Large graphs of diameter two and given degree

Jozef Širáň
Open University, Milton Keynes
Slovak University of Technology, Bratislava

Jana Šiagiová and Mária Ždímalová
Slovak University of Technology
Bratislava

Abstract

Let $r(d,2)$, $C(d,2)$, and $AC(d,2)$ be the largest order of a regular graph, a Cayley graph, and a Cayley graph of an Abelian group, respectively, of diameter 2 and degree d. The best currently known lower bounds on these parameters are $r(d,2) \geq d^2 - d + 1$ for $d-1$ an odd prime power (with a similar result for powers of two), $C(d,2) \geq (d+1)^2/2$ for degrees $d = 2q-1$ where q is an odd prime power, and $AC(d,2) \geq (3/8)(d^2-4)$ where $d = 4q-2$ for an odd prime power q.

Using a number theory result on distribution of primes we prove, for *all* sufficiently large d, lower bounds on $r(d,2)$, $C(d,2)$, and $AC(d,2)$ of the form $c \cdot d^2 - O(d^{1.525})$ for $c = 1$, $1/2$, and $3/8$, respectively. We also prove results of a similar flavour for vertex-transitive graphs and Cayley graphs of cyclic groups.

1 Introduction

The degree-diameter problem is to find, or at least give good estimates on, the largest order of a graph of given maximum degree and diameter. In a broader scope the problem also includes analysis and classification of the largest graphs of given degree and diameter that have been discovered. History and development of this area of research has been summed up in the relatively recent survey [16]. Despite numerous deep results there remain fundamental problems to be resolved, even for diameter two. We will concentrate on this case and refer the reader interested in higher diameters to [16].

For $d \geq 2$ let $n(d, 2)$ be the largest order of a graph of maximum degree d and diameter 2. The diameter requirement localized at a vertex v of degree d implies that any vertex of such a graph, distinct from v and not adjacent to v, must be one of the at most $d-1$ neighbours of some neighbour of v. This implies the bound $n(d, 2) \leq 1 + d + d(d-1) = d^2 + 1$, known as the *Moore bound* for diameter two. By the landmark result of Hoffman and Singleton [10] who initiated research into the degree-diameter problem, the equality $n(d, 2) = d^2 + 1$ holds if and only if $d = 2$, 3, 7, and possibly 57. The corresponding unique extremal graphs, that is, the Moore graphs of diameter two, are the pentagon, the Petersen graph, and the Hoffman-Singleton graph; the existence of a Moore graph of degree 57 is still in doubt. For all the remaining degrees d we have $n(d, 2) \leq d^2 - 1$ by [7].

The best lower bound on $n(d, 2)$ comes from the graphs constructed by Brown [3] and reads $n(d, 2) \geq d^2 - d + 1$ for all degrees d such that $d-1$ is an odd prime power. It was later observed in [5] and [7] that Brown's graphs can be extended by one vertex if $d-1$ is a power of 2, giving $n(d, 2) \geq d^2 - d + 2$ in this special case. Thus, at least for degrees closely related to prime powers, $n(d, 2)$ is asymptotically d^2.

Since Brown's graphs are not regular while the Moore graphs are, it is of interest to ask about a 'regular' version of the degree-diameter problem. As there are no regular graphs of odd order and odd degree, we also allow, but only for odd d, graphs of odd order with a single vertex of degree $d-1$ and all the remaining vertices of degree d; such graphs will be referred to as *almost regular* of degree d. Let now $r(d, 2)$ denote the largest order of a regular or an almost regular graph of degree $d \geq 2$ and diameter 2. Obviously $n(d, 2) \geq r(d, 2)$ but it is not clear at all whether equality holds, say, for some infinite set of degrees.

Observe that all the known Moore graphs of diameter two are not only regular but vertex-transitive as well. In contrast with this, a result of Higman (presented in [4]) says that if a graph of degree $d = 57$, diameter 2, and order $d^2 + 1 = 3250$ exists, it is not vertex-transitive. For the interest of the reader, the currently known best upper bounds on the order of this hypothetical graph can be found in [13]. This has generated interest in the parameter $vt(d,2)$ defined as the largest order of a vertex-transitive graph of degree $d \geq 2$ and diameter 2. By the above result we have $vt(d,2) = d^2+1$ for $d \in \{2,3,7\}$ and $vt(d,2) \leq d^2-1$ for all other degrees, including 57. The best available lower bound [15] in this case is $vt(d,2) \geq (8/9)(d+1/2)^2$ for all degrees of the form $d = (3q-1)/2$ where q is a prime power such that $q \equiv 1 \bmod 4$.

