More constructions of vertex-transitive non-Cayley graphs based on counting closed walks

Robert Jajcay
Department of Mathematics and Computer Science
Indiana State University, Terre Haute, IN 47809, U.S.A.
jajcay@helios.unl.edu

Jozef Širáň
KMaDG, SvF STU
Radlinskeho 11, 816 38 Bratislava
Slovakia
siran@vox.svf.stuba.sk

Abstract

A unifying approach to the problem of constructing vertex-transitive graphs that are not Cayley is presented. The general construction, based on representing vertex-transitive graphs as coset graphs of groups, is flexible enough to allow us to obtain new results as well as to reprove several older results concerning the non-Cayley numbers (orders of vertex-transitive graphs that are not Cayley).

1 Introduction

Although studied for more than a century now, vertex-transitive graphs have quite recently caused a great deal of activity. Their rich groups of automorphisms make them interesting from both the point of view of permutation groups as well as of combinatorics. Among the most recent achievements, we can mention the search for vertex-transitive graphs that are edge- but not arc-transitive in [1], or the discovery of vertex-, edge- but not arc-transitive graphs with primitive automorphism groups in [14].

Our paper focuses on a slightly different problem. Aside from the notoriously known Cayley graphs, not many families of vertex-transitive graphs were known and studied before 1990 (as pointed out, for instance, by Watkins in [15], who also invented the acronym VTNCG for vertex-transitive graphs that are not Cayley). The situation, however, has dramatically changed in the last four years. Initiated originally by the problem posed by Marušič in [9], of determining the so-called non-Cayley numbers, the orders of VTNCG's, the search for VTNCG's has brought a wide range of different constructions ([6], [7], [9], [10], [11], [12], [13], [14], and [15]).

In [7] we described a general method for finding new families of VTNCG's based on a simple combinatorial criterion for Cayley graphs and a representation of vertex-transitive graphs as coset graphs of finite groups. This paper is an extension of the results from [7]: we improve both the combinatorial criterion and the main construction, and find several previously unknown families of VTNCG's. Also, we present constructions of VTNCG's of order close to a product of two or more primes, and, in this way, obtain several results on non-Cayley numbers.

2 Preliminaries

Most of the general results obtained in our paper hold for both finite and infinite graphs. The parts considering finite graphs are mostly related to the problem of non-Cayley numbers (as the nature of the problem is inherently finite), clearly marked and easily recognizable by the reader. We always assume, though, that the graphs considered are locally finite (i.e., every vertex has finite valency), loopless, and without multiple edges.

Let G be a (finite or infinite) group and X be a unit-free symmetric subset of G, that is, $1 \notin X$ and $x^{-1} \in X$ whenever $x \in X$. The *Cayley graph* $\Gamma = C(G, X)$ 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 we do not require the set X to be a generating set for G and therefore we allow also disconnected Cayley graphs. The graph Γ is locally finite if and only if the set X is finite. In all cases, the group G acts regularly (as a subgroup of automorphisms) on the vertex set of $\Gamma = C(G, X)$ by left multiplication, which shows that every Cayley graph is vertex-transitive.

The key concept of our paper, powerful enough to give us all the Cayley and non-Cayley vertex-transitive graphs, is the one of a *coset graph*. Let G be a group, H a subgroup of G and X a symmetric subset of elements of G such that $H \cap X = \emptyset$. The vertex set of the *coset graph* $\mathrm{Cos}(G, H, X)$ is the set of all left cosets of H in G; two vertices (cosets) aH and bH are adjacent in $\mathrm{Cos}(G, H, X)$ if and only if $a^{-1}b \in HXH = \{hxh';\ x \in X \text{ and } h, h' \in H\}$. An alternate way to define the incidence relation on $\mathrm{Cos}(G, H, X)$ is by referring to the *associated Cayley graph* $C(G, X)$: Two cosets aH, bH are adjacent in $\mathrm{Cos}(G, H, X)$ provided that there exist $h, h' \in H$ such that ah and bh' are adjacent vertices in the associated Cayley graph $C(G, X)$. The coset graph $\mathrm{Cos}(G, H, X)$ can therefore be viewed as a graph obtained by "factoring" the associated Cayley graph $C(G, X)$ by the subgroup H. The coset graph $\mathrm{Cos}(G, H, X)$ is connected if and only if the set HXH is a generating set for the group G. Observe that in the special case when $H = \{1\}$, the coset graph reduces to a Cayley graph.

