

# Open Research Online

---

The Open University's repository of research publications and other research outputs

## Small vertex-transitive graphs of given degree and girth

### Journal Item

How to cite:

Jajcay, Robert and Širáň, Jozef (2011). Small vertex-transitive graphs of given degree and girth. *Ars Mathematica Contemporanea*, 4(2) pp. 375–384.

For guidance on citations see [FAQs](#).

© 2011 DMFA Slovenije

Version: Version of Record

Link(s) to article on publisher's website:

<http://amc-journal.eu/index.php/amc/article/view/124/146>

---

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online's data [policy](#) on reuse of materials please consult the policies page.

---

[oro.open.ac.uk](http://oro.open.ac.uk)

# Small vertex-transitive graphs of given degree and girth

Robert Jajcay \*

*Department of Mathematics and Computer Science  
Indiana State University, Terre Haute, IN 47809, USA*

Jozef Širáň †

*Department of Mathematics, SvF, Slovak University of Technology  
Radlinského 11, 813 68 Bratislava, Slovakia*

Received 6 November 2009, accepted 4 August 2011, published online 28 October 2011

---

## Abstract

We investigate the basic interplay between the small  $k$ -valent vertex-transitive graphs of girth  $g$  and the  $(k, g)$ -cages, the smallest  $k$ -valent graphs of girth  $g$ . We prove the existence of  $k$ -valent Cayley graphs of girth  $g$  for every pair of parameters  $k \geq 2$  and  $g \geq 3$ , improve the lower bounds on the order of the smallest  $(k, g)$  vertex-transitive graphs for certain families with prime power girth, and generalize the construction of Bray, Parker and Rowley that has yielded several of the smallest known  $(k, g)$ -graphs.

*Keywords:* Vertex-transitive graph, cage, degree, girth.

*Math. Subj. Class.:* 05C35

---

## 1 Introduction

We use the term  $(k, g)$ -graph to denote a (finite, simple)  $k$ -regular graph of girth  $g$ . A  $(k, g)$ -cage is a smallest  $k$ -regular graph of girth  $g$ ; its order is denoted by  $n(k, g)$ . The existence of a  $(k, g)$ -graph for any degree/girth pair  $(k, g)$  with  $k \geq 2$  and  $g \geq 3$  has been known since the 1960's [12], but the orders  $n(k, g)$  have been determined only for a very limited set of admissible pairs [6].

The main motivation for our paper is based on the observation that a large part of the currently known smallest  $(k, g)$ -graphs are vertex-transitive (often Cayley) graphs, that is,

---

\*Supported in part by the project APVV-0111-07.

†Supported by the projects APVV-0104-07, APVV-0223-10, and VEGA-1/0781/11.

*E-mail addresses:* [rjajcay@isugw.indstate.edu](mailto:rjajcay@isugw.indstate.edu) (Robert Jajcay), [siran@math.sk](mailto:siran@math.sk) (Jozef Širáň)

graphs possessing automorphism groups acting transitively on their vertex sets. This is due to a variety of reasons, the main probably being the fact that the girth of a vertex-transitive graph is easy to determine, since every vertex of a vertex-transitive graph lies on at least one girth cycle. The connection between the apparent “local symmetricity” of the known cages and the size of their automorphism groups is not well understood and there are no general theorems guaranteeing a high symmetry level for cages.

Based on the obvious usefulness of vertex-transitive graphs in small  $(k, g)$ -graph constructions, we set to investigate the general properties of the smallest vertex-transitive graphs of given degree and girth. Throughout, we adopt the notation  $VTC(k, g)$  and  $CC(k, g)$  to denote the order of a smallest vertex-transitive and Cayley graph of degree  $k$  and girth  $g$ , respectively.

Our paper consists of three parts. In the first part, we establish the existence of a Cayley graph for any pair  $(k, g)$ ,  $k \geq 2$ ,  $g \geq 3$ . Somewhat surprisingly, this result has not been previously proved, and no general explicit constructions are known. The results of Nedela and Škoviera include constructions of  $(k, g)$  vertex-transitive graphs, for all  $k \geq 2$ ,  $g \geq 3$ , using voltage graphs and lifts [9], and similar results can be deduced from the paper of Mačaj, Širáň and Ipolyiová [8], but none of these constructions can be easily adopted to construct Cayley graphs exclusively. Biggs in [2, 3] has shown the existence of Cayley graphs of degree  $k$  and girth *at least*  $g$ , for all  $g \geq 3$ .

In the second part of our paper we present some improvements on the well-known Moore bounds ([6]) for the case of vertex-transitive graphs by finding analogous lower bounds for  $VTC(k, g)$  where  $g$  is an odd prime power.

The third part is devoted to a generalization of a construction of Bray, Parker and Rowley [4] who currently hold a number of records in the case of  $k = 3$  ([6]). We show that their construction can be generalized to  $k > 3$  as well, and apply the methods developed in the first part of our paper to construct infinite families of vertex-transitive graphs of odd degree and sufficiently large girth.

