

Revisiting constructions of large Cayley graphs of given degree and diameter from regular orbits

Martin Bachratý

University of Auckland, Auckland, New Zealand, and
Slovak University of Technology, Bratislava, Slovakia

Jana Šiagiová

Slovak University of Technology, Bratislava, Slovakia

Jozef Širáň

Open University, Milton Keynes, U.K., and
Slovak University of Technology, Bratislava, Slovakia

Abstract

The largest order $C(d, k)$ of a Cayley graph of degree $d \geq 3$ and diameter $k \geq 2$ cannot exceed the Moore bound $M(d, k)$ the asymptotic form of which is $M(d, k) = d^k - O(d^{k-1})$ for $d \rightarrow \infty$ and a fixed k . The second and the third author (2012) and the three authors (2015) proved by direct constructions that the Moore bound for diameter $k = 2$ and $k = 3$, respectively, can be approached asymptotically by Cayley graphs in the sense that $C(d, k)/M(d, k) \rightarrow 1$ for some sequences of degrees $d \rightarrow \infty$. In this note we present a unifying principle underlying the two results, based on the existence of certain regular orbits of automorphism groups of suitable graphs.

Keywords: Degree; Diameter; Moore bound; Cayley graph.

1 Introduction

The largest order $n(d, k)$ of a graph of maximum degree d and diameter k turns out to be bounded above by the Moore bound $M(d, k) = 1 + d + d(d - 1) + \dots + d(d - 1)^{k-1}$. It is well known [12, 3, 6] that, leaving out trivial instances, for $d \geq 3$ and $k \geq 2$ the equality $n(d, k) = M(d, k)$ holds only for $k = 2$ and $d = 3, 7$, and possibly 57. For a survey of results about the difference $M(d, k) - n(d, k)$ for other values of d and k we refer to [18]. Among a large number of open problems on determining or at least estimating $n(d, k)$ we single out the one of Delorme [7] to evaluate $\mu(k) = \limsup_{d \rightarrow \infty} n(d, k)/d^k = \limsup_{d \rightarrow \infty} n(d, k)/M(d, k)$ for every fixed $k \geq 2$.

The best currently known results on Delorme's problem are the author's own observations [7] stating that $\mu(k) = 1$ for $k \in \{2, 3, 5\}$. The idea behind the observations is to take polarity quotients of the incidence graphs of generalised n -gons that admit a polarity for $n \in \{3, 4, 6\}$, see [17]. Note, however, that these polarity graphs are not even regular,

albeit having rather large automorphism groups compared to their orders. As regards other diameters, results on the values of μ are much weaker but by no means trivial. It is known [8] that $\mu(4) \geq 1/4$, and from [5] one can extract the bound $\mu(k) \geq (1.6)^{-k}$ for $k \geq 6$.

From a practical point of view, generation of record large graphs of given degree and diameter (at both theoretical and computational levels) is almost exclusively limited to Cayley graphs or vertex-transitive graphs in cases when the degree or diameter are beyond values manageable by other methods; cf. [14] and the on-line tables [22]. It is therefore natural to ask about the value of Delorme's limit superior when restricted to Cayley (or at least to vertex-transitive) graphs. The extreme case here would arise if the Moore bound can be *asymptotically approached*, in the sense of Delorme's limit superior being equal to 1, by Cayley graphs.

Formally, for $d \geq 3$ and $k \geq 2$ we let $vt(d, k)$ and $C(d, k)$ denote the largest order of a vertex-transitive and a Cayley graph, respectively, of degree d and diameter k ; clearly, $vt(d, k) \geq C(d, k)$. By non-trivial results of [10], the difference $M(d, k) - vt(d, k)$ can be arbitrarily large. More precisely, by [10] for any fixed degree $d \geq 3$ and any given positive integer t one has $vt(d, k) \leq M(d, k) - t$ for asymptotically almost all diameters k ; moreover, for every fixed $d \geq 3$ there exists an infinite sequence of diameters k such that $vt(d, k) \leq M(d, k) - k^{1/(2+o(1))}$ as $k \rightarrow \infty$. We point out that no results of such kind are available for the difference $M(d, k) - n(d, k)$ in general.