As in the case of Cayley graphs, the group G acts transitively as a group of automorphisms of $\mathrm{Cos}(G, H, X)$ by left multiplication, and therefore every coset graph is vertex-transitive. In fact, coset graphs are equivalent to vertex-transitive graphs in the sense that a graph Γ is vertex-transitive if and only if it is isomorphic to some coset graph. For more information on coset graphs we refer the reader to [8] or [7].

In order to be able to distinguish between the Cayley and non-Cayley graphs obtained by the coset graph construction, we shall use the following criteria formulated in two lemmas. The first lemma is a generalization of a result originally proved in [5]. It focuses on oriented closed walks of length p^n based at a fixed vertex (say, a_0), that is, on ordered sequences $(a_0, a_1, \ldots, a_{p^n} = a_0)$ of (not necessarily distinct) vertices such that a_{i-1} and a_i are adjacent for each i, $1 \leq i \leq p^n$.

Lemma 1 *Let $\Gamma = C(G, X)$ be a locally finite Cayley graph and p be a prime. Then the number of closed oriented walks of length p^n, $n \geq 1$, based at any fixed vertex of Γ, is congruent (mod p) to the number of elements in X for which $x^{p^n} = 1$.*

Proof. Let a be an arbitrary vertex of a Cayley graph $\Gamma = C(G, X)$ and p^n be a positive power of a prime. Let W denote the set of all closed oriented walks of length p^n based at a. Each of these walks can be uniquely associated to an ordered p^n-tuple $(x_1, \ldots, x_{p^n})$ of elements of X representing the succession of colors of arcs in the walk. Since the walks considered are closed, the associated p^n-tuples satisfy the equation

$$x_1 \ldots x_{p^n} = 1. \tag{1}$$

Conversely, each p^n-tuple of elements of X satisfying the equation (1) represents a closed oriented walk based at a, namely the walk $v_0 = a$, $v_1 = a \cdot x_1$, $\ldots$, $v_{p^n} = a \cdot x_1 \ldots x_{p^n} = a$. Let

$$I = \{(x_1, \ldots, x_{p^n}); x_i \in X,\ 1 \leq i \leq p^n,\ x_1 \ldots x_{p^n} = 1\}.$$

It follows that $|W| = |I|$. Now, consider the action of the cyclic shift Φ,

$$\Phi((x_1, \ldots, x_{p^n})) = (x_2, \ldots, x_{p^n}, x_1),$$

on the set I. The equation (1) readily implies the equation $x_2 \ldots x_{p^n} x_1 = 1$, thus Φ preserves I. Since Φ is of order p^n, the lengths of its orbits on I are necessarily non-negative powers of p. That further yields the fact that $|I|$ is congruent (mod p) to the number of orbits of Φ on I of length 1. Each such an orbit consists of a p^n-tuple $(x, \ldots, x)$, $x \in X$ and $x^{p^n} = 1$. That proves that $|I|$ is congruent (mod p) to the number of elements $x \in X$ with the property $x^{p^n} = 1$. Since $|W| = |I|$, this completes the proof of our lemma. □

Indeed, there are several possible generalizations of this lemma. Denote, for instance, by I_k the set of all p^k-tuples $(x_1, \ldots, x_{p^k})$, $x_i \in X$, $1 \leq i \leq p^k$ for which $x_1 \ldots x_{p^k} = 1$. Then, for any $k \geq 2$, the number of closed oriented walks of length p^k, based at any fixed vertex of Γ, is congruent (mod p^k) to the size of the set I_{k-1}. We shall not, however, use any of these stronger versions of Lemma 1 in our paper.

Instead, let us consider the simplest case of a composite length, namely, the number of closed oriented walks of length $n = pq$, the product of two distinct primes. This situation is described in the following lemma.

Lemma 2 *Let $\Gamma = C(G, X)$ be a locally finite Cayley graph, and p and q be two distinct primes. Let $n = pq$ and let j_n be the number of elements $x \in X$ for which $x^n = 1$. Then the number of closed oriented walks of length n, based at any fixed vertex of Γ, is congruent (mod p) to $j_n + kq$, where k is a nonnegative integer.*

Proof. The proof employs ideas similar to those used before in Lemma 1. Again, $|W|$, the size of the set of closed oriented walks of length n based at some vertex a, is equal to $|I|$, the size of the set $\{(x_1, \ldots, x_n); x_i \in X, \prod_{i=1}^{n} x_i = 1\}$. The action of Φ, $\Phi(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1)$, on I has possible orbits of size 1, p, q or pq; let k be the number of orbits of length q. It follows that $|I|$ is congruent (mod p) to kq plus the number of orbits of length 1. Now it is sufficient to realize that the length 1 orbits are constituted by elements $x \in X$ with the property $x^n = 1$. □

