Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 8 (2015) 55–67

Polarity graphs revisited

Martin Bachratý
Comenius University, Bratislava, Slovakia

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

Received 29 August 2013, accepted 2 March 2014, published online 22 April 2014

Abstract

Polarity graphs, also known as Brown graphs, and their minor modifications are the largest currently known graphs of diameter 2 and a given maximum degree d such that $d - 1$ is a prime power larger than 5. In view of the recent interest in the degree-diameter problem restricted to vertex-transitive and Cayley graphs we investigate ways of turning the (non-regular) polarity graphs to large *vertex-transitive* graphs of diameter 2 and given degree.

We review certain properties of polarity graphs, giving new and shorter proofs. Then we show that polarity graphs of maximum even degree d cannot be spanning subgraphs of vertex-transitive graphs of degree at most $d + 2$. If $d - 1$ is a power of 2, there are two large vertex-transitive induced subgraphs of the corresponding polarity graph, one of degree $d - 1$ and the other of degree $d - 2$. We show that the subgraphs of degree $d - 1$ cannot be extended to vertex-transitive graphs of diameter 2 by adding a relatively small non-edge orbital. On the positive side, we prove that the subgraphs of degree $d - 2$ can be extended to the largest currently known Cayley graphs of given degree and diameter 2 found by Šiagiová and the second author [*J. Combin. Theory Ser. B* **102** (2012), 470–473].

Keywords: Graph, polarity graph, degree, diameter, automorphism, group, vertex-transitive graph, Cayley graph.

Math. Subj. Class.: 05C25

E-mail addresses: mato4247@gmail.com (Martin Bachratý), j.siran@open.ac.uk (Jozef Širáň)

1 Introduction

A graph of diameter 2 and maximum degree d can have at most d^2+1 vertices. This can be seen by rooting the graph at a vertex of maximum degree and observing that the vertex set of the graph is the union of vertices at distance 0, 1 and 2 from the root, giving the estimate $1+d+d(d-1) = d^2+1$, also known as the Moore bound for diameter 2. Such a graph of order d^2+1 exists if and only if $d = 2, 3, 7$ and possibly 57, by the classical result of [9]. Examples for the first three degrees – the pentagon, the Petersen graph and the Hoffman-Singleton graph – are unique, and existence of a graph of diameter 2, degree 57 and order $57^2+1 = 3250$ is still an open problem. For all other values of $d \geq 4$ it is known [5] that the largest order of a graph of diameter 2 and maximum degree d is at most d^2-1, but by [11] examples of graphs of that order are known only for $d = 4, 5$. Investigation of large graphs of given degree and diameter in general is part of the well known degree-diameter problem, surveyed in [11].

If $d = q+1$ where q is prime power such that $q \geq 7$, the largest currently known order of a graph of diameter 2 and maximum degree d is d^2-d+1 if q is odd and d^2-d+2 if q is even. Examples of graphs of such order, missing the Moore bound only by d and $d-1$, are the polarity graphs $B(q)$ for odd q and their minor modifications for even q; both will be described in the next section. Extensions of polarity graphs by adding Hamilton cycles and maximum matchings taken from the complement were considered in [15] and give graphs of maximum degree d, diameter 2 and order at least $d^2-2d^{1.525}$ for every sufficiently large d. This shows that the Moore bound can be met at least asymptotically for *all* sufficiently large degrees.

The polarity graphs $B(q)$ were first introduced in 1962 by Erdős and Rényi [6] and later in 1966 independently by Brown [3] (and considered again by Erdős, Rényi and Sós [7]) in connection with asymptotic determination of the largest number of edges in a graph of a given order without cycles of length four. The notation $B(q)$ is derived from the fact that in the degree-diameter research community these graphs have also been known as Brown graphs after their second independent discoverer. Properties of polarity graphs have been studied in considerable detail in [12], including determination of the automorphism group of these graphs and their important subgraphs. Since polarity graphs are not regular, they cannot be vertex-transitive; nevertheless they have a relatively large automorphism group which has three orbits on vertices. The role of polarity graphs in the degree-diameter problem was realized later (cf. [11]) and their modification in the case when q is a power of two comes from [5] and [4].

In view of the recent advances in constructions of large vertex-transitive graphs with given degree and diameter [11] it is of interest to ask if one can modify polarity graphs to obtain large *vertex-transitive* graphs of a given degree and diameter 2 for an infinite set of degrees. We will consider modifications by inserting new edges into a polarity graph or into an induced subgraph of a polarity graph.

It is unclear if extending polarity graphs by Hamilton cycles and maximum matchings [15] can ever produce vertex-transitive graphs. In Section 4 we show that it is not possible to extend a polarity graph $B(q)$ for odd $q \geq 37$ to a vertex-transitive graph by increasing its maximum degree by two. Regarding subgraphs, the graph $B(q)$ for q a power of 2 contains two large vertex-transitive induced subgraphs, one of degree q and order q^2 and the other of degree $q-1$ and order $q(q-1)$. We prove that the first subgraph cannot be extended to a vertex-transitive graph of diameter 2 by adding non-edge orbitals induced by the smallest transitive group of automorphisms of the graph. In contrast with this, the second subgraph is shown to be isomorphic to the Cayley graph discovered in [14], which is extendable to a Cayley graph of diameter 2 and degree $d' + O(\sqrt{d'})$ for $d' = q - 1$ and which shows that the Moore bound for diameter 2 can be approached at least asymptotically. This equips the construction of [14] with a strong geometric flavour. Presentation of these results is preceded in Section 2 by a description of polarity graphs and their properties and in Section 3 by a study of symmetry properties of polarity graphs. In the final Section 5 we discuss possible generalizations.