Returning to Delorme's limit superior, the call now is to evaluate or at least estimate the values of $\limsup_{d \rightarrow \infty} vt(d, k)/M(d, k)$ and $\limsup_{d \rightarrow \infty} C(d, k)/M(d, k)$ for $k \geq 2$ in general and for $k \in \{2, 3, 5\}$ in particular. For general d and k the results available here are scarcer and, expectedly, not as good as those for $n(d, k)$. In the vertex-transitive case, ignoring edge directions in the digraphs of [11] yields $\lim_{d \rightarrow \infty} vt(d, k)/M(d, k) \geq 2^{-k}$ for every $k \geq 3$. For Cayley graphs, constructions of [15, 16] give $\lim_{d \rightarrow \infty} C(d, k)/M(d, k) \geq k \cdot 3^{-k}$ for every $k \geq 3$, with improvements of the lower bounds by [21] to $3 \cdot 2^{-4}$, $32 \cdot 5^{-4}$ and $25 \cdot 4^{-5}$ for $k = 3, 4$ and 5 , respectively.

For $k \in \{2, 3\}$, however, it was recently shown that $\limsup_{d \rightarrow \infty} C(d, k)/M(d, k) = 1$, meaning that the Moore bound for diameter 2 and 3 can be asymptotically approached by Cayley graphs. This was proved for $k = 2$ in [20] using Cayley graphs of one-dimensional affine groups over finite fields of characteristic 2; the construction was then shown in [2] to be equivalent with extending a suitable regular orbit of a polarity quotient of the incidence graph of a generalised triangle. The result for $k = 3$ was proved in [1] by a non-trivial adaptation of the method of [2] to polarity quotients of incidence graphs of generalised quadrangles, with an outline of reasons why such an approach is not likely to give an analogous result for diameter 5 from polarity graphs of generalized hexagons.

In this paper we present a general result underpinning both the above constructions and indicate how the results of [20] and [1] about Cayley graphs approaching the Moore bound for diameters 2 and 3 can be derived from this general principle using graphs associated with finite geometries.

2 The result

As explained in the Introduction, our aim is to show that the results of [20] and [1] about asymptotically approaching the Moore bound for diameter 2 and 3 by Cayley graphs are based on a certain underpinning principle which we now present and prove.

Theorem 1 *Let Γ be a graph of diameter $k \geq 2$ and maximum degree d , satisfying the following assumptions:*

- (1) *there is a group G acting on the vertex set V of Γ in such a way that G is regular on some orbit $O \subset V$;*
- (2) *every vertex $v \in V \setminus O$ adjacent to a vertex in O has a vertex stabiliser in G that acts regularly on the neighbours of v in Γ contained in O ; and*
- (3) *there exists a $\delta > 0$ with the property that for arbitrary vertices $u, v \in O$ there is a shortest $u - v$ path P in Γ such that every vertex of P has at least $d - \delta$ neighbours in O .*

Then, letting $\gamma = \gamma(\delta, k) = \delta + \delta(\delta - 1) + \dots + \delta(\delta - 1)^{k-2}$, there exists a Cayley graph $C(G, S)$ of diameter at most k and degree $|S| \leq d - \delta + \gamma(5\sqrt{d} + 2)$.

Proof. Let Λ be the subgraph of Γ induced by the vertex set O . By our assumption (1) and the classical result of [19], the graph Λ is isomorphic to a Cayley graph $C(G, X)$ for some generating set $X \subset G$. The assumption (3) applied to $u = v$ implies that the degree $|X|$ of Λ is at least $d - \delta$. For checking distances in the Cayley graph $\Lambda \simeq C(G, X)$ it is, of course, sufficient to consider shortest paths from a fixed vertex, say, $u \in O$, to all other vertices. Having fixed u , we will also be tacitly using the isomorphism from $C(G, X)$ onto Λ given by $g \mapsto ug$ for $g \in G$. In what follows we will extend X by a ‘small’ set Y in such a way that for any $v \in O$ for which every shortest $u - v$ path in Γ contains at least one vertex from $V \setminus O$ we will be able to find a $u - v$ path of length at most k in the Cayley graph $C(G, X \cup Y)$.