A special class of vertex-transitive graphs are Cayley graphs. Given a finite group G with a unit-free generating set S such that $S = S^{-1}$, the *Cayley graph* $Cay(G,S)$ has vertex set G and a pair of vertices $g, h \in G$ are adjacent 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 $G \backslash S$ is a product of two elements from S. We note that the graphs of [15] giving the lower bound at the end of the previous paragraph are vertex-transitive but not Cayley.

To further refine the analysis, for an arbitrary integer $d \geq 2$ 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. For $d = 2$ the three invariants have value 5, and from results summed up in [16] 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 constructions providing lower bounds which, as it appears, 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 [18]. 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 [14]. By [16] the only known lower bound valid for *all* degrees $d \geq 3$ is the folklore inequality $C(d,2) \geq AC(d,2) \geq CC(d,2) > d^2/4$. The values of $C(d,2)$ for $d \leq 20$ found with the help of computers can be looked up in the tables [19].

Our aim is to extend, at least in the asymptotic sense, the above best bounds on $n(d,2)$, $vt(d,2)$, $C(d,2)$, $AC(d,2)$, and $CC(d,2)$ from the very restricted sets of degrees related to prime powers to *arbitrary* degrees. The basis of our considerations is a number theory result of [2] about gaps between consecutive primes. Details, given in Section 3, are straightforward for Cayley graphs, less obvious for regular graphs, and non-trivial for vertex-transitive non-Cayley graphs.

For completeness we remark that interest in large Cayley graphs and digraphs of given diameter and degree has also been motivated by problems in group theory and theoretical computer science. Group theory connections via the concept of a basis of a group have been outlined in [14] and for links with design of interconnection networks we refer to [16]. Importance of Cayley graphs in computer generation of record large graphs of manageable degree and diameter is well known [16] and emphasized also by the recent results of [12] which led to rewriting the tables of current largest graphs kept in [19].

2 A review of two constructions

To make our explanations self-contained we begin with giving some details about the graphs of Brown [3] and McKay-Miller-Širáň [15].

For any prime power q the graph $B(q)$ of Brown has vertex set all the $q^2 + q + 1$ points of a finite projective plane over the Galois field $GF(q)$. In other words, vertices of $B(q)$ are equivalence classes $[a, b, c]$ of triples $(a, b, c) \neq (0, 0, 0)$ of elements of $GF(q)$, where two triples are equivalent if they are a non-zero multiple of each other. Two distinct vertices $[a, b, c]$ and $[a', b', c']$ are adjacent in $B(q)$ if and only if the triples are orthogonal, that is, if $aa' + bb' + cc' = 0$. In the terminology of projective geometry this means that vertices $[a, b, c]$ and $[a', b', c']$ are adjacent if and only if the point $[a, b, c]$ lies on the line with homogeneous coordinates $[a', b', c']$. The vertex set of $B(q)$ may also be identified with one-dimensional subspaces of a three-dimensional linear space over $GF(q)$, with adjacency defined by orthogonality of the subspaces. We remark that Brown's graphs are isomorphic to the graphs of [8] and a polarity version of this construction was given in [1].

The structure of Brown's graphs is known to a great detail and most of the few facts we need for our analysis can be easily verified by elementary linear algebra. Determination of the neighbours of a vertex $[a, b, c]$ of $B(q)$ amounts to classify solutions (x, y, z) of the linear equation $ax+by+cz = 0$. Apart from $(0, 0, 0)$ this equation has $q^2 - 1$ non-zero solutions representing $(q^2 - 1)/(q - 1) = q + 1$ distinct projective points, which are different from $[a, b, c]$ if and only if $a^2 + b^2 + c^2 \neq 0$. Thus, a vertex $[a, b, c]$ has q or $q + 1$

neighbours according to whether $a^2 + b^2 + c^2$ is equal to zero or not. The number of vertices of degree q is then equal to the number of self-orthogonal projective points (those for which $a^2 + b^2 + c^2 = 0$), which is known to be equal to $q+1$, see e.g. [1]. Further, for any two distinct vertices $u = [a, b, c]$ and $v = [a', b', c']$ the system $ax+by+cz = 0$ and $a'x+b'y+c'z = 0$ consists of two linearly independent equations and hence has a one-dimensional solution space which, apart from the zero solution, represents a projective point, that is, a unique vertex w of $B(q)$. If $w \in \{u, v\}$, then u and v are adjacent and exactly one of them is represented by a self-orthogonal triple (if both u and v were represented by self-orthogonal triples then the system would have two linearly independent solutions (a, b, c) and (a', b', c'), a contradiction), and if $w \notin \{u, v\}$ then w is the unique vertex adjacent to both u and v in $B(q)$.

