denote *the number of elements of order n in a subset X* of a group G, and let $\varepsilon_X(n)$ denote the number of $x \in X$ such that $x^n = 1_G$ (or, equivalently, the order of x divides n). We remark that all the results presented in this section hold for infinite locally finite Cayley graphs as well, but we shall state and use them for finite Cayley graphs only.

Theorem 2.1 *Let $\Gamma = Cay(G, X)$ be a Cayley graph, and let $b \in V(\Gamma)$. Then the following statements hold.*

(i) If $n = p^r$, where p is an odd prime and $r \geq 1$, or $n = 2^r$, where $r \geq 2$, then

$$|\mathcal{C}_\Gamma^b(n)| \equiv \omega_X(n) \pmod{p}.$$

(ii) If $n = p \cdot q$, where p and q are distinct primes, then

$$|\mathcal{C}_\Gamma^b(n)| \equiv \omega_X(n) + s \cdot q \pmod{p},$$

where s is a nonnegative integer.

Proof: Consider an arbitrary oriented cycle C of Γ of length n rooted at b. Then $C = v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n$, where $v_0 = b = v_n$, all the other vertices are distinct, and the e_i's are the corresponding arcs connecting the consecutive vertices of C. Since each arc e_i is associated with a unique generator $x_i \in X$, its color in X, the cycle C determines a sequence $x_1, x_2, \ldots, x_n$ of generators from X that satisfies the following additional properties:

(a) $x_1 x_2 \ldots x_n = 1_G$,

(b) $x_1 x_2 \ldots x_n$ is "cyclically reduced", that is, no shorter segment $x_j x_{j+1} \ldots x_{j+k}$, $1 \leq j \leq n$, $0 \leq k < n-1$ is equal to 1_G (with the addition in the indices performed in the "usual circular way" modulo n).

Clearly, there is a one-to-one correspondence between the set $\mathcal{C}_\Gamma^b(n)$ and the set $\mathcal{S}_X(n)$ of all words in X of length n satisfying (a) and (b), and so $|\mathcal{C}_\Gamma^b(n)| = |\mathcal{S}_X(n)|$.

Next, consider the action of the cyclic shift φ, mapping $x_1, x_2, \ldots, x_n$ to $x_2, x_3, \ldots, x_n, x_1$, on the set $\mathcal{S}_X(n)$. (Indeed, φ, being essentially a conjugation, preserves $\mathcal{S}_X(n)$.) As the order of φ is equal to n, we see that

$$|\mathcal{S}_X(n)| = \sum_{k|n} k \cdot n_k = n_1 + \sum_{k>1, k|n} k \cdot n_k,$$

where n_k stands for the number of orbits of φ on $\mathcal{S}_X(n)$ of length k.

To complete the proof, one just needs to realize that the only sequences $x_1, x_2, \ldots, x_n$ in $\mathcal{S}_X(n)$ fixed by the cyclic shift are the sequences of the form $x, x, \ldots, x$ for some $x \in X$. As any sequence $x, x, \ldots, x$ of length n belongs to $\mathcal{S}_X(n)$ if and only if the order of x is equal to n, we have that

$$|\mathcal{S}_X(n)| = \omega_X(n) + \sum_{k>1, k|n} k \cdot n_k.$$

In the case when $n = pq$, where p and q are distinct primes, we obtain

$$|\mathcal{S}_X(pq)| = \omega_X(pq) + p \cdot n_p + q \cdot n_q + pq \cdot n_{pq},$$

and so

$$|\mathcal{C}^b_\Gamma(n)| \equiv \omega_X(pq) + s \cdot q \pmod{p},$$

where $s = n_q$ is the number of orbits of φ of length q, which proves (ii).

The proof of (i) follows along the same lines, and is omitted. □

Combining Proposition 1.1 and Theorem 2.1, we have the following result.

Corollary 2.2 *Let $\Gamma = Cay(G, X)$ be a Cayley graph, $b \in V(\Gamma)$ a base vertex, and p a prime. Then the numbers $|\mathcal{W}^b_\Gamma(p)|$ and $|\mathcal{C}^b_\Gamma(p)|$ are congruent modulo p.*

Also, if p^r is the highest power of p dividing $|G|$ and $r' > r$, then the number $|\mathcal{C}^b_\Gamma(p^{r'})|$ is congruent to 0 modulo p.

Proof. The first part follows by Proposition 1.1 in view of the fact that the number $\varepsilon_X(p)$ of elements in X satisfying $x^p = 1$ is equal to the number $\omega_X(p)$ of elements of X of order p. The second part is true since G contains no elements of order $p^{r'}$. □

3 Cayley graphs of automorphism groups of vertex-transitive graphs

Recall that the notation $\Gamma[\Delta]$ stands for the *lexicographic product* of a graph Γ with a graph Δ obtained by replacing each vertex of Γ by a copy of Δ, and connecting all the vertices of any two copies of Δ that are positioned above an adjacent pair u, v of vertices of Γ (that is, the vertex set of $\Gamma[\Delta]$ is the Cartesian product $V(\Gamma) \times V(\Delta)$ with two vertices (u, v) and (u', v') adjacent whenever $u = u'$ and v and v' are adjacent in Δ, or whenever $u \neq u'$ and u is adjacent to u' in Γ). The graph $\overline{K_m}$ is the *totally disconnected* graph on m vertices with no edges. We denote the set of all vertices u adjacent to a vertex v of a graph Γ by $N(v)$.