Before proceeding we establish some terminology. Let us call a vertex v of Γ *tame* if it is incident to at least $d - \delta$ vertices from O . Also, let us call a vertex $v \in O$ *critical* if every shortest $u - v$ path in Γ contains at least one vertex from outside O . By the assumption (3), for every critical vertex v there is a shortest $u - v$ in Γ with all vertices tame; among all such paths let P_v be one with the largest number of vertices outside O . A vertex $v \in O$ will be said to be *strongly critical* if all vertices of P_v distinct from u and v (the inner vertices of P_v) lie outside O . Observe that if there were no critical vertices in O , then the statement of our theorem would be vacuously true. We therefore assume the existence of at least one critical, and a fortiori at least one strongly critical, vertex.

Consider the subgraph W of Γ arising as a union of the paths $P_v - \{u, v\}$ obtained by removal of the end-vertices u and v , ranging over all strongly critical vertices v . By (3), every vertex of W is adjacent to at most δ vertices in W , and u itself is adjacent to at most

δ vertices in W . Since the truncated paths $P_v - \{u, v\}$ have length at most $k - 2$, it follows that the number of vertices of W is at most $\gamma = \gamma(\delta, k) = \delta + \delta(\delta - 1) + \dots + \delta(\delta - 1)^{k-2}$.

For every $w \in W$ let $N_O(w)$ denote the set of neighbours of w in O . By the assumptions (2) and (3), the stabiliser H_w of the vertex w in G has order at most d and acts regularly on $N_O(w)$. By a general result of [13] on the so-called 2-bases in general groups, the group H_w admits a symmetric unit-free generating set S_w with $|S_w| \leq 5\lceil\sqrt{d}\rceil$ such that the Cayley graph $C(H_w, S_w)$ has diameter 2. Let Y_1 be the union of the sets $S_w \subset G$ taken over all $w \in W$. Further, for each $w \in W$ not adjacent to u choose a vertex $v_w \in N_O(w)$ and let $g_w \in G$ be the (unique) element for which $v_w = ug_w$. Let Y_2 be the union of the sets $\{g_w, g_w^{-1}\}$ taken over all $w \in W$ that are not adjacent to u . Finally, let $Y = Y_1 \cup Y_2$ and $S = X \cup Y$.

Our aim is to show that the Cayley graph $C(G, S)$ has diameter at most k . To prove this it is sufficient to check distances $d_\Gamma(u, v)$ in the graph Γ and $d_C(u, v)$ in the graph $C(G, S)$ between u and the critical vertices $v \in O$. We begin by considering an arbitrary strongly critical vertex v . If $v \in N_O(w)$ for some $w \in W$ such that w is adjacent to u , then the distance between $d_C(u, v) \leq 2$ since the Cayley graph $C(H_w, S_w)$ is now a subgraph of $C(G, S)$. If $v \in N_O(w)$ for some $w \in W$ such that w is not adjacent to u , we have $d_\Gamma(u, v) \geq 3$, but $d_C(u, v) \leq 3$. Namely, for our w such that $v \in N_O(w)$, the vertex u is adjacent to v_w because $g_w \in S$, and $d_C(v_w, v) \leq 2$ because the Cayley graph $C(H_w, S_w)$ is a subgraph of $C(G, S)$.

Let now v be a critical but not strongly critical vertex of O and suppose that P_v is a path from u to v of the form $P_v = uPxQyRv$ for some paths P and R lying entirely outside O and a path xQy in Λ . From our way of choosing the paths P_v we may assume that $uPx = P_x$ and $yRv = (P_z)g$ for $z = vg^{-1}$, where g is the (unique) element of G such that $ug = y$. Both x and y are strongly critical, and so by the conclusion made in the above paragraph $d_\Gamma(u, x) \geq d_C(u, x)$ and $d_\Gamma(u, z) \geq d_C(u, z)$. But since $ug = y$ and $zg = v$, we have $d_\Gamma(u, z) = d_\Gamma(y, v)$ and $d_C(u, z) = d_C(y, v)$, and hence also $d_\Gamma(u, v) \geq d_C(u, v)$.