## 2 The existence of Cayley graphs for given $(k, g)$

A graph  $G$  is called *vertex-transitive* if for any ordered pair  $(u, v)$  of vertices of  $G$  there exists an automorphism  $\phi$  of  $G$  such that  $\phi(u) = v$ . This definition implies that a vertex-transitive graph is locally the same around every vertex, and all its vertices lie on cycles of the same lengths. Hence if there are no short cycles in the vicinity of (any) one of the vertices, then there are no short cycles in the graph at all.

A vertex-transitive connected graph  $G$  is called *Cayley* if it has a group  $\Gamma$  of automorphisms such that  $\Gamma$  acts regularly on  $V(G)$ , which means that for all  $u, v \in V(G)$  there exists *exactly one* automorphism  $\varphi \in \Gamma$  such that  $\varphi(u) = v$ . An equivalent (and more customary) definition is as follows. Let  $\Gamma$  be a finite group, and let  $X = \{x_1, x_2, \dots, x_k\}$  be a generating set for  $\Gamma$  with the properties that  $X = X^{-1}$  and  $1_\Gamma \notin X$ . Then the *Cayley graph*  $C(\Gamma, X)$  has vertex set  $\Gamma$  and edges from each vertex  $g$  to the vertices  $gx_i$  for  $1 \leq i \leq k$ .

As mentioned before, there is no general proof of the existence of  $(k, g)$  Cayley graphs available in the literature. The results of Biggs [2, 3] come closest by proving the existence of  $k$ -regular Cayley graphs of girth *at least*  $g$  for any  $g \geq 3$ . Interestingly, the 1988 paper [2] takes advantage of the residual finiteness of the considered groups in a way somewhat similar to our use of residual finiteness in this paper. At that time, however, Biggs lacked

an essential ingredient used in our paper, namely, a family of Cayley maps constructed in 2007 by Šiagiová and Watkins [13]. Biggs' results have been also later proved in [6] using the ideas from [3] without the use of the concept of residual finiteness.

**Theorem 2.1** ([2]). Given any  $k, g \geq 3$ , there is  $k$ -regular Cayley graph  $G$  whose girth is at least  $g$ .

The Cayley graphs constructed to prove the above theorem in [3, 6] are based on permutation groups generated by involutions. Based on experimenting with explicit constructions of these groups, it appears that these groups are either the full symmetric groups  $\mathcal{S}_n$  (in the case when at least one of the involutions is odd) or the alternating groups  $\mathcal{A}_n$ , and their girths are strictly larger than  $g$ . The order of the obtained  $(k, g)$ -graphs is enormous; roughly exponential in the Moore bound for  $(k, g)$ .

Our construction of Cayley graphs of given degree  $k$  and *exact* girth  $g$  relies on a series of infinite Cayley maps constructed by Šiagiová and Watkins in [13]. In order to be able to use their construction, we need to introduce some further notation.

An *orientable map* is a 2-cell embedding of a graph in an orientable surface (that is, an embedding having the property that after removing the vertices and edges, one is left with faces homeomorphic to a 2-dimensional open disc). A *Cayley map*  $CM(\Gamma, X, p)$  is an orientable embedding of the Cayley graph  $C(\Gamma, X)$  satisfying the property that the local orientation of the arcs emanating from any vertex of the map induced by reading the names of the arcs counter-clockwise is the same and equal to the cyclic permutation  $p$  of  $X$ . While the most important feature of Cayley maps is the fact that each left multiplication by an element of  $\Gamma$  induces a different map automorphism, that is,  $\Gamma_L \leq \text{Aut}(\mathcal{M})$ , for all Cayley maps  $\mathcal{M} = CM(\Gamma, X, p)$ , we will simply take advantage of the fact that the underlying graph of a Cayley map is a Cayley graph.

Recall that the *covalence sequence* of a vertex  $v$  of an orientable map is the (cyclic) sequence of lengths of the faces incident to  $v$  (taken again in the counter-clock-wise order induced by the orientation of the map). Since the action of the orientation preserving automorphism group of a Cayley map is necessarily vertex-transitive, all the vertices of a Cayley map possess the same covalence sequence. The result we will need gives sufficient conditions for realizable covalence sequences of Cayley maps. If the cyclic sequence  $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_k)$  satisfies  $\sigma = \sigma^{-1}$ , we say that  $\sigma$  is *reversible*. If  $k$  is even, the terms  $\sigma_i$  and  $\sigma_{i+k/2}$  are said to be in *opposite positions*.

**Theorem 2.2** ([13]). Let  $\sigma$  be a cyclic sequence of length  $k \geq 3$ . If  $\sigma$  is reversible and contains either at most one odd term or exactly two odd terms and they are in opposite positions, then  $\sigma$  is a covalence sequence of a Cayley map.

The significance of the above result lies in the fact that in the case of vertex-transitive maps, their covalence sequences contain all the lengths of their faces. Thus, as the underlying graph of a Cayley map is automatically a Cayley graph, the above theorem gives rise to the following strategy for constructing Cayley graphs of given degree and girth.