2 Polarity graphs and their structure

Let q be a prime power and let $F = \mathrm{GF}(q)$ be the Galois field of order q. We let $\mathrm{PG}(2, q)$ denote the standard projective plane over F, with points 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, where two triples are equivalent if they are a non-zero multiple of each other. If $a = (a_1, a_2, a_3)$, we will simply write $[a] = [a_1, a_2, a_3]$. The vertex set of the *polarity graph* $B(q)$ is the set of all the $q^2 + q + 1$ points of $\mathrm{PG}(2, q)$, and 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 the corresponding triples are orthogonal, that is, if $ab^T = a_1b_1 + a_2b_2 + a_3b_3 = 0$. In the terminology of projective geometry this means that distinct vertices $[a]$ and $[b]$ are adjacent if and only if, in the projective plane $\mathrm{PG}(2, q)$, the point $[a]$ lies on the line with homogeneous coordinates $[b]$ and the point $[b]$ lies on the line with homogeneous coordinates $[a]$.

Parsons [12] derived a number of facts on the structure of polarity graphs. We will now give alternative proofs to some of the results of [12] we will need later. Our proofs are much shorter and are based on known facts about projective planes as presented in [8].

Let $[a] = [a_1, a_2, a_3]$ be a vertex of $B(q)$. Identification of neighbours of $[a]$ amounts to determining the solutions (x_1, x_2, x_3) of the linear equation $ax^T = a_1x_1 + a_2x_2 + a_3x_3 = 0$. This equation has $q^2 - 1$ non-zero solutions that represent $(q^2-1)/(q-1) = q+1$ distinct projective points, which are different from $[a]$ if and only if $aa^T = a_1^2 + a_2^2 + a_3^2 \neq 0$. It follows that a vertex $[a]$ has q or $q + 1$ neighbours in $B(q)$ according to whether aa^T is equal to zero or not. The projective triples $[a]$ of $\mathrm{PG}(2, q)$ such that $aa^T = 0$ are precisely those lying on the quadric $xx^T = 0$, which is non-degenerate (and hence a conic) if and only if q is odd. Accordingly, the vertices $[a]$ such that $aa^T = 0$ will be called *quadric vertices*.

Lemma 2.1. *The graph $B(q)$ contains exactly $q + 1$ quadric vertices.*

Proof. If q is odd, this is Theorem 5.21(i) of [8]. If q is even, a vertex $[a_1, a_2, a_3]$ is quadric if and only if $a_1^2 + a_2^2 + a_3^2 = 0$, which is in characteristic 2 equivalent to $a_1 + a_2 + a_3 = 0$, and there are exactly $(q^2 - 1)/(q - 1) = q + 1$ such projective triples in this case. □

The vertex set of $B(q)$ is thus a disjoint union of the set V of q^2 vertices of degree $q+1$ and the set W of $q+1$ quadric vertices, lying on the quadric $xx^T = 0$. Let V_1 be the subset of V comprising all vertices adjacent to at least one quadric vertex and let $V_2 = V \backslash V_1$. With this notation we now present further structural information on the polarity graphs $B(q)$ which we will use later.

Proposition 2.2. *For every prime power q the graph $B(q)$ has the following properties:*

(i) *The set W of quadric vertices is independent.*

(ii) *Each pair of vertices of V (adjacent or not) are connected by a unique path of length 2, while no edge incident to a quadric vertex is contained in any triangle; in particular, $B(q)$ has diameter 2.*

(iii) *If q is odd, then every vertex of V_1 is adjacent to exactly two quadric vertices, and $|V_1| = q(q+1)/2$, $|V_2| = q(q-1)/2$.*

(iv) *If q is odd, then the subgraphs of $B(q)$ induced by V_1 and V_2 are regular of degree $(q-1)/2$ and $(q+1)/2$, respectively.*

(v) *If q is even, then $|V_1| = q^2$ and V_2 is empty; moreover, V_1 contains a vertex v adjacent to all quadric vertices and every vertex in $V_1\backslash\{v\}$ is adjacent to exactly one quadric vertex and the subgraph of $B(q)$ induced by the set $V_1\backslash\{v\}$ is regular of degree q.*

Proof. Let $[a] = [a_1, a_2, a_3]$ and $[b] = [b_1, b_2, b_3]$ be two distinct vertices of $B(q)$, adjacent or not. Since the vectors a and b are linearly independent over F, the solution space of the linear system $ax^T = 0$, $bx^T = 0$ has dimension one. It follows that no pair of quadric vertices can be adjacent and that every pair of distinct vertices are connected by exactly one path of length two, proving (i) and (ii). Note that (ii) also follows from the property of $\mathrm{PG}(2, q)$ that any two points lie on a unique line.