The fact that $d_\Gamma(u, v) \geq d_C(u, v)$ for any critical vertex in Γ follows now easily by induction. This proves that the diameter of $C(G, S)$ is at most k . For the degree $|S|$ of $C(G, S)$ we trivially have $|S| \leq |X| + |Y_1| + |Y_2| \leq d - \delta + 5\lceil\sqrt{d}\rceil\gamma + 2\gamma$. \square

3 Applications

In this section we show how Theorem 1 can be applied to reprove the results of [2, 20] and [1] about asymptotically largest currently known Cayley graphs of diameter 2 and 3 with the help subgraphs arising from polarity quotients of incidence graphs of finite projective planes (for $k = 2$) and of finite generalized quadrangles (for $k = 3$).

3.1 Cayley graphs of diameter 2

Polarity graphs, denoted here $B(q)$, of finite projective planes of prime-power order q , were first introduced in [9] and later independently in [4]. Let $F = GF(q)$ be the Galois field of order a prime power q and let $\text{PG}(2, q)$ denote the standard projective plane over F . The vertex set of the polarity graph $B(q)$ is the set of all the $q^2 + q + 1$ points of $\text{PG}(2, q)$ represented by projective triples, that is, equivalence classes $[a]$ of triples $a = (a_1, a_2, a_3) \neq (0, 0, 0)$ of elements of F , two such triples being equivalent if and only if one is a non-zero multiple of the other. Two distinct vertices $[a]$ and $[b]$, where $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$, are adjacent in $B(q)$ if and only if $a_1b_1 + a_2b_2 + a_3b_3 = 0$. Simple linear algebra arguments imply that the degree of a vertex $[a]$ of $B(q)$ is equal to q or $q + 1$ according to whether $a_1^2 + a_2^2 + a_3^2$ is equal to zero or not, and that the diameter of $B(q)$ is equal to 2.

Although the graphs $B(q)$ are defined for every power $q = p^n$ of an arbitrary prime p , it turns out that they admit a subgroup G of the automorphism group $\text{Aut}(B(q))$ required in the statement of Theorem 1 only for $p = 2$, that is, for $q = 2^n$ for any $n \geq 1$. Assuming that $q = 2^n$ in what follows, we have $a_1^2 + a_2^2 + a_3^2 = (a_1 + a_2 + a_3)^2$ and consequently a vertex $[a]$ in $B(2^n)$ has degree q or $q + 1$ if $a_1 + a_2 + a_3 = 0$ or not. Thus, the set W of all the $q + 1$ vertices of $B(2^n)$ of degree q is $W = \{[1, a, a + 1]; a \in F\} \cup \{[0, 1, 1]\}$. The group $\text{Aut}(B(q))$ is isomorphic to $\text{P}\Gamma\text{O}(3, q)$, an extension of the projective orthogonal group $\text{PGO}(3, q)$ by the group $\text{Gal}(F)$ of all Galois automorphisms of F . For $q = 2^n$ all elements of $\text{PGO}(3, q)$ have the form

$$M(a, b, c, d) = \begin{pmatrix} 1 + a & 1 + c & 1 + a + c \\ 1 + b & 1 + d & 1 + b + d \\ 1 + a + b & 1 + c + d & 1 + a + b + c + d \end{pmatrix}$$

where $a, b, c, d \in F$ are such that $ad + bc = 1$; this group acts on vertices of $B(q)$ represented as *column* vectors by left multiplication.

Still assuming that $q = 2^n$, let G be the subgroup of $\text{PGO}(3, q)$ formed by all the matrices $M(a, b, c, d)$ such that $a + b + c + d = 0$; it can be shown that $|G| = q(q - 1)$. Let V_0 denote the set of all vertices of $B(q)$ of degree $q + 1$ and let $O = V_0 \setminus \{[t, t, 1]; t \in F\}$; note that $|O| = q(q - 1)$. We proceed by indicating the steps towards showing that the graph $\Gamma = B(2^n)$ of diameter 2 and maximum degree $2^n + 1$ together with the group G and the set O satisfy the assumption (1) – (3) of Theorem 1 and refer to [2] for details.