Although the following proposition may be considered a part of the "folklore" and together with Corollary 3.2 may be deduced from some of the earliest results in the area [16], the proof we provide gives a crucial insight into the connection between vertex-transitive graphs and Cayley graphs of their vertex-transitive automorphism groups.

Proposition 3.1 *Let Γ be a vertex-transitive graph of valence d, let $b \in V(\Gamma)$ be a fixed vertex, let $G \leq \mathrm{Aut}\ \Gamma$ act transitively on $V(\Gamma)$, let $m = |Stab_G(b)|$ be the order of the vertex stabilizer of b in G, and let $X = \{g \in G \mid g(b) \in N(b)\}$. Then the Cayley graph $Cay(G, X)$ is isomorphic to $\Gamma[\overline{K_m}]$.*

Proof. For each vertex $v \in V(\Gamma)$, let $\chi_v = \{g \in G \mid g(b) = v\}$ be the "fiber" of elements in G that map b to v. As the fibers are left cosets of $Stab_G(b)$, we see that $|\chi_v| = m$, for all $v \in V(\Gamma)$, and $\chi_v \cap \chi_u = \emptyset$, for any two distinct vertices u, v of Γ. Moreover, for any $v \in V(\Gamma)$, the subgraph of $Cay(G, X)$ induced by the set of vertices χ_v is isomorphic to $\overline{K_m}$. Namely, if $f \in \chi_v$ and $g \in X$, then $(fg)(b) = f(g(b)) \neq f(b)$, and so $fg \notin \chi_v$. Therefore the set of vertices of $Cay(G, X)$ splits into fibers of size m each of which induces a subgraph isomorphic to $\overline{K_m}$. In order to complete the proof, it remains to show that for any two distinct fibers χ_v and χ_u, the subgraph induced by the union $\chi_v \cup \chi_u$ is totally disconnected whenever v and u are not adjacent (in Γ), and is isomorphic to the complete bipartite graph $K_{m,m}$ whenever v and u are adjacent (in Γ). To see the first part, it suffices to realize that $(fg)(b)$ is adjacent to $f(b)$, for all $f \in \chi_v$ and $g \in X$. In other words, if χ_v and χ_u are connected by at least one edge, then u is adjacent to v. The second

part follows from a simple counting argument. The set X consists of a union of d sets of size m. Hence $|X| = d \cdot m$, and so each vertex of the fiber χ_v is adjacent to $d \cdot m$ vertices in the fibers neighboring χ_v. As argued in the previous lines, the fiber χ_v is connected only to those fibers χ_u for which v is adjacent to u, and so χ_v is neighboring precisely d fibers. It follows that any vertex of χ_v is adjacent to precisely m vertices in each of the neighboring fibers of χ_v. Consequently, the subgraph induced by the union $\chi_v \cup \chi_u$ is a complete bipartite graph as long as u and v are adjacent in Γ, as required. □

The following corollaries of Proposition 3.1 are interesting in their own right.

Corollary 3.2 *Let Γ be a connected vertex-transitive graph, and $b \in V(\Gamma)$ a base vertex. If $G \leq \mathrm{Aut}\ \Gamma$ is vertex-transitive, and $X = \{g \in G \mid g(b) \in N(b)\}$, then X generates G.*

Proof. Let $|Stab_G(b)| = m$. Since Γ is connected, $\Gamma[\overline{K_m}] \cong Cay(G, X)$ is connected, and thus X generates G. □

Corollary 3.3 *Let Γ be a vertex-transitive graph, and $b \in V(\Gamma)$ a base vertex. If $G, G' \leq \mathrm{Aut}\,\Gamma$ are vertex-transitive groups of the same order, and X and X' are their respective subsets of automorphisms mapping b to $N(b)$, then $Cay(G, X) \cong Cay(G', X')$.*

Clearly, if Γ is vertex-transitive, so is $\Gamma[\overline{K_m}]$, for all $m \geq 1$. If, in addition, G is a group of order $m \cdot |V(\Gamma)|$ acting transitively on $V(\Gamma)$ (not even necessarily faithfully), then, by Proposition 3.1, $\Gamma[\overline{K_m}]$ is also a Cayley graph (of G). This result can be reversed for all vertex-transitive graphs that do not contain a pair of vertices u, v such that $N(u) = N(v)$.

Proposition 3.4 *Let Γ be a vertex-transitive graph in which no two vertices have identical neighborhoods. Then $\Gamma[\overline{K_m}]$ is a Cayley graph if and only if there exists a group of order $m \cdot |V(\Gamma)|$ acting transitively on $V(\Gamma)$.*

Proof. In view of Proposition 3.1, it suffices to prove that if $\Gamma[\overline{K_m}] \cong Cay(G, X)$ for some group G, then G must act vertex-transitively on $V(\Gamma)$.