Let q be odd. Invoking Chapters 7 and 8 of [8], the set W forms a conic and hence an oval. By Corollary 8.2 of [8] applied to the oval W, every vertex of V_1 and V_2 corresponds to a line of $\mathrm{PG}(2, q)$ containing exactly two points of W (a bisecant) or no point of W (an external line), respectively, and $|V_1| = q(q + 1)/2$, $|V_2| = q(q-1)/2$, which proves (iii). Table 8.1 of [8] shows that a bisecant contains $(q-1)/2$ points each lying on exactly two lines determined by projective coordinates corresponding to a vertex in W, while an external line contains $(q + 1)/2$ points each of which lies on no line determined by projective coordinates corresponding to a vertex in W. This exactly translates to (iv).

If q is even, the $q + 1$ vertices of W have the form $[a_1, a_2, a_3]$ with $a_1 + a_2 + a_3 = 0$. The vertex $v = [1, 1, 1]$ adjacent to every vertex of W is, in the terminology of [8], the nucleus of W. By Corollary 8.8 of [8] on vertices different from the nucleus, every vertex of V_1 is incident to exactly one vertex of W and $V_2 = \emptyset$, proving (v). □

We note that the authors of [5] and [4] observed that, for q even, one may extend the polarity graph $B(q)$ by adding a vertex and making it incident to all vertices in W; the new graphs will still have diameter 2.

3 Polarity graphs and their automorphisms

The automorphism group of $B(q)$ was determined in [12]. Here we give a different and shorter proof, including a more detailed discussion on groups. The idea is to relate the polarity graphs $B(q)$ to the point-line incidence graph of $\mathrm{PG}(2, q)$. We will represent the points and lines of $\mathrm{PG}(2, q)$ by projective triples (vectors) of F^3 as in the case of vertices of $B(q)$, except that points will be represented by *row vectors* and lines will be represented by *column vectors* (distinguished by the 'transpose' superscript). In this notation, a point $[a]$ lies on a line $[b^T]$ in $\mathrm{PG}(2, q)$ if and only if $ab^T = 0$. The involution θ on the union of the point set and the line set of $\mathrm{PG}(2,q)$ that interchanges $[x]$ with $[x^T]$ is the *standard polarity* of $\mathrm{PG}(2,q)$. The *point-line incidence graph* $I(q)$ of $\mathrm{PG}(2,q)$ is the bipartite graph whose vertex set is the union of the point and line sets of $\mathrm{PG}(2,q)$, with a vertex $[a]$ adjacent to a vertex $[b^T]$ if and only if the point $[a]$ lies on the line $[b^T]$, that is, $ab^T = 0$. Observe that the standard polarity θ is an automorphism of the bipartite graph $I(q)$, interchanging its two vertex-parts.

The fundamental theorem of projective geometry (see e.g. [8]) tells us that the subgroup of all automorphisms of the graph $I(q)$ that fix each of its two vertex parts setwise is isomorphic to the extension $\mathrm{P\Gamma L}(3,q)$ of the 3-dimensional projective linear group $\mathrm{PGL}(3,q)$ over F by the group of Galois automorphisms of F over the prime field of F. Elements of $\mathrm{P\Gamma L}(3,q)$ are pairs (A,φ), where $A \in \mathrm{PGL}(3,q)$ can be identified with an invertible 3×3 matrix over F and $\varphi \in \mathrm{Gal}(F)$. The action of such an element (A,φ) on vertices $[x]$ and $[y^T]$ of $I(q)$ is given by first applying A via the assignment $[x] \mapsto [xA]$ and $[y^T] \mapsto [A^{-1}y^T]$ and then applying φ to all elements of the resulting projective triples.

We continue with a remark regarding orthogonal groups. By the 3*-dimensional projective orthogonal group* $\mathrm{PGO}(3,q)$ we mean the factor group of the subgroup of $\mathrm{GL}(3,q)$ consisting of orthogonal matrices by the centre of this subgroup (trivial if q is even and isomorphic to Z_2 if q is odd). In characteristic 2 our definition is different from what appears to be a more usual way of introducing an orthogonal group in terms of preservation of a bilinear form and having an irreducible action on a vector space; nevertheless we hope that no confusion will arise.

The obvious extension $\mathrm{P\Gamma O}(3,q)$ of $\mathrm{PGO}(3,q)$ by $\mathrm{Gal}(F)$ acts on $B(q)$ as a group of automorphisms. Indeed, an element of $\mathrm{P\Gamma O}(3,q)$ can be identified with a pair (A,φ) as above, but this time with A being a 3×3 orthogonal matrix, that is, such that $A^T = A^{-1}$, with the obvious identification of A with $-A$ if q is odd. The action is simply given by $(A,\varphi)[x] = [\varphi(xA)]$, and it preserves edges of $B(q)$ since $xy^T = 0$ is equivalent to $(xA)(yA)^T = 0$ by orthogonality of A. We begin by showing that that there are no other automorphisms of $B(q)$.