This discussion shows that the vertex set of $B(q)$ is a disjoint union of two sets for which we now reserve the symbols V and W, where vertices in V and W have degree $q+1$ and q, respectively, with $|V| = q^2$ and $|W| = q+1$. Further, the above arguments imply that the subgraph of $B(q)$ induced by the set W is edgeless, every pair of distinct vertices of W is connected by a unique path of length two, every edge joining two vertices of V lies in a unique triangle, while no edge joining a vertex of V with a vertex of W is contained in any triangle. In particular, $B(q)$ has diameter 2, and since its maximum degree is $q + 1$, we have $n(d, 2) \geq q^2 + q + 1 = d^2 - d + 1$ for $d = q + 1$.

Since $|W| = q + 1$, for any odd q we may extend $B(q)$ by an arbitrary perfect matching M between the (even number of) vertices in W and form thus a new graph $B^*(q)$. Since $B^*(q)$ is regular of degree $q+1$ and still has diameter 2, we have $r(d, 2) \geq d^2 - d + 1$ for $d = q + 1$ where q is an odd prime power. When q is a power of 2 it turns out that all the $q+1$ vertices of degree q in $B(q)$ have the form $[a, b, a+b]$ for $a, b \in GF(q)$ and hence are all joined to the vertex $[1, 1, 1]$ of degree $q+1$. In this case we use a different type of extension of $B(q)$ to a regular graph, pointed out in [5, 7]. Namely, we extend $B(q)$ by a new vertex incident to the $q+1$ vertices of degree q and denote the resulting regular graph $B^*(q)$, again. This way of adding the new vertex does not change the diameter and therefore $r(d, 2) \geq d^2 - d + 2$ for q a power of 2.

Although the extended graphs of Brown lead to very good lower bounds on $r(d, 2)$ when $d - 1$ is a prime power, they cannot be used for bounds on

$vt(d,2)$ for the same degrees, as we show next.

Proposition 1 *The extended Brown's graphs $B^*(q)$ are not vertex-transitive for any prime power q.*

Proof: The result is straightforward if q is a power of 2, since in this case it can be checked that $B^*(q)$ contains exactly two distinct vertices with identical neighbours.

Now, let q be odd. We will borrow the notation introduced earlier together with the facts about Brown's graphs derived above. We saw there that any pair of vertices in W is connected by exactly one path of length two. Thus, at most $(q+1)q/2$ vertices in V are adjacent to at least one vertex from W (in fact, by a refined argument it can be shown that there are exactly $(q+1)q/2$ such vertices but we will not need this here). This means that there is at least one vertex in V, say, v, not joined to any vertex in W. Since every edge joining two vertices of V lies in a unique triangle, the subgraph of $B(q)$ induced by all the neighbours of v is isomorphic to a matching of $(q+1)/2$ edges. Recall also that no edge incident to a vertex in W is contained in any triangle of $B(q)$. It follows that no matter how $B(q)$ is extended to $B^*(q)$ by a matching M between vertices of W, the subgraph of $B^*(q)$ induced by the set of all neighbours of any vertex $w \in W$ contains just one edge, namely, the edge $w'v'$ where $w' \in W$ is the unique vertex for which $ww' \in M$ and $v' \in V$ is the unique vertex adjacent to both w and w'. We conclude that the graphs $B^*(q)$ are never vertex-transitive. □