Given an admissible pair  $(k, g)$ , assume first that  $g$  is even. Then the covalence sequence  $(g, g, \dots, g)$  of length  $k$  is a covalence sequence for at least one Cayley map  $\mathcal{M}(k, g)$ . All the faces of this map are of length  $g$ , and the underlying Cayley graph  $\mathcal{C}(k, g)$  has valence  $k$ .

Similarly, in case when  $g$  is odd, one just needs to construct a suitable realizable covalence sequence whose smallest entry is equal to  $g$ . This can be achieved by considering the

sequences  $(a, \dots, a, g, a, \dots, a)$  for  $k$  odd and  $g$  in the central position and the sequence  $(a, \dots, a, g, g, a, \dots, a)$  for  $k$  even and the two  $g$ 's in central opposing positions (in either case we assume that  $a$  is an even integer larger than  $g$ ). The underlying Cayley graphs of both corresponding Cayley maps  $\mathcal{M}(k, g)$  are again  $k$ -valent Cayley graphs.

Even though all the faces of the maps constructed above are of length at least  $g$ , it is not immediately obvious that the *girth* of these maps is necessarily at least  $g$ . Except for the cases  $(k, g) = (3, 4)$  and  $(k, g) = (3, 5)$ , this follows from the following lemma.

**Lemma 2.3.** Let  $G$  be a finite plane graph such that its outer face is bounded by a cycle  $C$ . Assume that all inner faces of  $G$  have length at least  $g$  for some  $g \geq 3$ , and all vertices of  $G$  not contained in  $C$  have the same degree  $k \geq 3$ . If  $(k, g) \neq (3, 4), (3, 5)$ , then  $C$  has length at least  $g$ .

*Proof.* We may obviously assume  $g \geq 4$ . Let  $e$  be the number of edges in  $G$ ,  $\ell$  be the length of  $C$  and  $r$  be the number of vertices of  $G$  not in  $C$ . Further, let  $s$  be the number of inner faces of  $G$  and let  $t$  be the average length of the inner faces; clearly  $t \geq g$  and  $2e = \ell + st$ . Solving for  $s$  and substituting into Euler's formula  $(\ell + r) - e + s = 1$  leads, after rearrangement of terms, to  $\ell(t - 1) = (1 - r)t + e(t - 2)$ . Comparing  $2e$  with the sum of all vertex degrees in  $G$  yields  $2e \geq 2\ell + kr$ , and combining this with the previous equality and rearranging terms finally gives  $\ell \geq t + krt(1/2 - 1/k - 1/t)$ . If  $g \geq 4$  and  $(k, g) \neq (3, 4), (3, 5)$ , then  $1/k + 1/t \leq 1/2$  and hence  $\ell \geq g$ .  $\square$

Since, due to results obtained in [10], Theorem 8.1, the maps constructed by Štiagiová and Watkins are all embedded in the plane and satisfy the property that every finite cycle of the underlying graph divides the plane into two regions one of which contains only a finite number of the vertices of the graph, the above lemma determines that except for the cases  $(3, 4)$  and  $(3, 5)$ , the girth of the graphs underlying the Cayley maps  $\mathcal{M}(k, g)$  considered above is equal to  $g$ .

We need to stress however that the maps constructed in [13] are but for a very few exceptions infinite. Thus, for the remaining part of this section, we need to devise a strategy to make the maps  $\mathcal{M}(k, g)$  finite without disturbing the fact that they are Cayley of valence  $k$  and girth  $g$ .

The maps constructed in [13] are Cayley maps for a relatively simple class of groups given by their presentations. Namely, each entry  $\sigma_i$  of the realizable covalence sequence  $\sigma$  is associated with a specific word  $w_i$  in  $x_1, x_2, \dots, x_k$  of length  $\sigma_i$ , and the Cayley group of  $\mathcal{M}(k, g)$  is the group

$$\mathcal{G}(k, g) = \langle x_1, x_2, \dots, x_k \mid w_i = 1, \text{ for all } 1 \leq i \leq k \rangle.$$

Even though the majority of these groups are infinite, all of them belong to the class of residually finite groups (see, for example, [10], Theorem 8.1). A group  $\Gamma$  is said to be *residually finite* if, given any finite set of non-identity elements  $g_1, \dots, g_n$ , there is a homomorphism from  $\Gamma$  to a finite group which takes none of  $g_1, \dots, g_n$  to the identity. Equivalently,  $\Gamma$  is residually finite if any finite set  $g_1, \dots, g_n$  of elements of  $\Gamma$  admits for the existence of a normal subgroup of finite index which contains none of the elements on the list. The residual finiteness of the groups  $\mathcal{G}(k, g)$  enables us to construct finite Cayley graphs of given girth and degree.

**Theorem 2.4.** For every pair of parameters  $k \geq 2, g \geq 3$ , there exists a finite Cayley graph  $C(\Gamma, X)$  of valence  $k$  and girth  $g$ .

*Proof.* To resolve the two cases not covered by Lemma 2.3, note that the complete bipartite graph  $K_{3,3}$ , the  $(3, 4)$ -cage, is a Cayley graph of the dihedral group  $\mathcal{D}_3$  generated by the three reflections. As for the  $(3, 5)$ -case, we note that the buckyball of degree 3 on 60 vertices is a cubic graph of girth 5; it is also a Cayley graph of the alternating group  $\mathcal{A}_5$  with the generating set  $\{(1, 2, 3, 4, 5), (1, 5, 4, 3, 2), (1, 2)(3, 4)\}$ .