Theorem 3.1. *For every prime power q the automorphism group of the polarity graph $B(q)$ is isomorphic to* $\mathrm{P\Gamma O}(3,q)$.

Proof. Every automorphism α of $B(q)$ induces an automorphism $\tilde{\alpha}$ of $I(q)$ given by $\tilde{\alpha}[x] = \alpha[x]$ and $\tilde{\alpha}[x^T] = (\alpha[x])^T$ for every projective triple $[x]$. By the Fundamental theorem of projective geometry and our earlier discussion, the automorphism $\tilde{\alpha}$ may be represented by an action of a pair (A,φ) representing an element of $\mathrm{P\Gamma L}(3,q)$, given by $\tilde{\alpha}[x] = [\varphi(xA)]$ and $\tilde{\alpha}[x^T] = [\varphi(A^{-1}x^T)]$ for all projective triples $[x]$. But since $\tilde{\alpha}[x] = \alpha[x]$ and $\tilde{\alpha}[x^T] = (\alpha[x])^T$, we have $(\tilde{\alpha}[x])^T = \tilde{\alpha}[x^T]$ and hence $[\varphi(xA)]^T = [\varphi(A^{-1}x^T)]$. As this is valid for all pairs (A,φ), we have $[xA]^T = [A^{-1}x^T]$ for all projective triples $[x]$. Letting x be successively equal to $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,0)$ and $(1,0,1)$ one concludes that $A^{-1} = \delta A^T$ for some non-zero $\delta \in F$. Taking determinants yields $1 = |\delta A^T A| = \delta^3 |A|^2$ and this is an equation between elements of the (cyclic) multiplicative group F^* of F.

We will show that there is a $\gamma \in F^*$ such that $\gamma^2 = \delta$. This is obvious if q is even (since in such a case every element of F^* has a unique square root), or if $\delta = 1$. If q is odd and $\delta \neq 1$, then $1 = \delta^3|A|^2$ implies that a third power of $\delta \neq 1$ is equal to 1 or to a second power of $|A|^{-1}$ if $|A| \neq 1$. This is, in the cyclic group F^* of *even* order $q-1$, possible only if $q-1$ is divisible by 3 and there is a $\gamma \in F^*$ such that $\delta = \gamma^2$ (and, in the second case, if $|A| = \gamma^{-3}$). In all circumstances we therefore have a $\gamma \in F^*$ such that $\delta = \gamma^2$.

The matrix $A_\gamma = \gamma A$ is orthogonal, i.e., $A_\gamma^{-1} = A_\gamma^T$. Since all our calculations are done with projective triples, the action of the original automorphism $\tilde{\alpha}$ may equivalently be described by $\tilde{\alpha}[x] = [\varphi(xA_\gamma)]$ and $\tilde{\alpha}[x^T] = [\varphi(A_\gamma^{-1}x^T)]$ for all projective triples $[x]$, where the pair (A_γ, φ) represents an element of $\mathrm{P\Gamma O}(3,q)$ as a subgroup of $\mathrm{P\Gamma L}(3,q)$. This shows that every automorphism of $B(q)$ is induced by an element of $\mathrm{P\Gamma O}(3,q)$. Since this group acts on $B(q)$ as we saw earlier, the result follows. □

It is known (cf. [8]) that $\mathrm{PGO}(3,q) \cong \mathrm{PGL}(2,q)$ and $\mathrm{P\Gamma O}(3,q) \cong \mathrm{P\Gamma L}(2,q)$ for every prime power q. Theorem 3.1 thus implies that if $q = p^n$ where p is a prime, then the graph $B(q)$ has exactly $nq(q^2-1)$ automorphisms.

The groups $\mathrm{P\Gamma O}(3,q)$ and $\mathrm{PGO}(3,q)$ obviously preserve the sets W, V_1 and V_2 and the sets W, $\{v\}$ and $V_1\backslash\{v\}$, depending on whether q is odd or even; it is easy to show that these sets are, in fact, orbits of $\mathrm{PGO}(3,q)$ on the vertices of $B(q)$. Corollary 7.15 of [8] tells us that the group $\mathrm{PGO}(3,q)$ is triply transitive on W. For odd q the analysis of [12] shows that $\mathrm{PGO}(3,q)$ acts arc-transitively on the subgraphs induced by the vertex set V_1 and V_2. We can say much more if q is even, extending the last result of Section 6 of [12]. Let $B_0(q)$ be the subgraph of $B(q)$ induced by the set $V_0 = V_1\backslash\{v\}$.

Theorem 3.2. *If q is a power of 2, the automorphism group of the graph $B_0(q)$ is isomorphic to $\mathrm{P\Gamma O}(3,q)$. Moreover, if $q \geq 4$, the smallest subgroup of $\mathrm{P\Gamma O}(3,q)$ acting transitively on vertices of $B_0(q)$ is the group $\mathrm{PGO}(3,q)$, which also acts regularly on arcs of $B_0(q)$. In particular, $B_0(q)$ is a vertex-transitive non-Cayley graph if $q > 2$.*

Proof. For every $w \in W$ let N_w be the set of neighbours of w in $B(q)$ distinct from v. Part (v) of Proposition 2.2 implies that the sets N_w $(w \in W)$ form a partition of the vertex set of $B_0(q)$. In the subgraph $B_0(q)$ the distance of any two vertices is greater than 2 if and only if the two vertices are in the same set N_w for some $w \in W$. It follows that any automorphism of $B_0(q)$ preserves the partition $\{N_w;\ w \in W\}$ and hence extends to an automorphism of the entire polarity graph $B(q)$. Consequently, by Theorem 3.1, the automorphism group of $B_0(q)$ is isomorphic to $\mathrm{P\Gamma O}(3,q)$; this was also noted in Section 6 of [12].