Let us notice that the orbits of Φ of length q consist of n-tuples of elements from X of the form $(x_1, \ldots, x_q, x_1, \ldots, x_q, \ldots, x_1, \ldots, x_q)$, such that $(x_1 \cdot \ldots \cdot x_q)^p = 1$. The case when $|G|$ is finite and p *does not* divide $|G|$ is particularly interesting. In this case, G cannot contain elements of order p, and $x^{pq} = 1$ simplifies to $x^q = 1$. On the other hand, $(x_1 \ldots x_q)^p = 1$ can only be satisfied by q-tuples $(x_1, \ldots, x_q)$ that already satisfy the equation $x_1 \cdot \ldots \cdot x_q = 1$. The q-tuples $(x_1, \ldots, x_q)$, $x_1 \cdot \ldots \cdot x_q = 1$ together with the generators x satisfying $x^q = 1$ represent precisely the closed oriented walks of length q, based at a fixed vertex of Γ. We can conclude that, in the special case of p relatively prime to $|G|$, the number of closed oriented walks of length pq, based at a fixed vertex, is congruent (mod p) to the number of closed oriented walks of length q, based at the same vertex.

3 Main theorem

Let us start this section by quoting the key result from [7].

Theorem 1 *Let G be a group, let H be a finite subgroup of G, and let X be a finite symmetric subset of G such that $XHX \cap H = \{1\}$. Further, suppose that there exist at least $|X| + 1$ distinct ordered pairs $(x, h) \in X \times H$ such that $(xh)^p = 1$ for some fixed prime $p > |X||H|^2$. Then the coset graph $\Gamma = \mathrm{Cos}(G, H, X)$ is a vertex-transitive non-Cayley graph.*

A close examination of the proof provided in [7] reveals an immediate improvement of the original lower bound on p. Let l_p denote the number of distinct pairs (x, h) in $X \times H$ such that $(xh)^p = 1$. For obvious reasons, $l_p \leq |X||H|$, and, in general, l_p is often smaller than $|X||H|$. Without any alteration of the proof, the original bound $p > |X||H|^2$ can be replaced by $p > l_p|H|$, giving an improvement on the size of p used in applications. Consider, for instance, the case of the triangle group $(2, r, p)$ (Example 1 of [7]). The original lower bound $p > r^2$ can be improved by using the fact that $(x,1)$ obviously does not satisfy the identity $(x\cdot 1)^p=1$. Thus l_p is not bigger than $r-1$ and therefore it is enough to require $p>r(r-1)$. This lower bound matches the one in [6] obtained by more subtle methods.

For further improvements of the original theorem we will employ the more powerful Lemma 1 together with a simple counting principle. Here is the main theorem of this paper.

Theorem 2 *Let G be a group, let H be a finite subgroup of G, and let X be a finite symmetric unit-free subset of G such that $XHX\cap H=\{1\}$. Let $p_1^{k_1},\ldots,p_r^{k_r}$ be powers of distinct primes, and let $l_{p_i}, 1\le i\le r$, denote the number of distinct pairs (x,h) in $X\times H$ such that $(xh)^{p_i^{k_i}}=1$. Suppose that $\sum_{i=1}^r l_{p_i}>|X|$, and, for all i, $p_i>l_{p_i}|H|$. Then the coset graph $\Gamma=\mathrm{Cos}(G,H,X)$ is a vertex-transitive non-Cayley graph.*

Proof. The fact that X is a finite unit-free symmetric subset of G for which $XHX\cap H=\{1\}$ makes large parts of the original proof in [7] still valid for our case. In particular, for any two adjacent vertices aH, bH of $\Gamma=\mathrm{Cos}(G,H,X)$ there still exists a unique $x\in X$ such that $b\in aHxH$. Also, the valency of Γ is equal to $|H||X|$ as in [7].

In order to prove the theorem in its full strength, we start by proving it in the special case $r=1$ and $p_1^{k_1}=p^k$, with $p>l_p|H|$. Consider the set W of closed oriented walks of length p^k in Γ, based at a fixed vertex a_0H. As stated in [7], each of these walks can be uniquely associated to a (p^k+1)-tuple

$$(b_0;(x_1,h_1),(x_2,h_2),\ldots,(x_{p^k},h_{p^k})), \tag{2}$$

$$\text{where } x_i\in X,\ h_i\in H,\ b_0\in a_0H,\ \prod_{i=1}^{p^k} x_ih_i=1.$$