The assumption (1) holds true since G can be shown to have a regular action on the set $O \subset V$. Further, one may check that every vertex $v \in V \setminus O$ adjacent to a vertex in O has a vertex stabiliser in G that acts regularly on the neighbours of v contained in O , which is the assumption (2) of Theorem 1. Finally, the assumption (3) of Theorem 1 is also easily seen to be satisfied for $d = q + 1$ and $\delta = 2$. An evaluation of $\gamma = \gamma(\delta, k) = \delta + \delta(\delta - 1) + \dots + \delta(\delta - 1)^{k-2}$ for $k = 2$ and $\delta = 2$ gives $\gamma = 2$. Hence by Theorem 1 we obtain the existence of a Cayley graph $C(G, S)$ of order $|G| = (d - 1)(d - 2)$, diameter 2 and degree $|S| \leq d + 10\sqrt{d} + 2$ for every d of the form $d = 2^n + 1$, $n \geq 1$, giving rise to a family

of Cayley graphs of diameter 2 and orders asymptotically approaching the corresponding Moore bound as in [20, 2]. (The bound on $|S|$ given here is only slightly worse than the one of [20] in the $O(\sqrt{d})$ term, which is due to a larger generality of our Theorem 1.)

3.2 Cayley graphs of diameter 3

In the case of diameter 3 we construct, for every q of the form $q = 2^{2n+1}$, $n \geq 1$ a graph $A(q)$ as follows (we only include a brief description here and refer to [1] for many more details). Again, let $F = GF(q)$. The vertex set V of $A(q)$ will this time consist of all points of the projective geometry $PG(3, q)$ represented by projective triples $[x_0, x_1, x_2, x_3] \neq [0, 0, 0, 0]$ of elements of F . Adjacency in $A(q)$, however, is given by a more complicated rule than in the previous construction and we describe it next.

Let $\omega = 2^{n+1}$. A vertex $u = [x] = [x_0, x_1, x_2, x_3]$ will be adjacent to precisely the vertices $v = [y] \neq [x]$ that are points on the line of $PG(3, q)$ spanned by the vectors

$$(0, c^{\omega/2}, x_0^{\omega}, x_2^{\omega}), (c^{\omega/2}, 0, x_3^{\omega}, x_1^{\omega}), (x_0^{\omega}, x_3^{\omega}, 0, c^{\omega/2}), \text{ and } (x_2^{\omega}, x_1^{\omega}, c^{\omega/2}, 0)$$

where $c = x_0x_1 + x_2x_3$. Let G be the group formed by the set of matrices $M(r; a; b)$ given by

$$M(r; a; b) = \begin{pmatrix} 1 & f(a; b) & a & b \\ 0 & r^{\omega+2} & 0 & 0 \\ 0 & (a^{\omega+1} + b)r & r & a^{\omega}r \\ 0 & ar^{\omega+1} & 0 & r^{\omega+1} \end{pmatrix}$$

for all $r \in F^* = F \setminus \{0\}$ and $a, b \in F$, where $f(x; y) = x^{\omega+2} + xy + y^{\omega}$. The group G has order $q^2(q-1)$ and acts on $A(q)$ as a group of automorphisms by right multiplication. Following the calculations in [1] one finds that the graph $A(q)$ has diameter 3 and maximum degree $d = q + 1$. Moreover, a detailed analysis of [1] reveals that the group G acts on the graph $A(q)$ with exactly the following five orbits $O_1 - O_5$:

- $O_1 = \{[1, f(x, y), x, y]; x, y \in F\}$, of size q^2 ;
- $O_2 = \{[0, x, 1, y]; x, y \in F\}$, of size q^2 ;
- $O_3 = \{[0, x, 0, 1]; x \in F\}$, of size q ;
- $O_4 = \{[0, 1, 0, 0]\}$, the unique fixed point of G ; and
- $O_5 = V \setminus (O_1 \cup O_2 \cup O_3 \cup O_4)$, of size $q^2(q-1)$.

It follows that G , being a regular permutation group on the orbit $O = O_5$, satisfies the assumption (1) of Theorem 1. An analysis of stabilizers of vertices $v \in V \setminus O$ adjacent to vertices in $O = O_5$ shows that the condition (2) of Theorem 1 is fulfilled. Finally, by a thorough study of incidence of certain vertices of $A(q)$, rather involved details of which we omit, it follows that the condition (3) of Theorem 1 holds true for $\delta = 2$. For $k = 3$ and $\delta = 2$ we obtain $\gamma = 4$ and hence, by Theorem 1, there exists a Cayley graph $C(G, S)$ of order $q^2(q-1) = (d-1)^2(d-2)$, diameter 3 and degree $|S| \leq d + 20\sqrt{d} + 6$ for every d

of the form $d = 2^{2n+1} + 1$, $n \geq 1$. This gives a family of Cayley graphs of diameter 3 that asymptotically approaches the corresponding Moore bound as in [1]. Again, our bound on $|S|$ here differs from the one of [1] only in the slightly worse $O(\sqrt{d})$ term because of application of a more general result (our Theorem 1).