The rest of the proof will address the smallest group transitive on vertices of $B_0(q)$. It is easy to check that $B_0(2)$ is isomorphic to a complete graph of order 3, admitting a regular action of a subgroup of $\mathrm{P\Gamma O}(3,q) \cong S_3$ isomorphic to Z_3. From now on we therefore assume that $q \geq 4$.

By the remark after Theorem 3.1 we know that $\mathrm{P\Gamma O}(3,q) \cong \mathrm{P\Gamma L}(2,q)$, and for $q = 2^n$ with $n \geq 2$ we have $\mathrm{P\Gamma L}(2,q) \cong \mathrm{SL}(2,q) \rtimes Z_n$, the split extension being defined by the natural action of $Z_n \cong \mathrm{Aut}(\mathrm{GF}(q))$ on $\mathrm{SL}(2,q)$. In what follows we will, for simplicity of the arguments, identify the group $\mathrm{P\Gamma O}(3,q)$ with the group $G = \mathrm{SL}(2,q) \rtimes Z_n$. We also let $K = \mathrm{SL}(2,q)$ and note that K is normal in G.

Suppose that H is a subgroup of G acting transitively on the vertex set of $B_0(q)$. Letting $H_0 = H \cap K$ and observing that H_0 is normal in H, from the second group isomorphism theorem we have $H/H_0 \cong HK/K$. It follows that the order of H/H_0 is a divisor of n. On the other hand, the transitivity assumption on H implies that the order of H is a multiple of q^2-1, the number of vertices of $B_0(q)$. These two facts imply that $|H_0| = t(q^2-1)/n$ for some positive integer t. Since H_0 has now been identified with a subgroup of $K =$

$\mathrm{SL}(2,q)$, the task reduces to identification of subgroups of the group $\mathrm{SL}(2,q) \cong \mathrm{PSL}(2,q)$, $q = 2^n$, of order $t(q^2-1)/n$.

We will show that $\mathrm{PSL}(2,q)$ admits no such *proper* subgroup H_0 if $n \geq 2$, using Dickson's classification of subgroups of $\mathrm{PSL}(2,q)$ for $q = 2^n$ as displayed in [13]. By this classification, subgroups of $\mathrm{PSL}(2,q)$ split into four classes: (a) cyclic and dihedral subgroups, (b) affine subgroups, (c) subgroups isomorphic to A_4 or A_5 for n even, and (d) subgroups of the form $\mathrm{PSL}(2,2^m)$ where m is a divisor of n. We analyse the cases separately, recalling that throughout we assume $q = 2^n$ and $n \geq 2$.

(a) *Cyclic and dihedral subgroups.* The largest order of a subgroup of $\mathrm{PSL}(2,q)$ that is cyclic or dihedral is $2(q+1)$. It is easy to see that $2(q+1) < t(q^2-1)/n$ for $n \geq 3$ and all $t \geq 1$; if $n = 2$ then t has to be even and then the same inequality holds. It follows that H_0 cannot be cyclic or dihedral.

(b) *Affine subgroups.* The largest order of an affine subgroup of $\mathrm{PSL}(2,q)$ is $q(q-1)$ and the second largest order of such a subgroup is $\sqrt{q}(\sqrt{q}-1)$ if n is even. If $q(q-1) = t(q^2-1)/n$, then $nq = t(q+1)$ and $q+1$ would have to divide n, a contradiction. For the second largest order, observe that $\sqrt{q}(\sqrt{q}-1) < q+1 \leq (q^2-1)/n$, the last inequality being a consequence of $n \geq q-1$. We conclude that H_0 cannot be affine.

(c) *The groups* A_4, A_5. We may eliminate A_4 since its order is 12 and the order of $B_0(2^2)$ is 15. Since the order of $B_0(2^4)$ is 2^8-1, the only feasible value of n for $H_0 \cong A_5$ is $n = 2$. In this case, however, $A_5 \cong \mathrm{PSL}(2,2^2)$ and so H_0 would not be a proper subgroup of $\mathrm{PSL}(2,2^2)$.

(d) *Subgroups* $\mathrm{PSL}(2,2^m)$ *where* $m \mid n$. Let $H_0 \cong \mathrm{PSL}(2,2^m)$ for m a proper divisor of n. If $n \in \{2,3\}$, then $m = 1$ and the order of $\mathrm{PSL}(2,2)$ is too small for H_0 to be transitive on vertices of $B_0(2^n)$. If $n \geq 4$, then the largest order of such a subgroup H_0 is at most $\sqrt{q}(q-1)$. It is easy to check, however, that $\sqrt{q}(q-1) < (q^2-1)/n$ for $n \geq 4$, giving a contradiction again.