The (p^k+1)-tuple (2) canonically represents the walk in terms of its colors (for more details we refer the reader to the original proof in [7]). Furthermore, there exists a one-to-one correspondence between the set W and the set of all (p^k+1)-tuples satisfying (2). Denote the set of all such (p^k+1)-tuples by I, i. e.

$$I=\{(b_0;(x_1,h_1),\ldots,(x_{p^k},h_{p^k}));\ b_0\in a_0H,\ x_i\in X,\ h_i\in H,\ \prod_{i=1}^{p^k}x_ih_i=1\}.$$

Then $|W|=|I|$. Now, consider the action of the cyclic shift

$$\Phi:\Phi((b_0;(x_1,h_1),\ldots,(x_{p^k},h_{p^k})))=((b_0;(x_2,h_2),\ldots,(x_{p^k},h_{p^k}),(x_1,h_1)))$$

on I. Since p is a prime, each orbit of Φ on I has length 1 or a positive power of p. In addition, if a (p^k+1)-tuple $(b_0;(x_1,h_1),\ldots,(x_{p^k},h_{p^k}))$ constitutes a length 1 orbit of Φ, then $x_1=\ldots=x_{p^k}=x, h_1=\ldots=h_{p^k}=h$ and $(xh)^{p^k}=1$. If we denote the number of length 1 orbits of Φ on I by n, then $|I|=n \pmod p$, and therefore

$|W| = n \pmod p$. On the other hand, $n = l_p|H|$, the number of pairs (x, h) such that $(xh)^{p^k} = 1$ times the size of H. By the assumption, $l_p > |X|$, and therefore

$$|X||H| < n = l_p|H|. \tag{3}$$

Suppose now that Γ is a Cayley graph $C(G', X')$ for a group G' and generating set X'. Applying Lemma 1, we see that n has to be congruent (mod p) to the number of elements in X' of order divisible by p. This number cannot exceed the valency of Γ which we have determined to be $|X||H|$. Thus, $n > |X||H|$ has to be congruent (mod $p > l_p|H| = n$) to a number smaller than $|X||H|$. That is obviously impossible, and we conclude that Γ is not Cayley.

Let us consider the general case of powers of r distinct primes $p_1^{k_1}, \ldots, p_r^{k_r}$. Suppose, again, that $\Gamma = \mathrm{Cos}(G, H, X)$ is indeed a Cayley graph $C(G', X')$. Let j_i denote the number of generators $x' \in X'$ whose order is divisible by p_i, $1 \le i \le r$. Obviously,

$$j_1 + j_2 + \ldots j_r \le |X'| = |X||H|. \tag{4}$$

(The equality $|X'| = |X||H|$ follows from the fact that $|X'|$ has to be equal to the valency of Γ.)

Now, for each of the p_i's, we repeat the process outlined in the above part of our proof for the special case $r = 1$. Let W_i denote the set of all closed oriented walks of length $p_i^{k_i}$ in Γ based at an arbitrary but fixed vertex a_0H, let I_i be the set of all $(p_i^{k_i}+1)$-tuples $(b_0; (x_1, h_1), \ldots, (x_{p_i^{k_i}}, h_{p_i^{k_i}}))$, $b_0 \in a_0H$, $x_i \in X$, $h_i \in H$, $\prod_{i=1}^{p_i^{k_i}} x_i h_i = 1$, and let n_i be the number of orbits of length 1 of the cyclic shift on I_i. As argued before, $n_i = l_{p_i}|H|$ and $|W_i| = n_i \pmod{p_i}$, for all $1 \le i \le r$. Consider the sum $\sum_{i=1}^r n_i = |H| \sum_{i=1}^r l_{p_i}$. By one of the assumptions of our theorem, $\sum_{i=1}^r l_{p_i} > |X|$, and thus,

$$\sum_{i=1}^r l_{p_i}|H| > |X||H|. \tag{5}$$

The inequalities (4) and (5) together yield the following simple observation: there exists a prime p_s, $s \le r$ for which $l_{p_s}|H| > j_s$. The rest of the proof follows from Lemma 1. The number $|W_s|$ of closed oriented walks of length $p_s^{k_s}$ in Γ is, on one hand, congruent (mod p_s) to the number j_s. On the other hand, it is congruent (mod p_s) to the number $l_{p_s}|H| > j_s$. Since $p_s > l_{p_s}|H|$ by assumption, the latter is impossible. The proof is complete. □

We have stated Theorem 2 in the most general setting with the prime powers being quite arbitrary. For practical applications we would like to make the following remark. Suppose that G is finite and p is an odd prime that *does not* divide the order of G. Then p *does not* divide the size of the vertex set of $\Gamma = \mathrm{Cos}(G, H, X)$ either, and therefore Γ, even if it happens to be Cayley, *cannot* possibly have generators of order p. On the other hand, since G contains no elements of order p, the number of pairs (x, h) in $X \times H$, satisfying the equality $(xh)^p = 1$, is zero as well. Thus, p contributes 0 to both sides of our inequality and therefore carries no information of whether the obtained graph is Cayley or not. Consequently, to construct finite VTNCG's, we are only interested in prime powers that divide the order of G. (Obviously, there are no limits on their choice for infinite G's.)