For all the remaining cases, let  $\mathcal{C}(k, g) = C(\mathcal{G}(k, g), X)$  be the (possibly infinite) Cayley graph of degree  $k$  and girth  $g$  that is the base graph of the Cayley map  $\mathcal{M}(k, g)$ . Let  $S$  be the set of group elements of  $\mathcal{G}(k, g)$  corresponding to the vertices of  $C(\mathcal{G}(k, g), X)$  whose distance from the vertex labeled by the identity is at most the length of largest face of the corresponding map (recall that the maps are assumed to have at most two face lengths). Then  $S$  is a finite set of elements in a residually finite group, and there exists a finite index normal subgroup  $N_S$  of  $\mathcal{G}(k, g)$  that has an empty intersection with  $S$ . Consider now the factor group  $\mathcal{G}(k, g)/N_S$ , and its set of generators  $X/N_S = \{x_1N_S, x_2N_S, \dots, x_kN_S\}$ . In terms of the presentation of this factor group,  $X/N_S$  consists of  $k$  distinct elements (recall that  $X \subset S$ ) and all of its relators are either of the same length as the original relators of  $\mathcal{G}(k, g)$  or longer. It follows that  $C(\mathcal{C}(k, g)N_S, X/N_S)$  is a finite  $k$ -regular Cayley graph of girth  $g$ .  $\square$

### 3 Lower bounds for $VTC(k, g)$

The well-known *Moore bound* is a straightforward lower bound on the order  $n(k, g)$  of  $k$ -valent cages of girth  $g$ . The precise form of the bound depends on the parity of  $g$ :

$$n(k, g) \geq M(k, g) = \begin{cases} 1 + k + k(k - 1) + \dots + k(k - 1)^{(g-3)/2}, & g \text{ odd} \\ 2(1 + (k - 1) + \dots + (k - 1)^{(g-2)/2}), & g \text{ even} \end{cases} \quad (3.1)$$

Graphs for which equality holds are called *Moore graphs* and are relatively rare. They are known to exist if and only if  $k = 2$  and  $g \geq 3$  (cycles);  $g = 3$  and  $k \geq 2$  (complete graphs);  $g = 4$  and  $k \geq 2$  (complete bipartite graphs);  $g = 5$  and  $k = 2$  (the 5-cycle),  $k = 3$  (the Petersen graph),  $k = 7$  (the Hoffman-Singleton graph), and possibly  $k = 57$ ;  $g = 6, 8$ , or  $12$  and there exists a symmetric generalized  $n$ -gon of order  $k - 1$  [1, 5, 6]. It is of particular interest that all the known Moore graphs are vertex-transitive graphs. The unsettled case of  $k = 57$  has been shown to not be vertex-transitive; it is however not known whether the cage exists.

All  $(k, g)$ -cages outside the above list must be bigger than the Moore bound by at least one, with several parameter pairs known to force the graphs to be bigger by at least two (see e.g. [6]). The purpose of this section is to further improve these lower bounds for certain families of vertex-transitive graphs. Considering the above classification of Moore graphs, the reader should not be surprised that the results depend heavily on the number-theoretic relations between the parameters  $k$  and  $g$ .

The main argument is based on counting cycles passing through a fixed vertex of a vertex-transitive graph of order close to the Moore bound. In what follows, we use  $\mathcal{W}_G^b(n)$  to denote the set of closed walks of length  $n$  based at a fixed vertex  $b$  of a graph  $G$ , and  $\mathcal{C}_G^b(n)$  to denote the set of oriented cycles of length  $n$  rooted at  $b$ . It is for example not hard to verify that all the known Moore graphs (Cayley or non-Cayley) satisfy the interesting regularity property that each of their edges belongs to the same number of cycles. The following result concerning the number of closed walks in vertex-transitive graphs will form the basis of our generalization.

**Theorem 3.1** ([7]). Let  $G$  be a connected vertex-transitive graph of valence  $k$ ,  $b \in V(G)$ . Let a prime  $p > k$  be relatively prime to  $|V(G)|$ , and let  $r$  be a positive integer. Then

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

Let  $\mathcal{L}(k, g, 0)$  denote the set of integers

$$\{M(k, g) + 1, M(k, g) + 2, \dots, M(k, g) + k\}, \tag{3.2}$$

and  $\mathcal{L}(k, g, i)$ ,  $1 \leq i \leq k$ , denote the set

$$\{k(k-1)^{(g-1)/2} - ik, k(k-1)^{(g-1)/2} - ik + 1, \dots, k(k-1)^{(g-1)/2} - ik + i - 1\}. \tag{3.3}$$

The main result of this section increases the lower bound for  $VTC(k, g)$  for odd prime power girth  $g$  relatively prime to the numbers on the above lists.