The above arguments show that, for $q = 2^n$ and $n \geq 2$, the smallest subgroup of $\mathrm{P\Gamma O}(3,q) \cong \mathrm{P\Gamma L}(2,q)$ transitive on vertices of $B_0(q)$ is the group $\mathrm{PGO}(3,q) \cong \mathrm{PSL}(2,q)$. It is a matter of routine to check that this group is, in fact, regular on the arc set of $B_0(q)$. Combining the two facts we conclude that $B_0(q)$ is an arc-transitive (and, of course, vertex-transitive) non-Cayley graph for all $n \geq 2$. □

4 Vertex-transitive graphs from polarity graphs?

Polarity graphs are, of course, not vertex-transitive. Being the largest currently known examples of graphs of maximum degree $q+1$ and diameter 2, however, it is interesting to ask if one cannot add "a few" edges to a polarity graph to obtain a vertex-transitive graph. In [15] it was shown that it is impossible to construct a vertex-transitive graph of degree $q+1$ which would contain $B(q)$ as a spanning subgraph. We extend this result to the degree $q+3$ for odd $q \geq 37$.

Theorem 4.1. *For any odd prime power* $q \geq 37$ *there is no vertex-transitive graph of degree* $q+3$ *which contains the polarity graph* $B(q)$ *as a spanning subgraph.*

Proof. Let $B = B(q)$ and let B' be a graph containing B as a spanning subgraph. Let E and E' be the edge set of B and B', respectively; edges of the set E and $E' \setminus E$ will be called *old* and *new*, respectively. Suppose now that B' is a vertex-transitive graph of degree

$q+3$. Let u, v be vertices of B such that $e = uv$ is a new edge and let $N(u)$ and $N(v)$ be the set of neighbours of u and v in B. From the fact that any two distinct non-adjacent vertices of B are joined by a unique path of length 2 it follows that there is a unique vertex, say, w, in $N(u) \cap N(v)$. If $|N(u)| = |N(v)|$, the set of all old edges joining the set $N(u)\backslash\{w\}$ with the set $N(v)\backslash\{w\}$ forms a perfect matching between the two sets. If not, then $|N(u)|$ and $|N(v)|$ differ by one. Without loss of generality, if $|N(u)| = |N(v)| + 1$, then exactly one neighbour of u, say, t, is joined to w. In this case there is a perfect matching between the sets $N(u)\backslash\{w, t\}$ and $N(v)\backslash\{w\}$. It follows that any new edge $e = uv$ is contained in a set S_e of quadrangles such that (1) $|S_e| \geq q - 1$, and (2) any two quadrangles in S_e share just the edge e and its end-vertices u, v.

An edge $e \in E'$ will be called *thick* if there exists a set S_e of quadrangles with the properties (1) and (2) above. Note that this definition does not require e to be new, but the fact we have derived above implies that every new edge is thick. By the assumed vertex-transitivity, every vertex of B' must be incident to the same number, say, t, of thick edges. Since the degree of B' is supposed to be $q + 3$, every vertex in W is incident to at least three thick edges, so that $t \geq 3$. If $t = 3$, the three thick edges are all new and every vertex in V would be incident to exactly two new thick edges and one old thick edge. This would mean that there is a perfect matching on V formed by old thick edges, which is impossible since $|V| = q^2$ and q is odd. It follows that $t \geq 4$, every vertex in W is incident to at least one old thick edge and every vertex in V is incident to at least two old thick edges.

Properties of B imply that for any vertex $v \in V_2$ the subgraph of B induced by the set $N(v)$ is a perfect matching of $(q + 1)/2$ edges. Vertex-transitivity of B' then implies that for every vertex $w \in W$ the subgraph of B' induced by the set $N'(w)$ of all $q + 3$ neighbours of w in B' contains a subset E'_w of $(q + 1)/2$ mutually independent edges. Note that since there were no edges in $N(w)$ in the graph B, all the edges in E'_w must be new. At most three edges of E'_w join a vertex from $N(w)$ with a vertex in $N'(w)\backslash N(w)$, and so the subgraph of B' induced by the set $N(w)$ contains a subset $E_w \subset E'_w$ of least $(q + 1)/2 - 3 = (q - 5)/2$ new edges. Since any two neighbourhoods of vertices of W in the graph B intersect in exactly one vertex, the sets of new edges E_w, $w \in W$, are mutually disjoint. For counting, imagine that every new edge consists of two new half-edges incident to the corresponding end-vertices. The $q(q + 1)/2$ vertices of V_1, each incident with two new half-edges, are incident to a total of $q(q + 1)$ new half-edges. At least $(q + 1)(q - 5)$ of these are 'absorbed' by vertices of V_1 since the sets E_w, $w \in W$, are pairwise disjoint and $N(w) \subset V_1$ for every $w \in W$. It follows that there are at most $(q + 1)q - (q + 1)(q - 5) = 5(q + 1)$ new edges that join vertices of V_1 with vertices outside V_1. In particular, there are at most $5(q + 1)$ new edges between V_1 and V_2.