Although Theorem 2 handles as its special case the prime power p^k, its main strength (as opposed to the original Theorem 1) lies in its applicability to composite numbers. The possibility of considering the elements of X with respect to different primes adds a lot of freedom to the original construction from [7]. The following applications illustrate well the advantages of Theorem 2 over Theorem 1.

4 Applications

Construction 1. Let $p > q$ be two odd primes such that $2(p-q)(p-q+1) < q$. Take $y = (1\ 2 \dots p-q+1)$ and $x = (p-q+1 \dots p)$, two permutations of the set $\{1, 2, \dots, p\}$, and consider the permutation group $G = <x, y>$, generated by x and y. Let $H = <y>$ and $X = \{x, x^{-1}\}$. Obviously, $XHX \cap H = \{1\}$. Furthermore, $l_q \geq 2$, since x and x^{-1} are both of order q, and $l_p \geq 2$, since $(xy)^p = (x^{-1}y)^p = 1$. Thus, $l_q + l_p \geq 4 > 2 = |X|$. Also, $p > q > 2(p-q)(p-q+1)$, where $2(p-q)(p-q+1)$ is an upper bound for both $l_q|H|$ and $l_p|H|$. Theorem 2 implies that $\mathrm{Cos}(G, H, X)$ is a vertex-transitive non-Cayley graph. □

Construction 1 is very generic and can be altered in multiple ways. The set X can be, for instance, extended by any of the powers of x together with their inverses. The lower bound on q, however, has to be adjusted to $|X|(p-q)(p-q+1)$. Another extension of X can be made by adding any number of cyclic permutations of a prime length intersecting $\{1, 2, \dots, p\}$ at at most one point. Similarly, the subgroup $H = <y>$ can be replaced by just about any permutation group H' acting on $\{1, 2, \dots, p-q+1\}$, with a minor restriction that each of the elements of H', different from the identity, has to move the point $p-q+1$.

One of the basic questions related to VTNCG's is the problem of characterizing the positive integers n, for which there exists a VTNCG of order n, the so-called *non-Cayley numbers* ([9]). Since any of the multiples of a non-Cayley number is also non-Cayley, most of the work in the area is devoted to products of small powers of prime factors ([10], [11], [12], [14]). Although Construction 1 is easy to use and yields a large number of possible alterations, and, eventually, of new VTNCG's, the orders of the graphs obtained are usually close to factorials. Also, it is hard to control the orders of the graphs obtained. This makes this construction relatively unsuitable for finding non-Cayley numbers.

The following constructions do not suffer from this drawback. The applications included focus on the particular unresolved case $n = 2p_1p_2 \dots p_k$, $k \geq 2$ where $p_1, \dots, p_k$ are distinct primes, $p_i \equiv 3 \pmod 4$, $1 \leq i \leq k$ ([12]).

Construction 2. This is a generalization of the triangle group $(2, r, p)$ construction from [6]. Let $G = <x, y>$ be a two-generator group satisfying the identities $y^l = x^m = (xy)^n = 1$, and take $H = <y>$ and $X = \{x, x^{-1}\}$. Suppose further that both m and n are prime powers, $m = p_1^{j_1}$, $n = p_2^{j_2}$, and consider the coset graph

$\Gamma = \mathrm{Cos}(G, H, X)$. If l_{p_1}, l_{p_2} denote the number of products $xh \in XH$ of orders being powers of p_1, p_2, respectively, then obviously $l_{p_1} + l_{p_2} \geq |X| + 1 > |X|$. (Notice that, in fact, the set X can be extended by any number of nontrivial powers of x together with their inverses and the inequality will still hold true.) Theorem 2 asserts under these conditions that Γ is a VTNCG provided the folowing three conditions are satisfied:

$$p_1 > l_{p_1} \cdot |H| = l_{p_1} \cdot l,\ p_2 > l_{p_2} \cdot |H| = l_{p_2} \cdot l, \tag{6}$$

$$XHX \cap H = <1>. \tag{7}$$

Despite the relatively strict conditions on G and (l, m, n), there is an abundance of examples of such a situation in the theory of regular hypermaps (see e.g. [4]).

