A Note on Large Cayley Graphs of Diameter Two and Given Degree

Mária Ždímalová

Slovak University of Technology
Radlinského 11, 813 68 Bratislava, Slovak Republik
zdimalova@math.sk

Abstract: Let $C(d,2)$, $AC(d,2)$, *and* $CC(d,2)$ *be the largest order of a Cayley graph of a group, an Abelian group, and a cyclic group, respectively, of diameter 2 and degree d. The currently known best lower bounds on these parameters are* $C(d,2) \geq (d+1)^2/2$ *for degrees* $d = 2q-1$ *where* q *is an odd prime power,* $AC(d,2) \geq (3/8)(d^2-4)$ *where* $d = 4q-2$ *for an odd prime power* q, *and* $CC(d,2) \geq (9/25)(d+3)(d-2)$ *for* $d = 5p-3$ *where* p *is an odd prime such that* $p \equiv 2 \bmod 3$. *For diameter two we present a construction for `large' Cayley graphs of semidirect products of groups out of `small' Cayley graphs of cyclic groups, such that the ratio of the order of the graph to the square of the degree of the graph is approximately the same for both the input and the output graphs. As a consequence we obtain a lower bound on* $C(d,2)$ *of the form* $(9/25)d^2 - O(d)$ *for a much larger variety of degrees than those listed above.*

Keywords: Cayley graph; group; degree; diameter

1 Introduction

The interest in Cayley graphs and digraphs of given diameter and degree, and of order as large as possible, has been motivated by problems in group theory, graph theory, and theoretical computer science.

In group theory the interplay between the order, degree, and diameter has been studied in terms of bases. A h-basis of a finite group G is a subset B of G such that every element of G is a product of h not necessarily distinct elements of B. The most intristuing question in the study of h-basis is whether or not for each $h \geq 2$ there is a constant c_h such that every finite group G has a h-basis B satisfyiing $|B| \leq c_h |G^{1/h}|$, see [9, 10]. Using Classification of the Finite Simple

Groups an afirmative answer was given in [2, 3], with the value $c_2 = 4/\sqrt{3}$. For larger h, the existence of c_h was establishes only for various restricted types of groups [10, 4, 1] and the question is still very much open.

The problem translates into the language of graph theory by means of constructing minimal generating sets in groups such that the corresponding Cayley digraph has diameter h. The study of such digraphs is part of the *degree-diameter* problem which was initiated about fifty years ago and asks for identification of the largest graphs and digraphs of given degree and diameter. For history and latest development in the degree-diameter problem we recommend the survey [8] and the recent paper [5]. Not surprisingly, research into the degree-diameter problem was also motivated by questions in the design of interconnection networks in theoretical computer science; we again refer to [8] for more information.

In this paper we will only consider constructions of *undirected* Cayley graphs of diameter two, trying to make their order as large as possible. We therefore review related results on large Cayley graphs of given diameter and degree only in the special case of diameter 2.

Let G be a finite group and let S be unit-free generating set for G such that $S = S^{-1}$, that is, we assume that S is closed under taking inverse elements. The *Cayley graph* $Cay(G,S)$ has vertex set G, and two vertices $g,h \in G$ are joined by an edge if $g^{-1}h \in S$. Since this condition is equivalent to $h^{-1}g \in S$ because of $S = S^{-1}$, the Cayley graph $Cay(G,S)$ is undirected. Obviously, the degree of $Cay(G,S)$ is $|S|$, and the diameter of $Cay(G,S)$ is 2 if and only if every non-identity element of $G \setminus S$ is a product of two elements from S.

For an arbitrary integer $d \geq 3$ we let $C(d,2)$, $AC(d,2)$, and $CC(d,2)$ denote the largest order of a Cayley graph of a group, an Abelian group, and a cyclic group, respectively, of diameter 2 and degree d. From results summed up in [8] one can extract the upper bounds $C(d,2) \leq d^2 - 1$ and $CC(d,2) \leq AC(d,2) \leq 1 + d + d^2/2$ for all $d \geq 3$. Our interest, however, will be in the corresponding lower bounds.