The current largest *vertex-transitive* graphs of diameter 2, at least for a certain degrees, are the graphs of McKay-Miller-Širáň [15]; they have also been described in two different but equivalent ways in [17] and [9]. Keeping to the original description, let q be an arbitrary prime power such that $q \equiv 1 \bmod 4$ and let $F = GF(q)$. Let X be the set of all non-zero squares in F. Let $M(q)$ be the graph of order $2q^2$ with vertex set $V_0 \cup V_1$ where, for $r \in \{0,1\}$, the set V_r consists of triples (i,k,r) with $i,k \in F$. Every vertex (i,k,r) is adjacent to the q vertices $(j, k+(-1)^r ij, 1-r)$ for all $j \in F$, as well as to the $(q-1)/2$ vertices of the form $(i, k+\xi^r x, r)$ for all $x \in X$, with no other adjacency. It was proved in [15] that the graphs $M(q)$ are vertex-transitive (and non-Cayley) graphs of diameter 2. Since they have degree $d = (3q-1)/2$ and order $2q^2$, for such degrees d we have $vt(d,2) \geq (8/9)(d+1/2)^2$.

The full automorphism group of the graphs $M(q)$ was determined in [9]. In what follows we will just need information about certain subgroups of this group, which we collect from [15] and [17]. For any $s, t \in F$ the mapping $f_{s,t}$ given by

$$f_{s,t}(i, k, r) = (i + s, k + t - (-1)^r (is + s^2/2), r)$$

is an automorphism of $M(q)$. It can be checked that the collection of all such mappings forms a group H isomorphic, via the bijection $f_{s,t} \mapsto (s, t)$, to the direct product $F^+ \times F^+$ where F^+ is the additive group of F. Moreover, H acts regularly on both V_0 and V_1.

In order to introduce more automorphisms, let n be the largest integer such that 2^n divides $q - 1$ and let $q - 1 = 2^n(2\ell + 1)$. Letting $\lambda = \xi^{2\ell+1}$ one sees that λ has order 2^n in the multiplicative group F^* of the field F. It follows from [15] that the mapping g given by

$$g(i, k, r) = ((-\xi)^{\ell+r} i, \lambda k, 1 - r)$$

is an automorphism of the graph $M(q)$ interchanging V_0 and V_1. The group G generated by g and all the $f_{s,t}$ is a group of automorphisms of $M(q)$, transitive on the vertex set of this graph. We will not need any structural information about G later on.

3 Results

We are now ready to state and prove our main result.

Theorem 2 *We have the following lower bounds:*

(1) $n(d, 2) \geq r(d, 2) \geq q^2 + q + 1$ *for all* $d \geq 4$*, with* q *being the largest odd prime power such that* $q \leq d - 1$*,*

(2) $vt(d, 2) \geq 2q^2$ *for all odd* $d \geq 5$*, where* q *is the largest prime power such that* $q \equiv 5 \bmod 8$ *and* $(d + 1)/2 < q < (2d + 1)/3$*,*

(3) $C(d, 2) \geq 2q^2$ *for all degrees* $d \geq 5$*, where* q *is the largest odd prime power such that* $q \leq (d + 1)/2$*,*

(4) $AC(d, 2) \geq 6q(q-1)$ *for all* $d \geq 10$*, with* q *being the largest odd prime power such that* $q \leq (d + 2)/4$*, and*

(5) *$CC(d,2) \geq 9p(p-1)$ for all degrees $d \geq 12$, where p is the largest prime such that $p \equiv 2 \bmod 3$ and $d/6 \leq p \leq (d+3)/5$.*

Proof: The essence of the method is to use the known results summed up in the previous two sections and extend the corresponding graphs appropriately. We assume throughout the proof that d and q (and p in the last case) satisfy the conditions listed above.

(1) Let q be an odd prime power as in the statement; by Chebyshev's theorem we have $(d-1)/2 < q \leq d-1$. Let $L = B^*(q)$ be an extended Brown's graph of degree $q+1$, diameter 2, and order q^2+q+1. The complement $\overline{L}$ of L has degree $\Delta = q^2-1$. Let $j = \lfloor (d-q-1)/2 \rfloor$, which means that $d = q+1+2j$ if d is even, and $d = q+1+2j+1$ if d is odd. Our strategy will be to extend L by j 2-factors of $\overline{L}$ if d is even, and by j 2-factors and a maximum matching coming from a Hamilton cycle of $\overline{L}$ if d is odd, to obtain a regular and an almost regular graph of degree d and diameter 2, respectively.