We know that every vertex $w \in W$ is incident to an old thick edge; let $e = wv$ be such an edge, $v \in V_1$. Let S_e be a set of quadrangles with the properties (1) and (2) introduced earlier. At most 3 quadrangles of S_e can contain a new edge incident with w, at most 2 such quadrangles can contain a new edge incident with v, and since v has at most $(q - 1)/2 + 2$ neighbours from V_1 in the graph B', at most $(q - 1)/2 + 2$ quadrangles in S_e contain a new edge having both end-vertices in V_1. Note that in each quadrangle containing three old edges the fourth edge must be new. Consequently, there are at least $(q - 1) - ((q - 1)/2 + 7) = (q - 15)/2$ quadrangles in S_e containing at least one new edge joining a vertex in V_1 with a vertex in V_2. Since our considerations are valid for every vertex $w \in W$, the neighbourhoods $N(w)$ in the graph B intersect just in one vertex, and every vertex in V_1 is incident to two new edges, we conclude that there are at least

$((q+1)(q-15)/2)/2$ new edges joining V_1 with V_2. But we have seen earlier that the number of such edges is at most $5(q+1)$. Thus, $(q+1)(q-15)/4 \le 5(q+1)$, that is, $q \le 35$, contrary to our assumption that $q \ge 37$. □

Another obvious method to create large vertex-transitive graphs from polarity graphs is to take a large vertex-transitive subgraph of $B(q)$ and try to extend it to a vertex-transitive graph of diameter 2 by adding edges. The hottest candidate for this is the subgraph $B_0(q)$ if q is a power of 2, which we have encountered in the previous section.

Theorem 3.2, however, is bad news for adding edges to $B_0(q)$ to produce a vertex-transitive graph of diameter two. Namely, the most natural approach would be to take the smallest group H acting transitively on the set of vertices of $B_0(q)$ and identify the smallest possible number of H-orbits of non-adjacent pairs of vertices so that making these pairs adjacent would yield a graph of diameter 2 with $B_0(q)$ as a spanning subgraph. But by Theorem 3.2, for $q \ge 4$ the smallest such subgroup H is isomorphic to $\mathrm{PGO}(3,q)$, acting transitively and with vertex stabilisers of order q. It follows that an orbit furnishing new edges would increase the degree of the resulting graph by at least q. This would make the resulting graph uninteresting from the point of view of the degree-diameter problem.

Before continuing let us comment on the isomorphism of the groups $\mathrm{PGO}(3,q)$ and $\mathrm{PGL}(2,q)$, mentioned after the proof of Theorem 3.1. In [8] an isomorphism of the two groups is given, induced by the quadratic form $x_2^2 + x_1x_3$. While for odd q such a form is equivalent to $x_1^2+x_2^2+x_3^2$ which we have been using, this is not true for even q since for q a power of 2 the form $x_1^2+x_2^2+x_3^2$ is degenerate. It is easy to check that, with respect to this form, all elements of $\mathrm{PGO}(3,q)$ for q even have the form

$$\begin{pmatrix} 1+a & 1+c & 1+a+c \\ 1+b & 1+d & 1+b+d \\ 1+a+b & 1+c+d & 1+a+b+c+d \end{pmatrix}$$

where $a,b,c,d \in F = \mathrm{GF}(q)$ and $ad+bc = 1$, which implies that $(a,b) \neq (0,0)$. Then, for even q, one may check that the mapping $\phi :\ \mathrm{PGO}(3,q) \to \mathrm{PGL}(2,q)$ given by

$$\begin{pmatrix} 1+a & 1+c & 1+a+c \\ 1+b & 1+d & 1+b+d \\ 1+a+b & 1+c+d & 1+a+b+c+d \end{pmatrix} \mapsto \begin{pmatrix} c & a \\ d & b \end{pmatrix}$$

is a group isomorphism. We will use its inverse ϕ^{-1} in the proof of our last two result.

In contrast with Theorem 3.2, there exists a subgroup of $\mathrm{PGO}(3,q)$ that is transitive on the set $V^* = V_0 \setminus \{[t,t,1],\ t \in \mathrm{GF}(q)\}$; let $B^*(q)$ be the subgraph of $B_0(q)$ induced by the set V^*. Our last result shows that we can construct large Cayley graphs of diameter 2 and degree $d = q + O(\sqrt{q})$ by adding edges to $B^*(q)$. Since the order of $B^*(q)$ is $q(q-1) = d^2 - O(d^{3/2})$, the resulting graphs will be asymptotically approaching the Moore bound.

Theorem 4.2. *For every even prime power q there exists a Cayley graph of diameter 2 and degree $q + O(\sqrt{q})$ with $B^*(q)$ as a spanning subgraph.*

Proof. Let H be the subgroup of $\mathrm{PGO}(3,q)$ formed by all the matrices as in (4) for which $a+b+c+d = 0$. It is straightforward to check that $|H| = q(q-1)$ and that H acts regularly on the vertex set of the graph $B^*(q)$. It follows that $B^*(q)$ is a Cayley graph

$Cay(H, X)$ for the group H and some inverse-closed generating set $X \subset H$ such that $|X| = q - 1$, which is the degree of $B^*(q)$.