It appears that the currently known best lower bounds on these parameters are quite far from the upper bounds. For general Cayley graphs the best lower bound is $C(d,2) \geq (d+1)^2/2$ but we only have it for degrees $d = 2q-1$ where q is an odd prime power [11]. In the Abelian case the best available estimate is $AC(d,2) \geq (3/8)(d^2-4)$ (where $d = 4q-2$ for an odd prime power q, and for cyclic groups we have $CC(d,2) \geq (9/25)(d+3)(d-2)$ for $d = 5p-3$ where p is an odd prime such that $p \equiv 2 \bmod 3$; both results have been proved in [6]. By [7]

the only known lower bound on $C(d,2)$ valid for *all* d is the inequality $C(d,2) \geq AC(d,2) \geq \lfloor (d+2)/2 \rfloor \lceil (d+2)/2 \rceil$. For degrees $d \leq 20$ the values of $C(d,2)$ or their estimates that have been found with the help of computers can be looked up in the tables [12].

Our aim is to derive similar bounds for wider sets of degrees. In Section 2 we present, for diameter 2, a construction that takes as the input a Cayley graph of a cyclic group and produces a larger Cayley graph of a semidirect product of groups, such that the ratio of the order of the graph to the square of the degree of the graph is approximately the same for both Cayley graphs. We apply the construction to deriving new lower bounds on $C(d,2)$ in Section 3. In particular, our best estimate on $C(d,2)$ has the form $(9/25)d^2 - O(d)$ for a much larger variety of degrees than those listed above. In the course of our presentation we also discuss a few related questions.

2 The Construction

Our construction is based on the following general theorem.

Theorem 1 Assume that d and k are such that there exists a Cayley graph of degree d and diameter 2 for a cyclic group of order k with an involution-free generating set. Let n be a product of (not necessarily distinct) prime powers, each congruent to $1 \mod k$. Then there exists a Cayley graph of order $n^2 k$, diameter 2, and degree $dn + 2(n-1)$.

Proof. Let k be as in the statement of our theorem. Let n have a factorization $n = q_1 q_2 .. q_m$ in which all the (not necessarily distinct) prime powers q_i are congruent to $1 \mod k$. For $1 \leq i \leq m$ let $F_i = GF(q_i)$ be the Galois field of order q_i. Further, let $H_i = F_i \times F_i$ for $1 \leq i \leq m$, and let $H = H_1 \times H_2 \times \ldots \times H_m$. Since $q_i \equiv 1 \mod k$ for $1 \leq i \leq m$, in the (cyclic) multiplicative group of F_i there exists an element β_i of order k. Then, for each i, $1 \leq i \leq m$, the cyclic group Z_k has an action on H_i given by assigning, to every $j \in Z_k$, the automorphism of $H_i = F_i \times F_i$ given by taking the element $(u_i, v_i) \in H_i$ onto the element $(\beta_i^j u_i, v_i) \in H_i$. The product of these actions gives a homomorphism θ from Z_k into the automorphism group $Aut(H)$ of the group H. Consider the semidirect product $\mathrm{G} = \mathrm{H} \rtimes Z_k$ corresponding to the homomorphism θ.

We will write a general element of G in the concise form $((u_i, v_i), j)$ where $j \in Z_k$ and the part (u_i, v_i) stands for the $2m-$tuple $(u_1, v_1; u_2, v_2; \ldots; u_m, v_m)$

with $(u_i, v_i) \in H_i = F_i \times F_i$ and $1 \le i \le m$. With this notation, operation in the semidirect product $\mathrm{G} = \mathrm{H} \rtimes Z_k$ is given by

$$((u_i, v_i), j)((u_i', v_i'), j') = ((u_i + \beta_i^j u_i', v_i + v_i'), j + j')$$

and the inverse to $g = ((u_i, v_i), j)$ is $g^{-1} = ((-\beta_i^{-j} u_i, -v_i), -j)$.

By our assumption, we have a Cayley graph $Cay(Z_k, S)$ for an involution-free generating set S of Z_k such that $|S| = d$, with the property that every non-zero element of $Z_k \setminus S$ is a sum of two elements from S. Obviously, the set S can be partitioned into two subsets S' and $-S' = \{-s; s \in S'\}$ such that $S' \cap -S' = \emptyset$ and $S' \cup -S' = S$. In what follows we fix such a partition.