Let ϕ be the isomorphism from $\Gamma[\overline{K_m}]$ onto $Cay(G, X)$, and let χ_u, for each $u \in V(\Gamma)$, be the fiber of vertices of the copy of $\overline{K_m}$ above $u \in V(\Gamma)$. We will show that the images $\phi(\chi_u)$ form an imprimitivity block system for the left-multiplication action of G on $Cay(G, X)$. To be explicit, for any two vertices f, h in $\phi(\chi_u)$ and any $g \in G$, there exists a vertex $v \in V(\Gamma)$ such that both gf and gh belong to $\phi(\chi_v)$.

The argument is once again based on counting. Obviously, the number of walks of length 2 between any two vertices from the same fiber of $\Gamma[\overline{K_m}]$ is equal to $d \cdot m$. On the other hand, the number of walks of length 2 between two vertices belonging to two distinct fibers χ_u and χ_v is $d' \cdot m$, where d' is the number of fibers in $\Gamma[\overline{K_m}]$ that are common neighbors of χ_u and χ_v. Since d' equals the number of common neighbors of u and v in Γ, and by assumption, Γ contains no two vertices with identical neighborhoods, it follows that d' is strictly smaller than d.

The above property of walks of length 2 in $\Gamma[\overline{K_m}]$ is carried over to walks of length 2 in $Cay(G, X)$. Since the left multiplication by an element $g \in G$ is a graph automorphism of $Cay(G, X)$, the number of walks of length 2 between f and h must be equal to the number of walks of length 2 between gf and gh. Consequently, G preserves the images of fibers in $Cay(G, X)$.

The remaining part of the proof rests on the fact that the induced action of G on the fibers of $Cay(G, X)$ is transitive and preserves their adjacency. Hence, G acts transitively on the vertices of Γ preserving the structure of Γ, as claimed. □

4 Closed walks in vertex-transitive graphs

The next lemma together with the results proved in the previous section will allow us to prove our main theorem concerning vertex-transitive graphs.

Lemma 4.1 *Let m be a positive integer, Γ be a vertex-transitive graph, and b and b' be base vertices in the graphs Γ and $\Gamma[\overline{K_m}]$, respectively. Then for all positive integers n we have*

$$|\mathcal{W}^{b'}_{\Gamma[\overline{K_m}]}(n)| = m^{n-1} \cdot |\mathcal{W}^{b}_{\Gamma}(n)|.$$

Proof. Since all the considered graphs are vertex-transitive, we may assume that $b \in V(\Gamma)$ is the projection of $b' \in V(\Gamma[\overline{K_m}])$. As there are no edges

within the fibers of $\Gamma[\overline{K_m}]$, any closed walk of length n based at b' in $\Gamma[\overline{K_m}]$ projects onto a closed walk of length n in Γ based at b. Now, let W be a closed walk $W = u_0, e_1, u_1, e_2, \ldots, u_{n-1}, e_n, u_n$, where $u_0 = b = u_n$, in Γ. There are m edges in $\Gamma[\overline{K_m}]$ that start at b' and project onto e_1; each of their endpoints projects onto u_1. For each choice of a lift for e_1, there are m ways to lift e_2 so that its lift will start at the endpoint of the lift of e_1, and so there are m^2 ways to lift the first two edges of W into a walk in $\Gamma[\overline{K_m}]$ starting at b'. This same argument can now be repeated for all edges of W with the exception of the last edge e_n. Since any lift of W into a closed walk at b' must end at b', the lift of e_n is the unique edge connecting the end point of the lift of e_{n-1} and b'. Thus, each closed walk based at b is a projection of m^{n-1} closed walks based at b', and the assertion of the lemma follows. $\square$

Note that there is no simple analogue of the above lemma for cycles, as not every cycle in $\Gamma[\overline{K_m}]$ projects onto a cycle in Γ (although it certainly projects onto a closed walk in Γ). However, every oriented cycle of length n in Γ lifts to m^{n-1} oriented cycles of length n containing a fixed vertex b' of $\Gamma[\overline{K_m}]$, giving us a lower bound

$$|\mathcal{C}^{b'}_{\Gamma[\overline{K_m}]}(n)| \geq m^{n-1} \cdot |\mathcal{C}^b_\Gamma(n)|.$$

Suppose now that Γ is a vertex-transitive graph of valence d, $b \in V(\Gamma)$, and that $G \leq \mathrm{Aut}\ \Gamma$ acts transitively on $V(\Gamma)$. Let $X = \{g \in G \mid g(b) \in N(b)\}$. Recall that for most of this article, we are interested in the relationships among the following numbers: the number $|\mathcal{W}^b_\Gamma(n)|$ of closed walks of length n in Γ based at b; the number $|\mathcal{C}^b_\Gamma(n)|$ of oriented cycles of length n containing b; the number $\varepsilon_X(n)$ of elements x in a subset X of G that satisfy the identity $x^n = 1$; and the number $\omega_X(n)$ of elements in X of order n.

The following generalization of Proposition 1.1 relates these numbers for the class of all vertex-transitive graphs.