Observe that for $q \geq 3$ we have $\Delta > (q^2+q+1)/2$. By Dirac's theorem [6], the graph $\overline{L}$ contains a Hamilton cycle, say, C. The graph $\overline{L} \backslash E(C)$ has even degree and is therefore 2-factorable by the classical result of Petersen; let $F_1, \ldots, F_j$ be a collection of j pairwise edge-disjoint 2-factors of $\overline{L} \backslash E(C)$. If d is even, we let L' be the graph arising from L by putting in all the 2-factors F_i for $1 \leq i \leq j$. By our choice of j the graph L' is regular of degree d. If d is odd, let L' be obtained from L by putting in the 2-factors F_i for $1 \leq i \leq j-1$ together with a matching of $(q^2+q)/2$ edges taken from the Hamilton cycle C. The resulting graph L' is obviously almost d-regular. In both instances, L' has diameter 2 because (as a consequence of the inequality from Chebyshev's theorem) it is not complete and contains L as a spanning subgraph. This shows that $r(d,2) \geq q^2+q+1$ if q is the largest odd prime power not exceeding $d-1$, for any $d \geq 4$.

(2) We refer to the notation regarding the McKay-Miller-Širáň graph $M(q)$ introduced before the statement of this theorem. We will extend the graph $M(q)$ by adding new edges as follows. First, observe that the assumption $q \equiv 5 \bmod 8$ implies that $n = 2$ and $2\ell + 1 = (q-1)/4$, that is, λ is a non-square and $\lambda^2 = -1$. Let $Y \subset F$ be a set of non-squares closed under inverses, that is, $Y = -Y$, such that $|Y| = d - (3q-1)/2$; note that our assumptions imply that this number is positive, even, and smaller than $(q-1)/2$. Let us extend the graphs $M(q)$ by adding, at each vertex (i,k,r), a total of $|Y|$ new edges joining (i,k,r) to the vertices of

the form $(i, k + \lambda^r y, r)$ for all $y \in Y$. The resulting graph, denoted $M_Y(q)$, is regular of degree d and has diameter 2 because it contains $M(q)$ as a subgraph. More importantly, by a direct computation one can verify that the generators $f_{s,t}$ and g of the group G introduced above preserve all the added edges. This shows that G is transitive on vertices of $M_Y(q)$, which completes the proof of (2). As far as the assumption $(d+1)/2 < q < (2d+1)/3$ is concerned, we note that the value of $q = (2d+1)/3$ is taken care of by the McKay-Miller-Širáň graphs for all $q \equiv 1 \bmod 4$, while in the case $q = (d+1)/2$ we obtain the Cayley graphs of [18] which will appear in the next part of the argument.

(3) Let L be a Cayley graph of degree $2q-1$, diameter 2, and order $2q^2$, constructed in [18]. An inspection of the construction shows that the graph L is a Cayley graph $Cay(G, X)$ for a non-Abelian group G of order $2q^2$ containing q^2 involutions, and for an inverse-closed generating set X of size $2q-1$ containing q involutions. It is clearly possible to select additional inverse-closed set $Y \subset G$ disjoint from X such that Y contains $d - 2q + 1$ generators, including some odd number of involutions if d is even. This yields a Cayley graph $L' = Cay(G, X \cup Y)$ of degree d, diameter 2, and order $2q^2$. Consequently, $C(d, 2) \geq 2q^2$ for the largest odd prime power $q \leq (d+1)/2$.

(4) Let L be the Cayley graph $Cay(G, X)$ from [14] of diameter 2 for an Abelian group G of order $6q(q-1)$ that contains precisely 3 elements of order 2, where X is an inverse-closed generating set of size $4q-2$ containing exactly two elements of order 2. Let us select an additional inverse-closed set $Y \subset G$ disjoint from X such that Y contains $d-4q+2$ generators, including an involution if d is odd. Clearly, the Cayley graph $L' = Cay(G, X \cup Y)$ has degree d, diameter 2, and order $6q(q-1)$.