We now introduce a generating set for G. First, let

$$Y = \{((u_i, u_i), s) \in G;\ u_i \in F_i \text{ and } s \in S'\}.$$

By the formula for inverses in G we have (replacing $-u_i$ with u_i)

$$Y^{-1} = \{((\beta_i^{-s} u_i, u_i), -s);\ u_i \in F_i \text{ and } s \in S'\}.$$

We will also need another subset Y' of G given by

$$Y' = \{((u_i, 0), 0), ((0, u_i), 0);\ u_i \in F_i \text{ and } u_i \neq 0 \text{ for some } i\};$$

observe that $(Y')^{-1} = Y'$. Finally, let $X \in Y \cup Y^{-1} \cup Y'$; clearly, X is a unit-free subset of G such that $X = X^{-1}$.

Obviously, $|G| = n^2 k$ and $|X| = nd + 2(n-1)$. In the remaining part of the proof we show that the Cayley graph $Cay(G, X)$ has diameter 2. This is equivalent to showing that every non-identity element $g \in G$ such that $g \notin X$ is a product of two elements from X. We will consider several cases depending on the last coordinate of g.

We begin with $g = ((u_i, v_i), 0)$. Since g is not in X, at least one u_i and also at least one $v_{i'}$ are non-zero. Then, g is a product of two elements from $Y' \subset X$ as follows:

$$g = ((u_i, v_i), 0) = ((u_i, 0), 0)((0, v_i), 0).$$

If $g = ((u_i, v_i), s)$ with $s \in S'$, then $u_i \neq v_i$ for at least one i as $g \notin X$. Then, g is a product of two generators from $Y' \cup Y$ of the form

$$g = ((u_i, v_i), s) = ((0, v_i - u_i), 0)((u_i, u_i), s).$$

In the case when $g = ((u_i, v_i), -s)$ for some $s \in S'$ we let $w_i = \beta_i^s u_i$ for $1 \le i \le m$. Since $g \notin X$, it follows that $w_i \neq v_i$ for at least one i. One can check that g is now a product of two generators in $Y' \cup Y^{-1} \subset X$ of the form

$$g = ((u_i, v_i), -s) = ((0, v_i - w_i), 0)((\beta_i^{-s} w_i,\ w_i), -s).$$

The last case to consider is $g = ((u_i, v_i),\ j)$ where $(u_i, v_i) \in H_i$ are arbitrary, and $j \in Z_k \setminus S$ such that $j \neq 0$. By our assumption on the graph $Cay(Z_k, X)$, there exists $s, t \in S'$ such j is equal to either $s+t$, or $s-t$, or else $-s-t$. We show that either way g is a product of two elements from $Y \cup Y^{-1} \subset X$. We give details only in the third case when $j = -s-t$, leaving the first two (and easier) cases to the reader. The key is to show that there are elements $((\beta_i^{-s} x_i, x_i), -s)$, $((\beta_i^{-t} y_i, y_i), -t) \in Y^{-1} \subset X$ such that

$$g = ((u_i, v_i), -s-t) = ((\beta_i^{-s} x_i, x_i), -s)((\beta_i^{-t} y_i, y_i), -t).$$

Evaluating the product we obtain

$$((u_i, v_i), -s-t) = ((\beta_i^{-s} x_i + \beta_i^{-s}(\beta_i^{-t} y_i), x_i + y_i), -s-t).$$

For each i, $1 \le i \le m$, the 2×2 linear system

$$\beta_i^{-s} x_i + \beta_i^{-s-t} y_i = u_i, \quad x_i + y_i = v_i$$

has a solution $x_i, y_i \in F_i$ since the determinant of the system is $\beta_i^{-s}(1 - \beta_i^{-t})$, which is non-zero for any $s, t \in S'$ by the choice of β_i. This proves the existence of the two generators $((\beta_i^{-s} x_i, x_i), -s) \in X$ and $((\beta_i^{-t} y_i, y_i), -t) \in X$ in the above product for g.