Theorem 4.2 *Let Γ be a connected vertex-transitive graph, $b \in V(\Gamma)$, let $G \leq \mathrm{Aut}\ \Gamma$ act transitively on $V(\Gamma)$, m be the order of a vertex-stabilizer in G, and let $X = \{g \in G \mid g(b) \in N(b)\}$. Then the following statements hold.*

(i) If p is an odd prime divisor of m and $r \geq 1$ or $p = 2$ divides m and $r \geq 2$, then $\varepsilon_X(p^r) \equiv 0 \pmod p$, and for each prime $q \neq p$, there exists a nonnegative integer s such that $\varepsilon_X(pq) + sq \equiv 0 \pmod p$.

(ii) If p is an odd prime not dividing m and $r \geq 1$ or $p = 2$ does not divide m and $r \geq 2$, then $\varepsilon_X(p^r) \equiv |\mathcal{W}^b_\Gamma(p^r)| \pmod{p}$, and, for each prime $q \neq p$, there exists a nonnegative integer s such that $\varepsilon_X(pq) + sq \equiv |\mathcal{W}^b_\Gamma(pq)| \pmod{p}$.

Proof. We prove the theorem for the case $n = p^r$ only. The case $n = pq$ follows along similar lines.

Consider the Cayley graph $Cay(G, X)$. In view of Proposition 3.1, recall that $Cay(G, X) \cong \Gamma[\overline{K_m}]$ with the fibers χ_v, $v \in V(\Gamma)$, being the elements of G mapping b to v. Let f be any vertex from the fiber χ_b (that is, an element of $Stab_G(b)$). It follows from Proposition 1.1 that the number $|\mathcal{W}^f_{Cay(G,X)}(p^r)|$ of closed walks of length p^r based at f, is congruent (modulo p) to the number $\varepsilon_X(p^r)$. In addition, Lemma 4.1 asserts that $|\mathcal{W}^f_{Cay(G,X)}(p^r)| = m^{p^r-1} \cdot |\mathcal{W}^b_\Gamma(p^r)|$. Thus,

$$\varepsilon_X(p^r) \equiv m^{p^r-1} \cdot |\mathcal{W}^b_\Gamma(p^r)| \pmod{p}.$$

Consequently, if p divides m then $\varepsilon_X(p^r) \equiv 0 \pmod{p}$. On the other hand, if p does not divide m, Fermat's little theorem gives us $m^{p^r-1} \equiv 1 \pmod{p}$, and so $\varepsilon_X(p^r) \equiv |\mathcal{W}^b_\Gamma(p^r)| \pmod{p}$. □

In the case when p is relatively prime to the order of $|G|$ (hence, X contains no elements of order p), we obtain a simple but interesting corollary.

Corollary 4.3 *Let Γ be a connected vertex-transitive graph, $b \in V(\Gamma)$, let $G \leq \mathrm{Aut}\,\Gamma$ act transitively on $V(\Gamma)$, and suppose that p is an odd prime that does not divide $|G|$ and $r \geq 1$ or $p = 2$ does not divide $|G|$ and $r \geq 2$. Then,*

$$|\mathcal{W}^b_\Gamma(p^r)| \equiv 0 \pmod{p}.$$

Two similar statements hold under the weaker assumption that p is relatively prime to the order of the graph Γ.

Corollary 4.4 *Let Γ be a connected vertex-transitive graph of valence d, $b \in V(\Gamma)$. Let a prime $p > d$ be relatively prime to $|V(\Gamma)|$, and let r be a positive integer. Then*

$$|\mathcal{W}^b_\Gamma(p^r)| \equiv 0 \pmod{p}.$$

Proof. Since $p > d$ and Γ is connected, it follows that p does not divide the order of $Stab_G(b)$. Namely, an element of order p with fixed vertices has orbits of length p and orbits of length 1. By connectedness, at least one fixed vertex has to be adjacent to the p vertices in some orbit of length p. Such an element cannot exist in a graph Γ of valence $d < p$. Consequently, p does not divide the order of Aut Γ, and the result follows by Corollary 4.3. $\square$

Corollary 4.4 combined together with the contrapositive of Corollary 4.3 gives us additional information on the prime divisors of $|Stab_G(b)|$.

Corollary 4.5 *Let Γ be a connected vertex-transitive graph of valence d, and $b \in V(\Gamma)$. Let $G \leq$ Aut Γ act transitively on $V(\Gamma)$, and let $p < d$ be a prime relatively prime to $|V(\Gamma)|$. If for some positive integer r ($r \geq 2$ when $p = 2$), the number $|\mathcal{W}_\Gamma^b(p^r)|$ is not congruent to 0 modulo p, then p divides $|Stab_G(b)|$.*

To conclude this section, the following definitions are needed. The *diameter* $diam(\Gamma)$ of Γ is the smallest integer l such that the distance $d_\Gamma(u, v) \leq l$, for all $u, v \in V(\Gamma)$. The *girth* $g(\Gamma)$ of Γ, is the length of the shortest cycle in Γ. By $N_i(b)$ we denote the set of vertices of Γ at distance i from b.