These applications suggest looking for further instances of graphs and subgroups of their automorphism groups satisfying the assumptions of Theorem 1, even in cases when Delorme's limit superior will be smaller than one but comparable to, or larger than, the estimates summed up in the Introduction.

Acknowledgement. All three authors acknowledge support from the research grants APVV 0136/12, APVV-15-0220, VEGA 1/0026/16, and VEGA 1/0142/17.

References

- [1] M. Bachratý, J. Šiagiová and J. Širáň, Asymptotically approaching the Moore bound for diameter three by Cayley graphs, submitted (2015).
- [2] M. Bachratý and J. Širáň, Polarity graphs revisited, *Ars Math. Contemp.* 8 (2015), 55–67.
- [3] E. Bannai and T. Ito, On finite Moore graphs, *J. Fac. Sci. Tokyo Univ.* 20 (1973), 191–208.
- [4] W. G. Brown, On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.* 9 (1966), 281–285.
- [5] E. A. Canale and J. Gómez, Superfluous edges and exponential expansions of deBruijn and Kautz digraphs, *Discrete Applied Math.* 138 (2004), 303–331.
- [6] R.M. Damerell, On Moore graphs, *Proc. Cambridge Phil. Soc.* 74 (1973), 227–236.
- [7] C. Delorme, Large bipartite graphs with given degree and diameter, *J. Graph Theory* 8 (1985), 325–334.
- [8] C. Delorme, Examples of products giving large graphs with given degree and diameter, *Discrete Applied Mathematics* 37/38 (1992), 157–167.
- [9] P. Erdős and A. Rényi, On a problem in the theory of graphs, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* 7 (1962), 623–641.
- [10] G. Exoo, R. Jajcay, M. Mačaj and J. Širáň, The defect of vertex-transitive graphs of given degree and diameter, submitted (2014).

- [11] V. Faber, J. W. Moore and W. Y. C. Chen, Cycle prefix digraphs for symmetric interconnection networks, *Networks* 23 (1993), 641–649.
- [12] A. J. Hoffman and R. R. Singleton, On Moore graphs with diameter 2 and 3, *IBM J. Res. Develop.* 4 (1960), 497–504.
- [13] G. Kozma and A. Lev, Bases and decomposition numbers for finite groups, *Arch. Math.* 58 (1992), 417–424.
- [14] E. Loz and J. Širáň, New record graphs in the degree-diameter problem, *Australasian J. Combin.* 41 (2008), 63–80.
- [15] H. Macbeth, J. Šiagiová and J. Širáň, Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups, *Discrete Math.* 312 (2012), 94–99.
- [16] H. Macbeth, J. Šiagiová, J. Širáň and T. Vetrík, Large Cayley graphs and vertex-transitive non-Cayley graphs of given degree and diameter, *J. Graph Theory* 64 (2010), 87–98.
- [17] H. van Maldeghem, ‘Generalized polygons’, Birkhäuser, 1998, 502 pp.
- [18] M. Miller and J. Širáň, Moore graphs and beyond: A survey of the degree/diameter problem, *Electr. J. Combin.* 20 (2) (2013), Dynamic Survey DS14v2, 92 pp.
- [19] G. Sabidussi, On a class of fixed-point free graphs, *Proc. Amer. Math. Soc.* 9 (1958), 800–804.
- [20] J. Šiagiová, J. Širáň, Approaching the Moore bound for diameter two by Cayley graphs, *J. Combin. Theory Ser. B* 102 (2012), 470–473.
- [21] T. Vetrík, Cayley graphs of given degree and diameters 3, 4 and 5, *Discrete Math.* 313 (2013), 213–216.
- [22] On-line tables of the current largest graphs for the degree-diameter problem: combinatoricswiki.org/wiki/The_Degree_Diameter_Problem_for_General_Graphs