Example 1. All computations included in this example as well as in the following examples have been based on the primitive representations listed in [3] using the software package GAP.

Let G be the projective special linear group $PSL_2(23)$ represented on 24 points. Then G is a $(4, 11, 23)$ group : $G = <x, y>$, $x^{11} = y^4 = (xy)^{23} = 1$, where

$$\mathrm{x} = (1,18,12,9,8,11,16,20,2,5,4)(3,17,15,7,13,24,23,6,21,19,10),$$

and

$$\mathrm{y} = (1,11,3,20)(2,17,4,8)(5,23,16,12)(6,14,22,24)(7,13,10,9)(15,21,19,18).$$

Take $H = <y>$ and $X = \{x, x^{-1}\}$. The number l_{11} of products in XH of order 11 is 2, as well as l_{23}, the number of products of order 23. Further, $XHX \cap H = <1>$, and since $|H| = 4$, the conditions in (6) are readily satisfied. The resulting vertex-transitive graph $\mathrm{Cos}(G, H, X)$ is therefore non-Cayley. Its order $|G|/|H|$ is $11 \cdot 23 \cdot 24/4 = 2 \cdot 3 \cdot 11 \cdot 23 = \mathbf{1518}$, a new non-Cayley number. □

Example 2. Now, consider the primitive action of $G = PSL_2(43)$ on 44 points. Then G is a $(3, 7, 11)$ group: $G = <x, y>$, $x^7 = y^3 = (xy)^{11} = 1$. Taking $H = <y>$ and $X = \{x, x^{-1}\}$, the numbers l_7 and l_{11} are both equal to 2, and $XHX \cap H = <1>$ again. The VTNCG obtained is of order $44 \cdot 43 \cdot 21/3 = 2^2 \cdot 7 \cdot 11 \cdot 43$. □

Because of its squared factor 2^2, the non-Cayley number obtained in Example 2 has been previously known. One way to obtain a previously unknown non-Cayley number would be to consider an element of order 2 instead of 3 for the element y. Although this actually works and the obtained non-Cayley number $2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$ is really new, it seems to be more efficient to "shoot" for $2 \cdot 7 \cdot 11 \cdot 43$ right away and to get $2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$ as a consequence. In order to do that we need to factorize G by a *subgroup* of order 6 (there are no *elements* of order 6 in $PSL_2(43)$). However, the number 6 is not only too big for using 7 as one of the primes considered, it is also too big for using the number 11 (since l_{11} has to be at least 2, we get the inequality $11 < l_{11} \cdot |H| = l_{11} \cdot 6$; unsuitable for the use of Theorem 2). That leaves us with 43 alone. The main obstacle in using Theorem 2 for this situation is the fact that we need to use a set X with *at least* $|X| + 1$ pairs $(x, h) \in X \times H$ satisfying $(xh)^p = 1$, for some (quite restricted) prime p. That forces an existence of *at least* one pair (x,h), $(xh)^p = 1$, with $h \neq 1$. If it were not for this condition, we could simply use sets X consisting of prime power elements and the pairs $(x,1)$ would provide us with a sufficient number of prime-power pairs. The necessity for existence of at least $|X|+1$ pairs in Theorem 2 comes from the fact that, for a general Cayley graph $C(G,X)$, we are unable to make any statements about the number of generators $x \in X$, whose order is a power of p. However, for special cases of orders of Cayley graphs (in particular for the relatively simple cases of "interesting" candidates for non-Cayley numbers), we are able to limit the number of generators of certain prime orders. Consider, for instance, the order $2p_1p_2\ldots p_k$, where $2 < p_1 < p_2 < \ldots p_k$ are distinct primes. Let G be a group of this order. In the case when none of the divisors of $2p_1\ldots p_{k-1}$ different from 1 is congruent to 1 (mod p_k), the Sylow theorem yields that the Sylow p_k-subgroup of G is necessarily normal in G. That further yields that G cannot be generated by elements of order p_k only. Thus, no *connected* Cayley graph $C(G,X)$ of order $2p_1p_2\ldots p_k$ satisfying the above mentioned condition can be generated by $|X|$ elements of order p_k.

Such a situation allows the following refinement of the lower bound on the number of products of prime power order used in Theorem 2.