Theorem 4.6 *Let Γ be a vertex-transitive graph of valence d, $b \in V(\Gamma)$, let $t \leq diam(\Gamma)$ be a positive integer, $G \leq$ Aut Γ act transitively on the set of t-arcs of Γ, and let $X_t = \{x \in G \mid x(b) \in N_t(b)\}$. Then for all positive integers n the numbers $\omega_{X_t}(n)$ and $\varepsilon_{X_t}(n)$ are both multiples of $|N_t(b)|$.*

Moreover, in the case when $t = 1$ the order of each $x \in X_1$ is greater than or equal to the girth of Γ.

Proof. Let $u \in N_t(b)$ be arbitrary, let X_u denote the set of all elements x in X_t that satisfy $x(b) = u$, and let X_u^n denote the subset of X_u consisting of elements of order n. Since G acts transitively on t-arcs of Γ, and every vertex $v \in N_t(b)$ is at the end of at least one t-arc originating at b, it follows that for every vertex $v \in N_t(b)$, there exists an element $a_v \in Stab_G(b)$ such that $a_v(b) = b$ and $a_v(u) = v$. Since $a_v X_u a_v^{-1} \subseteq X_v$, and conjugation preserves the orders of elements, we infer that $a_v X_u^n a_v^{-1} \subseteq X_v^n$. Hence $|X_u^n| \leq X_v^n$, and by reversing the roles of u and v, $|X_u^n| = |X_v^n|$, for all $u, v \in N_t(b)$. The first part of the lemma now follows in view of the equality

$$\omega_{X_t}(n) = \sum_{u \in N_t(b)} |X_u^n| = |N_t(b)| \cdot |X_u^n|,$$

with the result concerning $\varepsilon_{X_t}(n)$ being just a slight alteration of the above.

As for the second statement of the theorem, note that X_1 is our "usual" set X. Thus, $x(b) \in N(b)$ for all $x \in X_1$, and the vertices $x^i(b)$ and $x^{i+1}(b)$ are distinct and adjacent for all $i \geq 0$. It follows that any two consecutive vertices in the sequence $b, x(b), x^2(b), \ldots, x^{|x|-1}(b), x^{|x|}(b) = b$ are adjacent, and the sequence contains a cycle of length not greater than $|x|$. Thus, $g(\Gamma) \leq |x|$, for all $x \in X_1$. □

Note that if Γ is a Cayley graph $Cay(G, X)$, it is obviously true that $g(\Gamma) \leq |x|$ for all $x \in X$. Thus, the second part of Theorem 4.6 is a generalization of this result to all vertex-transitive groups of automorphisms. This together with Corollary 3.2 yields the observation that any vertex-transitive automorphism group of a connected graph Γ of girth g is generated by a set of elements all of which are of order not smaller than g.

The last result of this section involves the special case $t = 1$. Graphs that admit an automorphism group that acts transitively on 1-arcs are sometimes called *arc-transitive* or *symmetric graphs* and constitute an important part of the class of all vertex-transitive graphs. By Theorem 4.6, if $t = 1$ then for any $G \leq \mathrm{Aut}\Gamma$ acting arc-transitively on Γ and the respective set X, the valence $d = N_1(b)$ divides the number $\varepsilon_X(n)$ for all positive integers n. This observation imposes yet additional conditions on the numbers $\varepsilon_X(p)$. In particular, let p be a prime larger than d and suppose that $|\mathcal{W}_\Gamma^b(p)| \not\equiv 0 \pmod{p}$. In this case p does not divide $|Stab_G(b)|$ and, by applying Theorem 4.2, we obtain $\varepsilon_X(p) \equiv |\mathcal{W}_\Gamma^b(p)| \pmod{p}$. In addition, Theorem 4.6 gives us that $\varepsilon_X(p)$ must be a non-zero multiple of d congruent to $|\mathcal{W}_\Gamma^b(p)|$ modulo p. Also, since $p > d$ is odd and X is closed under taking inverses, $\varepsilon_X(p)$ must be even. As $d \cdot |Stab_G(b)| = |X| \geq \varepsilon_X(p)$, the order of the stabilizer $Stab_G(b)$ of b in G must be at least as large as $\varepsilon_X(p)/d$. We summarize these observations in the following corollary.

Corollary 4.7 *Let Γ be a graph of valence d admitting an arc-transitive action of a group G. Then d divides $|Stab_G(b)|$. Moreover, if p is a prime strictly larger than d and N is the smallest even multiple of d congruent, modulo p, to $|\mathcal{W}_\Gamma^b(p)|$, then*

$$|Stab_G(b)| \geq \frac{N}{d}.$$

5 Applications

As we have pointed out in the introduction, our motivation for developing counting tools of the kind presented in this article is to be able to assess certain automorphism properties of graphs without computing their full automorphism groups. Unless the computational complexity of finding the full automorphism group of a highly symmetric graph will prove to be polynomial in the number of vertices of the graph (a result considered to be very unlikely), any "cycle- or walk-counting method" that is polynomial in the number of vertices will result in limited information about the full automorphism group of the graph. Nevertheless, as we demonstrate in the following examples, the methods developed in our paper appear to be quite effective when applied to the more specific questions of whether a graph is Cayley or whether a graph is vertex-transitive.

We present two types of examples. First we consider two very familiar vertex-transitive graphs, the Petersen and Coxeter graph, and illustrate the actual usage of our techniques. Then we apply our methods to an infinite class of graphs and show the potential of our methods for obtaining some more general results.