**Theorem 3.2.** Let  $G$  be a vertex-transitive graph of valence  $k$  and girth  $g = p^r > k$ , where  $p$  is an odd prime and  $r \geq 1$ . If  $G$  is not a Moore graph, and  $g$  is relatively prime to all the integers in the union

$$\bigcup_{0 \leq i \leq k} \mathcal{L}(k, g, i), \tag{3.4}$$

then the order of  $G$  is at least  $M(k, g) + k + 1$ .

*Proof.* Note that since  $p$  is assumed odd, so is  $g$ . Following the basic underlying idea of the proof of the Moore bound (3.1), all the  $(k, g)$ -graphs contain a (non-induced) rooted tree  $T_{k,g}$  of order  $M(k, g)$  with all the non-leaf vertices of degree  $k$ , and all the leaves of distance  $(g-1)/2$  from the root. Hence, if we assume  $G$  to be a  $(k, g)$ -graph, and choose a (random) vertex  $r$  of  $G$  to be the root of a copy of  $T_{k,g}$  in  $G$ , each of the leaves of the  $T_{k,g}$  must connect to  $k-1$  additional vertices of  $G$ , none of which can be of distance smaller than  $(g-1)/2$  from  $r$ , as all those vertices are assumed to be of degree  $k$  already.

Let us assume that  $k$  and  $g$  satisfy the restrictions from the statement of the theorem and that  $G$  is a vertex-transitive  $(k, g)$ -graph of order  $M(k, g) + s$ ,  $s > 0$ . Then  $G$  contains  $T_{k,g}$  and an additional set  $S$  of  $s$  vertices  $v_1, v_2, \dots, v_s$  not contained in  $T_{k,g}$ . It follows that the distance of the vertices in  $S$  from the root  $r$  of  $T_{k,g}$  is at least  $(g+1)/2$ . If we assume that at least one of these vertices is of distance larger than  $(g+1)/2$ , then this vertex must be adjacent to  $k$  vertices of distance more than  $(g-1)/2$  from the root. All of its neighbors must then lie outside the tree  $T_{k,g}$ , and hence  $s > k$ . It follows that if there exists such a vertex, the theorem holds true.

Next, we will assume that no such vertex exists,  $s \leq k$ , and that all the vertices in  $S$  are of distance  $(g+1)/2$  from  $r$ . Consequently, all the neighbors of the vertices in  $S$  are either leaves of  $T_{k,g}$  or elements of  $S$ . If  $g > k$ , the  $S$ -induced subgraph of  $G$  must be a forest (possibly with no edges), and hence there are at most  $s-1$  edges connecting the vertices of  $S$ . It follows that there are at least  $s \cdot k - s + 1$  edges connecting the leaves of  $T_{k,g}$  and the vertices in  $S$ , and  $G$  has a very specific structure.

Let us denote the number of edges between  $S$  and the leaves of  $T_{k,g}$  by  $t$ . We have shown that

$$s \cdot k - s + 1 \leq t \leq s \cdot k. \tag{3.5}$$

Observe that there are three kinds of edges adjacent to the leaves. Each leaf is adjacent to exactly one vertex of distance  $(g-3)/2$  from the root, and the remaining edges connect the

leaf to a mixture of the other leaves and the elements from  $S$  (with one of the groups possibly missing). Furthermore, if we denote the edges adjacent to the root  $r$  by  $e_1, e_2, \dots, e_k$ , they give rise to  $k$  branches of  $T_{k,g}$ , and each vertex of  $S$  must be attached to each of these branches at most once: If one of the vertices  $v_i$  was attached to some branch at least twice, say to the  $e_j$ -branch, it would give rise to a small cycle through  $v_i$ , its two neighbors in the  $e_j$  branch and the non-root endpoint of  $e_j$ , of length  $(g-3)/2 + (g-3)/2 + 2 = g-1 < g$ ; a violation of the girth of  $G$ . This very same argument can be also used to show that the edges connecting a fixed leaf to other leaves must go to different branches as well.

As  $g$ , the girth of  $G$ , is assumed odd, there are no closed walks in  $G$  of length  $g$  that are not at the same time cycles, and thus

$$C_G^r(g) = \mathcal{W}_G^r(g).$$

Let us count the number of oriented cycles of length  $g$  passing through the root  $r$  of  $T_{k,g}$ . Note first that each such cycle must contain exactly two leaves of distance  $(g-1)/2$  from  $r$  and of distance 1 from each other, with the two leaves belonging to distinct branches. Clearly, none of these cycles can contain any vertices from  $S$ . As each leaf of  $T_{k,g}$  is either attached to another leaf or an element of  $S$ , each (oriented) edge connecting a leaf to another leaf gives rise to a different oriented  $g$ -cycle and there are no other  $g$ -cycles in  $G$ : the number  $C_G^r(g)$  is equal to the number of (oriented) edges between the leaves of  $T_{k,g}$ . Hence,

$$C_G^r(g) = k(k-1)^{(g-1)/2} - t.$$

The rest of the proof relies on Theorem 3.1. Namely, as  $g$  is assumed to be relatively prime to the numbers on the list (3.2) which *must* contain the order of  $G$ ,  $\mathcal{W}_G^r(g) = C_G^r(g)$  must be congruent to 0 modulo  $p$ . On the other hand,  $\mathcal{W}_G^r(g)$  *must* be contained among the numbers in the union  $\bigcup_{1 \leq i \leq k} \mathcal{L}(k, g, i)$  (with  $\mathcal{L}(k, g, i)$  representing the possibilities for  $s = i$ ), none of which is congruent to 0 modulo  $p$ . We obtain a contradiction, and conclude that  $s$  must be greater than  $k$ .  $\square$