(5) Let L be a Cayley graph $Cay(G, X)$ for a cyclic group G of order $9p(p-1)$, degree $5p-3$ and diameter 2 with the single element of order 2 being outside the generating set X, as given in [14]. Choose an additional inverse-closed set $Y \subset G$ disjoint from X such that Y contains $d - 5p + 3$ generators, including the involution if d is odd. Clearly, the Cayley graph $L' = Cay(G, X \cup Y)$ has degree d, diameter 2, and order $9p(p-1)$. We only need to apply this process for primes p such that $p \geq d/6$ as otherwise we have a better bound $CC(d, 2) > d^2/4$ from [16]. □

Using a highly non-trivial number theory result on the distribution of primes it is possible to eliminate q from some of the bounds appearing in

Theorem 2. The roots of the result are in a still unresolved conjecture of Legendre on the existence of a prime between n^2 and $(n+1)^2$ for any positive integer n. Replacing $(n+1)^2$ with x and allowing any real $x \geq 2$ leads to a stronger form of the conjecture, stipulating that for any real $x \geq 2$ there is a prime p such that $x - 2\sqrt{x} + 1 < p \leq x$. The first result in this direction was given by Hoheisel [11] of which we just need a consequence saying that there exists a real number $\theta < 1$ such that the interval $[x - x^{\theta}, x]$ contains a prime number for any sufficiently large x. Clearly, the stronger form of Legendre's conjecture would follow, at least for sufficiently large x, if one could prove that $\theta < 1/2$ in Hoheisel's result. This has generated research towards making the exponent θ as small as possible. The current record is $\theta = 0.525$, established by Baker, Harman and Pintz [2]. That is, by [2], for any sufficiently large x there is a prime p such that $x - x^{0.525} \leq p \leq x$.

We will use this result of [2] to prove lower bounds on the order of the largest graphs of given degree and diameter 2 for all sufficiently large degrees.

Corollary 3 *For all sufficiently large degrees d we have:*

(a) $n(d,2) \geq r(d,2) > d^2 - 2d^{1.525}$,

(b) $C(d,2) > (1/2)d^2 - 1.39d^{1.525}$,

(c) $AC(d,2) > (3/8)d^2 - 1.45d^{1.525}$.

Proof: Let d be sufficiently large and let q be the largest odd prime power such that $q \leq D$ where D is equal to $d-1$, $(d+1)/2$, and $(d+2)/4$ according as we are in the case (a), (b), and (c). The result of [2] gives

$$q \geq D - D^{0.525} \tag{1}$$

and we will use this estimate in all three instances. In the case (a) when $D = d - 1$ we invoke the first part of Theorem 2 combined with (1) which, for all sufficiently large d, gives

$$r(d,2) \geq q^2 + q + 1 > (D - D^{0.525})^2 + D - D^{0.525} > d^2 - 2d^{1.525} \ .$$

If $D = (d+1)/2$, by the third part of Theorem 2 together with (1) we obtain

$$C(d,2) \geq 2q^2 \geq 2(D - D^{0.525})^2 > (1/2)d^2 - 2^{0.475}d^{1.525} > (1/2)d^2 - 1.39d^{1.525}$$

for all sufficiently large degrees d, which proves (b). In the case (c) when $D = (d+2)/4$ we combine the fourth part of Theorem 2 with (1), which yields

$$AC(d,2) \geq 6q(q-1) > 6(D - D^{0.525} - 1)^2 > (3/8)d^2 - 3 \cdot 4^{-0.525} d^{1.525} \ ,$$

that is, $AC(d,2) > (3/8)d^2 - 1.45d^{1.525}$ for all sufficiently large d. □

4 Remarks

The construction of the extended graphs of Brown together with Proposition 1 leads to the following interesting question. Given a graph G of maximum degree d, what is the smallest number $\delta = \delta_G$ such that there exists a vertex-transitive graph H of degree $d+\delta$ that contains G as a spanning subgraph? The problem is equivalent to finding a vertex-transitive spanning subgraph of largest degree in the complement of G. In this terminology, Proposition 1 says that $\delta_G > 0$ if $G = B^*(q)$, and it would be interesting to determine the value of δ_G in this case.

Our second remark concerns the number-theoretic approximation bound of [2]. Unfortunately, there appears to be no result on the existence of a prime *from a given congruence class* in the interval $[x - x^\theta, x]$ for some $\theta < 1$ and all sufficiently large x. If there was such a result, the proof of Corollary 3 would apply also to the cases (2) and (5) of Theorem 2 and we would obtain bounds on $vt(d,2)$ and $CC(d,2)$ of the form $(8/9)d^2 - O(d^{1+\theta})$ and $(9/25)d^2 - O(d^{1+\theta})$ for all sufficiently large odd degree d and general degree d, respectively.