Example 1. Let us first consider the well-known *Petersen graph* $\mathcal{P}$ and let b be any fixed vertex of $\mathcal{P}$. The relevant numbers of oriented cycles and walks through b are listed in the following table (the data was kindly provided to us by Geoff Exoo).

n	5	6	7	8	9	10
$\lvert\mathcal{C}^b_{\mathcal{P}}(n)\rvert$	12	12	0	24	36	0
$\lvert\mathcal{W}^b_{\mathcal{P}}(n)\rvert$	12	99	168	759	1764	6315

If $\mathcal{P}$ were a Cayley graph, it would have to be a Cayley graph of a group G of order 10 (the size of $\mathcal{P}$) generated by a set X of 3 elements (the valence of $\mathcal{P}$). None of the listed numbers alone indicates the fact that $\mathcal{P}$ is not a Cayley graph. For example, if we take $p = 7$, neither the number of oriented cycles nor the number of walks reveals anything: both numbers $\mathcal{C}^b_{\mathcal{P}}(7)$ and $\mathcal{W}^b_{\mathcal{P}}(7)$ are congruent to $0 \pmod 7$ indicating 0 elements of order 7 in X (as one should expect for a group of order 10). Similarly, both $\mathcal{C}^b_{\mathcal{P}}(9)$ and $\mathcal{W}^b_{\mathcal{P}}(9)$ are congruent to $0 \pmod 3$, and thus the potential generating set X contains no

elements of order 3 either. It takes a combination of two of these numbers to obtain the desired result. First, due to the congruence $|\mathcal{C}^b_{\mathcal{P}}(5)| \equiv 2 \pmod 5$ (or $|\mathcal{W}^b_{\mathcal{P}}(5)| \equiv 2 \pmod 5$), we deduce that X would have to contain two elements of order 5. Since X has to be closed under taking inverses, the third element completing X would have to be an involution. However, the congruence $|\mathcal{C}^b_{\mathcal{P}}(8)| \equiv 0 \pmod 2$ implies that the number of involutions in X would have to be even, and we have to conclude that X cannot be completed as needed, and $\mathcal{P}$ is not a Cayley graph (as it is well-known). □

It is interesting to observe that $|\mathcal{W}^b_{\mathcal{P}}(8)| \equiv 1 \pmod 2$ which is not enough to deduce that $\mathcal{P}$ is not Cayley. This observation seems to suggest the possibility of the existence of a non-Cayley vertex transitive graph where none of the numbers of cycles or walks nor any combination of those would allow one to deduce that the graph is not Cayley. Similarly, there may exist a pair of vertex-transitive graphs with exactly the same cycle- and walk-numbers, out of which one would be Cayley and one would be non-Cayley. On the other hand, if the non-existence of such graphs could be shown, this may potentially imply an algorithm with time complexity polynomial in the size of the graph that would decide whether a vertex-transitive graph is Cayley or not.

Since $\mathcal{P}$ is vertex-transitive but not Cayley, the smallest vertex-transitive automorphism group of $\mathcal{P}$ has to be of size at least 20. It is once again well-known that $\mathcal{P}$ does indeed possess a vertex-transitive automorphism group of this order. In the following example we estimate the size of the smallest *arc-transitive* automorphism group G of $\mathcal{P}$.

Example 2. Let G be the smallest arc-transitive automorphism group of $\mathcal{P}$. Since the number of arcs of $\mathcal{P}$ is equal to 30 and the order of G must be divisible by this number, $|G|$ is at least 30. Using the number of closed walks of length 5 based at b, we shall show that $|G|$ is, in fact, at least 60.

Our table shows that there are 12 closed walks of length 5 at any base point b. Thus, defining X the usual way, we obtain that the number $\varepsilon_X(5) \equiv 2 \pmod 5$. Furthermore, 3, the valence of the Petersen graph, divides $\varepsilon_X(5)$. The smallest (even) integer divisible by 3 and congruent to 2 modulo 5 is 12. Therefore $\varepsilon_X(5) \geq 12$, and consequently $|X| \geq 12$. The order of $Stab_G(b)$ is therefore at least $12/3 = 4$, and since 3 must divide the order of $Stab_G(b)$, we have $|Stab_G(b)| \geq 6$. It follows that the size $|G|$ of the smallest arc-transitive group of the Petersen graph is at least $6 \cdot 10 = 60$. □

Note that the Petersen graph does indeed possess an arc-transitive group of order 60 isomorphic to the alternating group $\mathcal{A}_5$. Although this information cannot be derived from our computations using the number of closed walks of length 5, the lower bound for the size of G was computed using the order of the graph, its valence and the number of closed walks of length 5 exclusively.

In addition, Corollary 4.7 has the following consequence about the set X of elements in $\mathcal{A}_5$ mapping some fixed b to its neighbors. Of the $3 \cdot 6 = 18$ elements of X, exactly 2 or 12 must be of order 5, as $\varepsilon_X(5) \equiv 12 \pmod 5$ and $\varepsilon_X(5)$ is necessarily even. (In fact, using the action of A_5 on $\mathcal{P}$, it may be seen that this number is 12.)