Although the number theoretic conditions listed in the statement of our theorem appear very restrictive, there are many parameters suitable for the application of the theorem. Take for example the case of trivalent graphs,  $k = 3$ ,  $M(3, g) = 1 + 3(2^{(g-1)/2} - 1)$ . In this case (since  $k$  is odd), the smallest non-Moore  $(k, g)$ -graph must be of order at least  $M(k, g) + 2$ . This allows us to leave out the possibility of only one vertex included in the set  $S$  and to leave  $M(3, g) + 1$  and the set  $\mathcal{L}(3, g, 1)$  out of the set of prohibited numbers. Our theorem applies to all cases when  $g$  is an odd prime power relatively prime to the seven integers

$$3 \cdot 2^{(g-1)/2}, \quad 3 \cdot 2^{(g-1)/2} + 1, \quad 3 \cdot 2^{(g-1)/2} - 6, \quad 3 \cdot 2^{(g-1)/2} - 5, \\ 3 \cdot 2^{(g-1)/2} - 9, \quad 3 \cdot 2^{(g-1)/2} - 8, \quad 3 \cdot 2^{(g-1)/2} - 7$$

and a quick test reveals that out of the first 150 odd primes, 147 satisfy the conditions of the theorem. For example, the first prime on this list is the number 7. This implies that the smallest trivalent vertex-transitive graph of girth 7 must be of order at least  $M(3, 7) + 3 + 1 = 26$ . This agrees with the fact that the unique  $(3, 7)$ -cage, the McGee graph of order 24 (see [6]), is the smallest trivalent cage that is not vertex-transitive. The next number on the list is the number 13 which is the smallest unsettled trivalent case. Our result implies that the smallest vertex-transitive trivalent graph of girth 13 must be of order  $M(3, 13) + 3 + 1 = 194$ . The smallest known trivalent graph of girth 13 is a Cayley graph

of order 272 constructed by Hoare (as reported by Biggs in [3]). Royle [11] has shown that a smaller (3, 13)-graph cannot be a Cayley graph. McKay and Myrvold have shown that there is no (3, 13)-graph of order smaller than 202.

Running a similar test for  $k = 5$  shows that 144 of the first 150 odd primes satisfy the conditions. The first number on the list is the number 11.

It is also interesting to note that Theorem 3.1 allows one to show the non-existence of vertex-transitive  $(k, g)$ -graphs of order equal to the Moore bound.

**Corollary 3.3.** If  $g = p^r$  is relatively prime to  $M(k, g)$  and  $k(k - 1)^{(g-1)/2}$ , then there is no vertex-transitive  $(k, g)$ -graph of order  $M(k, g)$ . In particular, if  $p$  is relatively prime to  $k, k - 1$ , and  $k + 2$ , there is no vertex-transitive  $(k, p^r)$ -graph of order  $M(k, p^r)$ , for any  $r \geq 1$ .

*Proof.* Following the argument presented in the proof of Theorem 3.2, we see that the number of  $g$ -cycles in a  $(k, g)$ -Moore graph that contain the root  $r$  of  $T_{k,g}$  is  $k(k - 1)^{(g-1)/2}$ . As this number is once again equal to the number of closed oriented  $g$ -walks through  $r$ , Theorem 3.1 applied to the order of the graph  $M(k, g)$  and this number yields the result of the first part of the theorem.

For the second part, assume that  $p$  is relatively prime to  $k, k - 1$ , and  $k + 2$ , and note that this implies that  $p^r$  is relatively prime to  $k(k - 1)^{(p^r-1)/2}$ . Moreover, due to Fermat’s Little Theorem,  $(k - 1)^{(p-1)} \equiv 1 \pmod{p}$ , and consequently,

$$(k - 1)^{(p^r-1)} = (k - 1)^{(p-1)(p^{r-1}+\dots+1)} \equiv 1 \pmod{p}.$$

It follows that  $(k-1)^{(p^r-1)/2}$  is a square root of 1 modulo  $p$ , and therefore  $(k-1)^{(p^r-1)/2} \equiv \pm 1 \pmod{p}$ . Summing up the terms yields  $M(k, g) = 1 + k \frac{(k-1)^{(g-1)/2} - 1}{k-2}$ , and we have two possibilities to consider. If  $(k - 1)^{(p^r-1)/2} \equiv 1 \pmod{p}$ , then  $M(k, p^r) \equiv 1 \pmod{p}$ , and  $p^r$  is relatively prime to  $M(k, g)$  and  $k(k - 1)^{(g-1)/2}$ . If  $(k - 1)^{(p^r-1)/2} \equiv -1 \pmod{p}$ , then  $(k - 2)M(k, g) \equiv -k - 2 \not\equiv 0 \pmod{p}$ , and the same is true again. In either case, the first part of our theorem implies the desired result.  $\square$

Running the test for  $k = 3$  yields the well-known answer: The only primes  $p$  among the first 150 odd primes for which there may exist a vertex-transitive  $(3, p)$ -graph of order  $M(3, p)$  are the primes 3 and 5. The same result is true when testing for  $k = 5$ , the test for  $k = 4$  also excludes  $g = 5$ , and similar results hold when testing for powers of odd primes.