In the vertex-transitive case we have stated part (2) of Theorem 2 just for $q \equiv 5 \bmod 8$ and odd degrees d. Recalling that n has been defined as the largest integer such that 2^n divides $q-1$, with $q - 1 = 2^n(2\ell + 1)$, our statement of (2) corresponds to the instance when $n = 2$. We can extended (2) to all $n \geq 2$ as follows:

(2') *If q is the largest prime power such that $q \equiv 2^n + 1 \bmod 2^{n+1}$ and $(d+1)/2 < q < (2d+1)/3$, then $vt(d,2) \geq 2q^2$ for all d of the form $d = (3q-1)/2 + 2^{n-1}m$ for $m \leq 2\ell$.*

Indeed, to establish (2'), the only change required in the proof of (2) is to take the set Y to be a union of m orbits of the permutation of F^* given by $y \mapsto \lambda^2 y$ consisting of non-squares. Such a more general version, however, does not appear as appealing as the simplest form for $n = 2$ that we have used in the presentation of part (2) of Theorem 2.

Finally, we remark that an analysis of the orbit structure of the group G of automorphisms of the McKay-Miller-Širáň graphs $M(q)$, introduced in the last paragraph of Section 2, shows that it is not possible to add an extra G-invariant perfect matching to $M(q)$ and hence extend the statement (2) of Theorem 2 to even degrees.

Acknowledgement

The authors acknowledge the support of this research by the VEGA Research Grants 1/0489/08 and 1/0280/10, the APVV Research Grants 0040-06 and 0104-07, and the APVV LPP Research Grants 0145-06 and 0203-06.

References

[1] M. Abreu, C. Balbuena and D. Labbate. Adjacency matrices of polarity graphs and of other C_4-free graphs of large size. *Des. Codes Cryptogr.*, 55:221-233, 2010.

[2] R. C. Baker, G. Harman and J. Pintz. The diference between consecutive primes. II. *Proc. London Math. Soc.*, 83:532–562, 2001.

[3] W. G. Brown. On graphs that do not contain a Thompsen graph. *Canad. Math. Bull.*, 9:281–285, 1996.

[4] P. J. Cameron. *Permutation Groups.* Cambridge Univ. Press, 1999.

[5] C. Delorme. Examples of products giving large graphs with given degree and diameter. *Discrete Applied Math.*, 37-38:157–167, 1992.

[6] G. Dirac. Some theorems on abstract graphs. *Proc. Lond. Math. Soc.*, 2:69–81, 1952.

[7] P. Erdös, S. Fajtlowicz and A.J. Hoffman. Maximum degree in graphs of diameter 2. *Networks*, 10:87–90, 1980.

[8] P. Erdös, A. Rényi, and V. T. Sós. On a problem of graph theory. *Stud. Sci. Math. Hung.*, 1:215-235, 1966.

[9] P. Hafner. Geometric realization of the graphs of McKay-Milller-Širáň. *J. Combin. Theory Ser. B*, 90:223–232, 2004.

[10] A. J. Hoffman and R. R. Singleton. On Moore graphs with diameters 2 and 3. *IBM J. Res. Dev.*, 4:497–504, 1960.

[11] G. Hoheisel. Primzahlprobleme in der Analysis. *S. Preuss. Ak. Wiss.*, 2:1–13, 1930.

[12] E. Loz and and J. Širáň. New record graphs in the degree-diameter problem. *Australas. J. Combin.*, 41:63–80, 2008.

[13] M. Mačaj and J. Širáň. Search for properties of the missing Moore graph. *Linear Algebra Appl.*, 432:2381-2398, 2010.

[14] H. Macbeth, J. Šiagiová and J. Širáň. Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups. *Submitted*, 2009.

[15] B.D. McKay, M. Miller and J. Širáň. A note on large graphs of diameter two and given maximum degree. *J. Combin. Theory Ser. B*, 74:110–118, 1998.

[16] M. Miller and J. Širáň. Moore graphs and beyond: A survey of the degree-diameter problem. *Electronic J. Combinat.*, Dynamic survey No. D14 (61pp), 2005.

[17] J. Šiagiová. A note on the McKay-Miller-Širáň graphs. *J. Combin. Theory Ser. B*, 81:205–208, 2001.

[18] J. Šiagiová and J. Širáň. A note on large Cayley graphs of diameter two and given degree. *Discrete Math.*, 305:379–382, 2005.

[19] On-line tables of the current largest graphs for the degree-diameter problem at `www.eyal.com.au/wiki/The_Degree/Diameter_Problem`.