Theorem 3 *Let p be a prime and let n be a positive integer such that no finite group of order n can be generated by a set of elements the orders of all of which are powers of p. Let $\Gamma = \mathrm{Cos}(G,H,X)$ be a coset graph of order n $(= |G|/|H|)$, which satisfies the following conditions:*

(i) $XHX \cap H = \{1\}$ and $<HXH> = G$,

(ii) the number l_p, of pairs $(x,h) \in X \times H$ for which $(xh)^{p^k} = 1$, is greater than or equal to $|X|$,

(iii) $p > l_p|H|$.

Then Γ is a vertex-transitive non-Cayley graph.

Proof. Because of the second part of condition (i), Γ is connected. Compared to Theorem 2, all we need to prove is that the new bound $l_p \geq |X|$ is sufficient for granting Γ to to be non-Cayley. Suppose again the opposite, $\Gamma = C(G',X')$, and consider the number of closed oriented walks of length p, based at a fixed vertex. This number has to be congruent (mod p) to both j_p, the number of elements $x \in X'$ whose order is a power of p, and the number $l_p|H|$. Since G' cannot be generated by elements of order p^k alone, j_p is strictly less than the valency of Γ, i. e. $j_p < |X||H|$. On the other hand, $l_p|H| \geq |X||H|$, by assumption. This congruence is impossible, since $p > l_p|H|$, and we conclude that Γ is not Cayley. □

No matter how restrictive the conditions imposed on n look, there are numerous examples of this kind of a situation. Let us at least mention the order $2p_1p_2$ considered by Miller and Praeger in [12]. As proved in Theorem 1 of their paper, the number $2p_1p_2$ is non-Cayley whenever p_1 and p_2 are odd primes and p_2 divides $p_1 - 1$.

This is indeed a case when no group of order $2p_1p_2$ can be generated by elements of order p_1 only. Their original (rather sophisticated) proof can therefore be replaced by a simple assertion that the group used in their construction certainly satisfies all the conditions of Theorem 3. (However, without the knowledge of the suitable group none of this would be possible.)

Another nice example of the use of Theorem 3 is the case $2 \cdot 7 \cdot 11 \cdot 43$ mentioned above:

Example 3. Let $G = PSL_2(43)$ in its action on 44 points, and take $H = \langle y, z \rangle$ to be the 6-element subgroup of G generated by the permutations

$$y = (3,6,22)(4,29,15)(5,39,13)(7,41,33)(8,38,23)(9,20,21)(10,19,14)$$
$$(11,30,34)(12,16,35)(17,42,31)(18,44,28)(24,40,43)(25,26,37)(27,36,32),$$
$$z = (1,2)(3,17)(4,27)(5,18)(6,31)(7,34)(8,21)(9,23)(10,12)(11,33)(13,44)$$
$$(14,16)(15,36)(19,35)(20,38)(22,42)(24,25)(26,43)(28,39)(29,32)(30,41)(37,40),$$

and $X = \{x, x^{-1}\}$ with

$$x = (2,3,44,42,43,29,22,35,15,13,33,39,18,36,8,24,7,41,17,11,20,19,31,$$
$$5,40,14,26,25,34,28,4,38,21,37,9,27,6,12,32,30,10,23,16).$$

All we need to consider here is the number l_{43} equal to 2. Since $43 > 2 \cdot 6$ and $XHX \cap H = \langle 1 \rangle$, the conditions (i), (ii), (iii) of Theorem 3 are satisfied. Furthermore, the Sylow theorem ensures that no group of order $|G|/|H| = 21 \cdot 43 \cdot 44/6 = 2 \cdot 7 \cdot 11 \cdot 43$ can be generated by elements of order 43 only, and $2 \cdot 7 \cdot 11 \cdot 43 = \mathbf{6622}$ is therefore a new non-Cayley number. A similar construction using a subgroup $|H|$ of order 14 yields another new non-Cayley number: $2 \cdot 3 \cdot 11 \cdot 43 = \mathbf{2838}$. (All our attempts to construct an order $2 \cdot 3 \cdot 7 \cdot 11$ VTNCG have failed because of too many elements of order 43 in $X \cdot H$.) □

While all the previous examples yield finite number of non-Cayley numbers, infinite families of new non-Cayley numbers are certainly of the highest interest. One such an infinite family is provided by the following construction.