We conclude this section with a conjecture that, if true, covers all the  $k$ -valent vertex-transitive graphs of odd girth  $g$ .

**Conjecture 3.4.** Let  $G$  be a vertex-transitive graph of valence  $k$  and girth  $g$  that is an odd number. If the order of  $G$  is greater than the Moore bound  $M(k, g)$ , then this order is at least  $M(k, g) + k - 1$ .

Although we have obviously not been able to complete the proof of this conjecture, the reason we expect it to be true can be described as follows: As in the proof of Theorem 3.2, if we assume that at least one of the vertices added to  $T_{k,g}$  is of distance at least  $(g + 3)/2$  from its root, the above theorem must hold true. If all the  $s$  added vertices are of distance  $(g + 1)/2$  from  $r$ , and we assume by means of contradiction that  $s < k - 1$ , there must exist an  $e_i$ -subbranch of  $T_{k,g}$  with the property that out of its  $k - 1$  subbranches at least one is not directly attached to the elements of  $S$  and at least one is directly attached to at least

one element in  $S$ . It appears likely that one may be able to find some counting criterion that would distinguish the end point of the edge  $e_i$  from the root  $r$ , thereby violating the vertex-transitivity of  $G$ .

#### 4 Generalization of the Bray, Parker, Rowley construction

Further improvements on some of the records obtained using Cayley graphs were made by Bray, Parker and Rowley [4]. They constructed a number of current record holders for degree three by factoring out the 3-cycles in trivalent Cayley graphs. Their construction starts with a trivalent Cayley graph,  $C(\Gamma, X)$ ,  $|X| = 3$ , subject to the condition that the generating set  $X$  contains an involution,  $\alpha$ , two mutually inverse elements of order 3,  $\delta, \delta^{-1}$ , and that the graph has no cycles of length 4. The graph  $BPR(\Gamma; X)$  is then defined as follows: the vertex set  $\mathcal{T}$  of  $BPR(\Gamma; X)$  is the set of triangles of  $C(\Gamma, X)$  with triangle  $T_i$  adjacent to triangle  $T_j$  in  $BPR(\Gamma; X)$  if at least one of the vertices of  $T_i$  is adjacent in  $C(\Gamma, X)$  to at least one of the vertices of  $T_j$  via an edge labeled by the involution  $\alpha$ . The graph  $BPR(\Gamma; X)$  is a cubic graph with  $|\Gamma|/3$  vertices and  $\Gamma$  acts transitively on the vertices of  $BPR(\Gamma; X)$ . The Bray, Parker, Rowley construction can be generalized as follows.

Let  $G$  be a graph, and  $\mathcal{C}$  be a set of pairwise disjoint cycles of  $G$ . The *cycle factor* of  $G$ ,  $G' = CF_{\mathcal{C}}(G)$  is the graph with the vertex set  $\mathcal{C}$  under the adjacency connecting cycles joined by at least one edge (that is,  $C_1, C_2 \in \mathcal{C}$  are connected if there exist vertices  $v_1 \in C_1$  and  $v_2 \in C_2$  such that  $v_1$  and  $v_2$  are adjacent in  $G$ ). For example, the above defined graph  $BPR(\Gamma; X)$  is the cycle factor  $CF_{\mathcal{C}}(C(\Gamma, X))$  where  $\mathcal{C}$  is the set of all 3-cycles of  $C(\Gamma, X)$ .

**Theorem 4.1.** Let  $G$  be a trivalent vertex-transitive graph with the shortest cycle of odd length  $g_1$  and the second shortest cycle of length  $g_2$ . If  $g_2 > 2g_1$ , then the cycle factor graph  $G' = CF_{\mathcal{C}}(G)$  obtained by factoring out all the  $g_1$ -cycles of  $G$  is a vertex-transitive  $g_1$ -valent graph of order  $|V(G)|/g_1$  and girth greater than or equal to  $2g_2/g_1$ .

*Proof.* Let  $G$  be as above. We claim that each vertex of  $G$  lies on exactly one cycle of length  $g_1$ . First, since  $G$  is assumed to contain at least one cycle of length  $g_1$  and to be vertex-transitive, it follows that each vertex of  $G$  must lie on at least one cycle of length  $g_1$ . Furthermore, as the degree of  $G$  is 3, any two cycles that share a vertex must share an edge. Thus, if we allowed for the existence of a vertex  $v$  of  $G$  that lies on two cycles of length  $g_1$ , the two cycles would share at least one edge incident to  $v$ . Consider the set of all edges shared by these two cycles. This set must be a path as otherwise at least one pair of arches connecting two consequent disconnected shared paths would give rise to at least one cycle of length smaller than  $g_1$  (by the Pigeonhole Principle). This yields that the set of non-shared edges of the two cycles comprises a cycle. Its length must be even and smaller than  $2g_1$ ; a contradiction. It follows that the vertex set of  $G$  splits into non-overlapping  $g_1$ -cycles.