Summing up, our arguments imply that the Cayley graph $Cay(G, X)$ has diameter 2, order $n^2 k$ and degree $nd + 2(n-1)$. □

3 Applications

Theorem 1 allows us to construct, from an infinite sequence of diameter-two Cayley graphs of *cyclic* groups, a new infinite sequence of diameter-two Cayley graphs of *non-Abelian* groups, such that the ratio of the order of the graph to the square of the degree of the graph is approximately the same for both the input and the output graphs. We formalize this as follows.

Corollary 1 Suppose that there is a positive constant λ and increasing infinite sequences of positive integers d_l and k_l with $k_l / d_l^2 \to \lambda$ as $l \to \infty$, such that for every $l \geq 1$ there is a Cayley graph of degree d_l and diameter 2 for a cyclic group of order k_l with an involution-free generating set. Then, for every $l \geq 1$ and for any positive integer n_l which is a product of prime powers all congruent to 1 mod k, there is a Cayley graph of order $k_l = n_l^2 k_l$ and degree $\delta_l = n_l d_l + 2(n_l - 1)$; moreover, $k_l / \delta_l^2 \to \lambda$ as $l \to \infty$.

Proof Most of the statement is a direct consequence of Theorem 1. The fact that $k_l / \delta_l^2 \to \lambda$ as $l \to \infty$ follows from the assumption $k_l / d_l^2 \to \lambda$ as $l \to \infty$ by an easy limit calculation. □

The obvious advantage of our Theorem 1 and Corollary 1 in constructions of `large' Cayley graphs of a given degree and diameter 2 is a much wider variety of degrees of the resulting graphs. The drawback is that the output graphs are Cayley graphs for non-Abelian groups. Nevertheless, in the absence of more general results our approach appears to be fruitful. We illustrate this on two examples in which the input sequences are the currently largest Cayley graphs of cyclic groups of diameter 2 and given degree described in [6].

In Theorem 3 of [6] it was proved that $CC(d,2) \geq (9/25)(d+3)(d-2)$ for $d = 5p - 3$ where p is an odd prime such that $p \equiv 2$ mod 3, by exhibiting a Cayley graph of diameter 2 for a cyclic group of order $9p(p-1)$ with an involution-free generating set of size $d = 5p - 3$. Applying our Theorem 1 to this situation we immediately obtain:

Corollary 2 Let p be an odd prime such that $p \equiv 2$ mod 3. Let n be a product of prime powers, each congruent to 1 mod $9p(p-1)$. Then, there exists a Cayley graph of order $9n^2 p(p-1)$, degree $(5p-1)n - 2$, and diameter 2. In particular, we have a lower bound on $C(d,2)$ of the form $(9/25)d^2 - O(d)$ for all degrees of the form $d = (5p-1)n + 2c$ where n is as above, for any integer constant $c \geq -1$ while $p \to \infty$.

Proof Letting $k = 9p(p-1)$, $d = 5p - 3$, invoking the result of Theorem 3 of [6] outlined before the statement of the corollary and applying our Theorem 1, we obtain, for any n as in the statement, the existence of a Cayley graph of order $kn^2 = 9n^2 p(p-1)$, degree $nd + 2(n-1) = (5p-1)n - 2$, and diameter 2. We may extend the generating set X constructed in the proof of Theorem 1 by any set of $2(c+1)$ non-involutory elements and their inverses, for any $c \geq -1$; this adds $2(c+1)$ to the degree but does not increase the diameter. For any such constant c

and for $p \to \infty$ we therefore obtain Cayley graphs of degree $d = (5p-1)n + 2c$, the same order $9n^2 p(p-1)$, and diameter 2. The conclusion about the lower bound on $C(d,2)$ follows. □

This illustrates well the point raised earlier. We have started with the bound $CC(d,2) \geq (9/25)(d+3)(d-2)$, proved in [6] for a very restricted set of degrees of the form $d = 5p-3$ where p is an odd prime such that $p \equiv 2 \mod 3$. Our Corollary 2 yields a lower bound on $C(d,2)$ of the asymptotic order $(9/25)d^2 - O(d)$ for a much wider set of degrees compared with the above, but our approach requires going beyond Abelian groups.