Example 3. Similarly, the vertex stabilizer of any arc-transitive automorphism group G of the *Coxeter graph* must be of size at least 6; the situation is almost identical to the previous example.

Namely, there are precisely 12 closed walks of length 7 at any base point. It follows that $\varepsilon_X(7) \equiv 12 \pmod 7$ and $\varepsilon_X(7)$ is one of the numbers $5, 12, 19, \ldots$ which must be divisible by 2 and 3. Thus, $\varepsilon_X(7) \geq 12$ which yields $|X| \geq 12$ and hence $|Stab_G(b)| \geq 12/3 = 4$. The fact that 3 must divide $|Stab_G(b)|$ gives a lower bound $|Stab_G(b)| \geq 6$. □

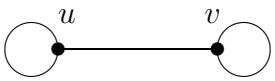
Yet again, Coxeter graph does possess an arc-transitive automorphism group with the corresponding vertex stabilizers of size 6. This means that the obtained lower bound is best possible. One should not, however, expect the bound to be always sharp.

In our last example we will explore the properties of a class of graphs called generalized Petersen graphs. Of the many possible definitions we find it useful to define this class using the language of regular covers and voltage assignments. We begin by recalling some of the basic definitions. The reader interested in a more detailed treatment is advised to consult [4].

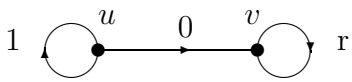
If Γ is an undirected graph, we associate each edge of Γ with a pair of opposite arcs and denote the set of all such arcs by $D(\Gamma)$. A *voltage assignment* on Γ is any mapping α from $D(\Gamma)$ into a group G that satisfies the condition $\alpha(e^{-1}) = (\alpha(e))^{-1}$ for all $e \in D(\Gamma)$ (with e^{-1} being the opposite arc of e and $(\alpha(e))^{-1}$ being the inverse of $\alpha(e)$ in G). The *derived regular cover* of Γ with respect to a voltage assignment α on Γ is a graph denoted by Γ^α. The vertex set $V(\Gamma^\alpha)$ consists of $|V(\Gamma)| \cdot |G|$ vertices $u_g = (u, g)$,

$(u, g) \in V(\Gamma) \times G$. Two vertices u_g and v_f are adjacent in Γ^α if $e = (u, v)$ is an arc of Γ and $f = g \cdot \alpha(e)$ in G.

All generalized Petersen graphs are regular covers of the same graph – the "dumbbell graph" $\mathcal{D}$ which is a graph with two vertices u, v that are joined by an edge and have loops attached to them.



Let $k \geq 3$ be an integer and $1 \leq r \leq k$ be an integer relatively prime to k. The *generalized Petersen graph* $\mathcal{P}(k, r)$ is then the regular cover of the dumbbell graph $\mathcal{D}$ with respect to the voltage assignment $\alpha : D(\mathcal{D}) \longrightarrow \mathcal{Z}_k$ that assigns 0 to the arcs connecting the two vertices of the graph, 1 and -1 to the arcs of the loop at u and r and $-r$ to the arcs of the loop at v.



For example, the "classical" Petersen graph $\mathcal{P}$ is the generalized Petersen graph $\mathcal{P}(5, 2)$.

The main advantage of having the generalized Petersen graphs defined as a regular cover of a relatively small graph stems from the fact that counting cycles and walks in generalized Petersen graphs comes down to counting walks in the dumbbell graph. More precisely, any oriented n-cycle based at a fixed vertex u_g of a generalized Petersen graph $\mathcal{P}(k, r)$ projects onto a (unique) u-based closed n-walk W in $\mathcal{D}$ satisfying the following properties

(i) W is non-reversing; that is, no two consecutive arcs in the walk are opposite to each other (including the first and the last one),

(ii) W has net voltage 0; that is, the sum of the voltages of all the arcs encountered in the walk is 0, and

(iii) W has no proper closed sub-walk of net voltage 0.

Similarly, any closed n-walk through u_g in $\mathcal{P}(k, r)$ projects onto a (unique) u-based closed n-walk in $\mathcal{D}$ of net voltage 0.

Note that for any given fixed n, it is possible to pre-compute *all* u-based closed n-walks in $\mathcal{D}$. We demonstrate this approach and some of its consequences in our last example.

Example 4. Let $n = 5$, and consider the list of all closed walks in $\mathcal{D}$ of length 5 based at the vertex u. It is easy to determine that the total number of such walks in $\mathcal{D}$ is 102. The list of all possible net voltages for these walks is even shorter: $1, -1, 3, -3, 5, -5, r, -r, r-2, r+2, -r+2, -r-2, 2r+1, 2r-1, -2r+1, -2r-1, 3r, -3r$. Since $k \geq 3$ and r is relatively prime to k, some of these numbers can never be congruent to 0 $\pmod{k}$ (for example 1 or r will never be congruent to 0 $\pmod{k}$). Despite the seemingly limited information contained in this list, it still allows us to derive some general results concerning generalized Petersen graphs.