Next, let  $C$  be a fixed  $g_1$ -cycle, and  $u, v$  be vertices of  $C$ . Then  $u$  is adjacent to a vertex  $u'$  outside  $C$  that belongs to a  $g_1$ -cycle  $C'$ , and  $v$  is adjacent to  $v'$  that belongs to  $C''$ . Then  $C'$  and  $C''$  are disjoint  $g_1$ -cycles. To see this, assume the opposite, namely,  $C' = C''$ . Then the arch between  $u$  and  $v$  together with the arch between  $u'$  and  $v'$  and the edges  $uu'$  and  $vv'$  give rise to a cycle of length smaller than  $2g_1$  that shares edges with both  $C$  and  $C'$  – a contradiction. We conclude that  $C$  is adjacent to  $g_1$  distinct  $g_1$ -cycles of  $G$ .

It is easy to see that the automorphism group of  $G$  acts transitively on the set of its  $g_1$ -cycles, and therefore also on the vertices of  $CF_{\mathcal{C}}(G)$ . To complete the proof, we need

to determine the girth of  $CF_C(G)$ . Let  $K$  be any cycle of  $G$  of length at least  $g_2$ , and let  $C$  be a  $g_1$ -cycle with a non-empty intersection with  $K$ . Then (following the same trail of argument as above), the intersection must be a path. In the case when this path is longer than  $(g-1)/2$ , by replacing this path by its complement in  $C$  one obtains a shorter cycle  $K'$  whose factor in  $G'$  is the same as the factor of  $K$ . Hence, without loss of generality, we may assume that the intersections of  $K$  with  $g_1$ -cycles are of lengths smaller than  $g_1/2$ . As  $g_1$ -cycles do not share vertices, any two intersection paths must be separated by an edge not belonging to a  $g_1$ -cycle but joining two distinct  $g_1$ -cycles. Each such edge constitutes an edge in a cycle of  $G'$ , and hence the length of the factored cycle is at least the length of  $K$  divided by  $g_1/2$ .  $\square$

The basic idea for this observation took shape for the first time during the visit by Gabriela Araujo Pardo to the second author at the Indiana State University. At that time, we could not reliably produce vertex-transitive graphs with a cycle spectrum whose first and second cycle lengths are far apart. In view of the results of Section 2, we see that this is not a problem any more. Namely, one can construct a trivalent Cayley graph for any pair  $g_1, g_2$ , with  $g_1$  odd and  $g_2$  even and larger than  $g_1$ , by considering the Cayley maps of covalence  $(g_2, g_1, g_2)$ . Based on these graphs, our cycle factoring construction yields  $g_1$ -valent vertex-transitive graphs of arbitrary large girth.

## References

- [1] E. Bannai and T. Ito, On finite Moore graphs, *J. Fac. Sci. Tokyo, Sect. IA*, **20** (1973), 191–208.
- [2] N. L. Biggs, Girth and residual finiteness, *Combinatorica* **8** (1988), 307–312.
- [3] N. L. Biggs, Cubic graphs with large girth, *Combinatorial Mathematics: Proceedings of the Third International Conference, Annals of the New York Academy of Sciences* **555** (1989), 56–62.
- [4] J. Bray, C. Parker and P. Rowley, Cayley type graphs and cubic graphs of large girth, *Discrete Math.* **214** (2000), 113–121.
- [5] R. M. Damerell, On Moore graphs, *Proc. Cambridge Phil. Soc.* **74** (1973), 227–236.
- [6] G. Exoo and R. Jajcay, Dynamic cage survey, *Electron. J. Combin.*, Dynamic Survey 16, September 2008.
- [7] R. Jajcay, A. Malnič and D. Marušič, On the number of closed walks in vertex-transitive graphs, *Discrete Math.* **307** (2007), 484–493.
- [8] M. Mačaj, J. Širáň and M. Ipolyiová, Injectivity radius of representations of triangle groups and planar width of regular hypermaps, *Ars Math. Contemp.* **1** (2008), 223–241.
- [9] R. Nedela and M. Škovič, Regular maps on surfaces with large planar width, *European J. Combin.* **22** (2001), 243–261.
- [10] R. B. Richter, J. Širáň, R. Jajcay, T. W. Tucker and M. E. Watkins, Cayley maps, *J. Combin. Theory Ser. B* **95** (2005), 189–245.
- [11] G. Royle, *Cubic Cages*, <http://mapleta.maths.uwa.edu.au/~gordon/remote/cages/index.html>.
- [12] H. Sachs, Regular graphs with given girth and restricted circuits, *J. London Math.* **38** (1963), 423–429.
- [13] J. Šiagiová and M. E. Watkins, Covalence sequences of planar vertex-homogeneous maps, *Discrete Math.* **307** (2007), 599–614.