Construction 3. Let $p \geq 11$ be a prime and let G be the projective special linear group $PSL_2(p)$ of order $p(p^2-1)/2$. Suppose further that none of the divisors of $(p^2-1)/4$ different from 1 is congruent to 1 (mod p) and consider the matrices

$$y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Both y and x are elements of G, the first one of order 2 and the second of order p. Let $H = \langle y \rangle$ and $X = \{x, x^{-1}\}$. Then $G = \langle HXH \rangle$, $XHX \cap H = \langle 1 \rangle$, and $2 \leq l_p \leq 4$, since both $x \cdot 1$ and $x^{-1} \cdot 1$ are of order p and there are at most 4 elements in $X \cdot H$. Thus, $l_p \geq |X| = 2$, and since p has been taken to be greater than or equal to 11, also $p > l_p|H| = l_p \cdot 2$. All the requirements of Theorem 3 are therefore satisfied, and we conclude that the coset graph $\mathrm{Cos}(G, H, X)$ is vertex-transitive and non-Cayley of order $p(p^2 - 1)/4$.

Here is a list of the first few non-Cayley numbers obtained from the above described construction. The dash denotes the primes that do not yield a non-Cayley number; bold-face denotes the previously unknown non-Cayley numbers.

p	11	13	17	19	23	29	31	37	41	43	47	53
order	330	–	–	1710	3036	–	7440	–	–	**19886**	25944	–

The next new non-Cayley number obtained in this manner is the number **5666226**. □

We conclude our paper with a general construction that seems to be especially well suited for applying Theorem 3.

Construction 4. Order $(pq)^n$
Let $p > q$ be two primes and $1 < n < p/2$ be a positive integer. Suppose that p *does not* divide any of the numbers $q^i - 1$, $1 \leq i \leq n$. Then any group of order $(pq)^n$ contains a normal Sylow p-group and *cannot* be generated by elements of order p^k alone. Once more, this conclusion allows us to construct a coset graph satisfying the conditions of Theorem 3. Let G be the *wreath product* of the group $\mathcal{Z}_p \times \mathcal{Z}_q$ with $\mathcal{Z}_n$ acting on $\{1, 2, \ldots, n\}$ in the usual cyclic way. Then $|G| = n(pq)^n$. Let $H = <((0,0), \ldots, (0,0); (12 \ldots n))>$ be the isomorphic copy of $\mathcal{Z}_n$ in G. Let $X = \{((1,0), (0,0), (0,0), \ldots, (0,0); id), ((p-1,0), (0,0), (0,0), \ldots, (0,0); id)\}$. Then $XHX \cap H = \{((0,0), \ldots, (0,0); id)\}$, HXH generates G, $l_p = 2$, and $p > l_p|H| = 2n$, by assumption. All this together proves that $\mathrm{Cos}(G, H, X)$ is a VTNCG of order $(pq)^n$. □

Note also that the wreath product construction introduced here can be extended to constructions of VTNCG's of any order m^n, $n \geq 2$, for which one can somehow prove that no group of order m^n can be generated exclusively by elements of prime-power order p^k, for some prime factor p of m.

References

[1] B. Alspach, D. Marušič and L. Nowitz, Constructing graphs that are 1/2 transitive, *J. Austral. Math. Soc.* (series A) **56** (1994), 391-402.

[2] B. Alspach and T.D.Parsons, A construction for vertex-transitive graphs, *Can. J. Math.* **34** (1982), 307-318.

[3] L.G.Chouinard II., R. Jajcay and S.S. Magliveras, Finite groups, *in Handbook of Combinatorial Design* (C. Colbourn and J. Dinitz, eds.), in preparation.

[4] R. Cori and A. Machi, Maps, hypermaps and their automorphisms: A survey I, II, III, *Expositiones Math.* **10** (1992), 403-427, 429-447, 449-467.

[5] D. Frונček, A. Rosa and J. Širáň, The existence of selfcomplementary circulant graphs, *European J. Combin.* (in press).

[6] P. Gvozdjak and J. Širáň, A topological construction of arc-transitive non-Cayley graphs, *Acta Math. Univ. Comenianae* **LXIII** (1994), 309-313.

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

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

[9] D. Marušič, Cayley properties of vertex-symmetric graphs, *Ars Combinatoria* **16B** (1983), 297-302.

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

[11] B. D. McKay and Ch. E. Praeger, Vertex-transitive graphs which are not Cayley graphs, I and II, *Preprints* (submitted).

[12] A. A. Miller and C. E. Praeger, Non-Cayley vertex-transitive graphs of order twice the product of two odd primes, Research Report at The University of Western Australia.

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

[14] C. E. Praeger and M.-Y. Xu, Vertex primitive graphs of order a product of two distinct primes, *J. Combin. Theory* Ser. B. (in press).

[15] M. E. Watkins, Vertex-transitive graphs that are not Cayley graphs, *in: Cycles and Rays* (G. Hahn et al. (eds.), Kluwer, Netherlands, 1990), 243-256.

(Received 1/9/95)