Suppose, for example, that $k > 5$ and $r = 2$. In this case, the only net voltages equal to 0 modulo k are $r-2$ and $-r+2$, each appearing exactly three times. Thus, any generalized Petersen graph $\mathcal{P}(k, 2)$ with $k > 5$ has exactly 6 closed walks of length 5 based at a fixed vertex. As all generalized Petersen graphs are of valence 3, the prime 5 cannot divide the order of the stabilizer of any of its vertices (unless, of course, the graph is not vertex-transitive). By Theorem 4.2 we see that if $\mathcal{P}(k, 2)$ were vertex-transitive, the number of generators in X of order 5 would have to be congruent to 6 modulo 5. By Corollary 4.4, the number 5 must divide the order of the graph (equal to $2k$). We conclude that *no generalized Petersen graph $\mathcal{P}(k, 2)$ with k greater than 5 and relatively prime to 5 is a vertex-transitive graph.* In case when 5 divides k, the number of generators of order 5 in X must be congruent to 1 modulo 5 and even (recall that X is closed under inverses). Hence $|X| \geq 6$, and the stabilizer of the smallest vertex-transitive automorphism group (if there exists one) of $\mathcal{P}(k, 2)$ with k greater than 5 and divisible by 5 must be at least $6/3 = 2$. Consequently, *no $\mathcal{P}(k, 2)$ with $k > 5$ and divisible by 5 is a Cayley graph.*

Using oriented cycles, we can further strengthen the second of the above observations. Of all the closed walks in $\mathcal{D}$ of length 5 based at the vertex u, there are 28 that satisfy the above properties (i),(ii),(iii). If we consider the case $k > 5$ and $r = 2$ again, all the six walks of voltage $r - 2$ and $-r + 2$ we considered in the previous paragraph satisfy these properties. Once again, every generalized Petersen graph $\mathcal{P}(k, 2)$ has exactly 6 oriented cycles of length 5 containing a fixed vertex. If these graphs were Cayley of the form $Cay(G, X)$, X would have to contain exactly 1 element of order 5 (as 1 is the only number smaller than or equal to $|X| = 3$ that is congruent to 6 modulo 5). As X has to be closed under taking inverses, the number of elements of

order 5 in X would also have to be even. This contradiction extends the last statement of the paragraph above and asserts that *no generalized Petersen graph* $\mathcal{P}(k,2)$ *with* $k > 5$ *is a Cayley graph.* □

With respect to the above example, we wish to note that the class of generalized Petersen graphs has been repeatedly classified and it is known that $\mathcal{P}(k,r)$ is a vertex-transitive graph if and only if $r^2 \equiv \pm 1 \pmod{k}$ or $(r,k) = (2,10)$ and is a Cayley graph if and only if $r^2 \equiv 1 \pmod{k}$ [14, 11]. Our results certainly agree with these general facts.

References

[1] A. Clark, "Elements of abstract algebra", Dover Publ., New York, 1984.

[2] E. Dobson, On solvable groups and circulant graphs, Eur. J. Comb. 21, No. 7, 881-885.

[3] D. Fronček, A. Rosa and J. Širáň, The existence of selfcomplementary circulant graphs, *European J. Combin.* (1996), no. 7, 625–628.

[4] J.L.Gross and T.W. Tucker, Topological graph theory, Wiley, New York, 1987.

[5] M.-C. Heydemann, Cayley graphs and interconnection networks, in *Graph Symmetry*, Kluwer Academic Publishers (1997), 167–224.

[6] D.F. Hsu, Introduction to a special issue on interconnection networks, Networks **23** (1993), 211–213.

[7] R. Jajcay and J. Širáň, A construction of vertex-transitive non-Cayley graphs, *Australasian J. Combin.* **10** (1994), 105-114.

[8] R. Jajcay and J. Širáň, More constructions of vertex-transitive non-Cayley graphs based on counting closed walks, Australas. J. Combin. 14 (1996), 121–132.

[9] R. Kurcz, Closed walks in coset graphs and vertex-transitive non-Cayley graphs, Acta Math. Univ. Comenian. 68 (1999), no. 1, 127–135.

[10] P. Lorimer, Vertex-transitive graphs: Symmetric graphs of prime valency, *J. Graph Theory* **8** (1984), 55-68.

[11] M. Lovrečič Saražin, A note on the generalized Petersen graphs that are also Cayley graphs, *J. Combin. Theory Ser.* B **69** (1997), no. 2, 226-229.

[12] D. Marušič and R. Scapellato, Classifying vertex-transitive graphs whose order is a product of two primes, *Combinatorica* **14** (2) (1994), 187-201.

[13] A. A. Miller and C. E. Praeger, Non-Cayley vertex-transitive graphs of order twice the product of two odd primes, *J. Algebr. Comb.* 3, No. 1, (1994), 77-111.

[14] R. Nedela and M. Škoviera, Which generalized Petersen graphs are Cayley graphs?, *J. Graph Theory* **19** (1995), 1-11.

[15] C. E. Praeger and M.-Y. Xu, Vertex primitive graphs of order a product of two distinct primes, *J. Combin. Theory* Ser. B. 59 (1993), no. 2, 245–266.

[16] G. Sabidussi, Vertex-transitive graphs, *Monatsh. Math.* 68 (1964), 426-438.