For our second application we borrow another result of [6], namely, Theorem 4. It gives, for each prime $p \equiv 2 \mod 3$, a Cayley graph of a cyclic group of order $3p(p-1)$ of diameter 2 and degree $3(p-1) + 2\lfloor r/2 \rfloor + 2(\lceil (p-1)/r \rceil - 1))$ where $r = \lceil \sqrt{p-1} \rceil$, with an involution-free generating set. Proceeding as in the proof of Corollary 2, but leaving out the obvious details, yields the following result.

Corollary 3 Let p be any prime such that $p \equiv 2 \mod 3$. Let n be a product of prime powers, all congruent to 1 mod $3p(p-1)$. Then, there exists a Cayley graph of order $3n^2 p(p-1)$, degree $n(3(p-1) + 2\lfloor r/2 \rfloor + 2(\lceil (p-1)/r \rceil - 1)) + 2(n-1)$, and diameter 2.

Mimicking the proof of Corollary 2 we conclude that for any integer constant $c \geq -1$ and for all degrees of the form $d = n(3(p-1) + 2\lfloor r/2 \rfloor + 2(\lceil (p-1)/r \rceil - 1)) + 2n + 2c$ the quantity $C(d,2)$ is bounded from below by an expression of the form $d^2/3 - O(d^{3/2})$ for $p \to \infty$. This bound is, in terms of the multiplicative constant at d^2, weaker than the result of Corollary 2. Nevertheless it applies to a rather different set of degrees and is therefore worth having in an explicit form.

Acknowledgement

The author wishes to thank Jozef Širáň for his assitance in the preparation of this paper. Research of the author was supported by the VEGA Research Grant No. 1/0489/08, the APVV Research Grants No. 0040-06 and 0104-07, and the APVV LPP Research Grants No. 0145-06 and 0203-06. The author acknowledge the "Program na podporu mladých vedeckých výskumníkov," FCE, Slovak University of Technology in Bratislava, 7601 Podpora mladých výskumníkov-Veľké vrcholovo-tranzitívne a cayleyovské grafy daného stupňa a priemeru- VVTCG, 781000.

References

[1] E. Bertram, M. Herzog: On Regular Bases of Finite Groups, Amer. Math. Monthly, Vol. 103, No. 9, 1996, pp. 796-799

[2] L. Finkelstein, D. Kleitman, T. Leighton: Applying the Classification Theorem for Finite Simple Groups to Minimize Pin Count in Uniform Permutation Architectures, in Proceedings of Aegean Workshop on Computing, Lecture Notes in Computer Science, Vol. 319, Springer-Verlag, Berlin/New York, 1988, pp. 247-256

[3] G. Kozma, A. Lev: Bases and Decomposition Numbers of Finite Groups, Arch. Math. 58, 1992, pp. 417-424

[4] G. Kozma, A. Lev: On h-bases and h-decompositions of the Finite Solvable and Alternating Groups, J. Number Theory 49, 1994, pp. 385-391

[5] E. Loz, and J. Širáň: New Record Graphs in the Degree-Diameter Problem, Australasian J. Combin. 41, 2008, pp. 63-80

[6] H. Macbeth, J. Šiagiová, J. Širáň: Cayley Graphs of Given Degree and Diameter for Cyclic, Abelian, and Metacyclic Groups, Preprint 2009, submitted

[7] B. McKay, M. Miller, J. Širáň: A Note on Large Graphs of Diameter Two and Given Maximum Degree, Journal of Combinatorial Theory, Series B 74, 1998, pp. 110-118

[8] M. Miller, J. Širáň: Moore Graphs and Beyond: A Survey of the Degree - Diameter Problem, Electronic J. Combinat., Dynamic survey No. D14, 2005, 61pp

[9] H. Rohrbach: Ein Beitrag zur additiven Zahlentheorie, Math. Z. 42, 1937, pp. 1-30

[10] H. Rohrbach: Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage, Math. Z. 42, 1937, pp. 538-542

[11] J. Šiagiová, J. Širáň: A Note on Large Cayley Graphs of Diameter Two and Given Degree, Discrete Math. 305, 2005, No. 1-3, pp. 379-382

[12] On-Line Table of Current Largest Graphs for the Degree-Diameter Problem: www.eyal.com.au/wiki/The_Degree/Diameter_Problem