In order to create a Cayley graph of diameter 2 from $B^*(q)$ by adding $O(\sqrt{q})$ edges it is sufficient to show that one can extend the generating set X to a set $X' \supset X$ by adding $O(\sqrt{q})$ elements of H. Since we are dealing with a Cayley graph, it is sufficient to check distances from one particular vertex u, say, $u = [1, 0, 0]$. Compared with the graph $B(q)$, in our new graph $B^*(q)$ the vertex u lost two neighbours, namely, $v_1 = [0, 1, 1]$ and $v_2 = [0, 0, 1]$. We consider the effect caused by losing the two neighbours separately.

Since uv_1 is not an edge of $B^*(q)$, we lost the paths of length 2 joining u with vertices in the subset U_1 of $B^*(q)$ of the form $[1, t, t]$, $t \in F$, $t \neq 0, 1$. Consider the subgroup $H_1 < H$ formed by the matrices $\phi^{-1}(J_g)$, $g \in F^*$, where

$$J_g = \begin{pmatrix} g & 0 \\ g + g^{-1} & g^{-1} \end{pmatrix} .$$

It may be verified that $H_1 \cong F^*$ and H_1 acts regularly on the set $U_1 \cup \{u\}$. Geometrically, H_1 can be identified with the group of homologies (that is, central-axial collineations with a non-incident center-axis pair) with centre v_1 and axis vv_2. Since F^* is Abelian (in fact, cyclic), there exists an inverse-closed set X_1 of at most $\lceil 2\sqrt{q} \rceil$ elements such that the Cayley graph $Cay(H_1, X_1)$ with vertex set $U_1 \cup \{u\}$ has diameter 2.

The effect of the missing edge uv_2 is that we lost the paths of length 2 joining u with vertices in the subset U_2 of $B^*(q)$ of the form $[a + 1, a, 0]$, $a \in F^*$. Let now $H_2 < H$ be the subgroup of H consisting of the matrices $\phi^{-1}(L_a)$, $a \in F^+$, where

$$L_a = \begin{pmatrix} a + 1 & a \\ a & a + 1 \end{pmatrix} .$$

Obviously, $H_2 \cong F^+$ and H_2 is easily seen to be a regular permutation group on the set $U_2 \cup \{u\}$. From the point of view of geometry, H_2 can be identified with the group of elations (central-axial collineations with an incident center-axis pair) with centre $[1, 1, 0]$ and axis vv_2. Again, it is well known that there exists an inverse-closed set X_2 of at most $\lceil 2\sqrt{q} \rceil$ elements, making $Cay(H_2, X_2)$ a graph of diameter 2 with vertex set $U_2 \cup \{u\}$.

It is now easy to check that the graph $Cay(H, X')$ with $X' = X \cup X_1 \cup X_2$ has the required properties. □

Cayley graphs of diameter 2, order $q(q - 1)$ and degree $q + O(\sqrt{q})$ for even q have been recently constructed in [14] as follows. For q a power of 2 and $F = \mathrm{GF}(q)$ consider the one-dimensional affine group $G_q = \mathrm{AGL}(1, q) \simeq F^+ \rtimes F^*$, with elements written as pairs (g, a), $g \in F^*$, and $a \in F^+$ and with multiplication in the form $(g, a)(h, b) = (gh, ah + b)$ for $g, h \in F^*$ and $a, b \in F^+$. The set $Y_q = \{(y^2, y);\ y \in F^*\}$ is an inverse-closed generating set of G_q. The graphs of [14] are formed by taking the Cayley graph $Cay(G_q, Y_q)$ and adding a suitable set of further $O(\sqrt{q})$ generators to Y_q.

Our last result shows that, quite surprisingly, the Cayley graphs $Cay(G_q, Y_q)$ from [14] are isomorphic to the graphs $B^*(q)$. This gives the construction of [14] a strong geometric flavour.

Theorem 4.3. *If q is a power of 2, the graph $Cay(G_q, Y_q)$ is isomorphic to $B^*(q)$.*

Proof. We will use the notation introduced in the proof of Theorem 4.2, by which the graph $B^*(q)$ is isomorphic to the Cayley graph $Cay(H, X)$. It may be checked that every element of H can be written as a product $\phi^{-1}(J_g L_a)$ with $g \in F^*$ and $a \in F^+$. Let us identify this product with the ordered pair $[g, a]$. One easily verifies that in this identification the multiplication $\circ$ of elements of H is represented in the form $[g, a] \circ [h, b] = [gh, ah^{-2} + b]$. A further composition of the mapping $\phi^{-1}(J_g L_a) \mapsto [g, a]$ with $\psi : \; [g, a] \mapsto (g^{-2}, a)$ establishes an isomorphism $H \cong G_q$.

It remains to analyse the generating set X, which is uniquely determined by the elements of H that take a fixed vertex of $B^*(q)$ to all its neighbours; in what follows our fixed vertex will be $u = [1, 0, 0]$. Now, multiplication of the row vector $(1, 0, 0)$ by the matrix $\phi^{-1}(J_g L_a)$ yields the vector $(1 + ag, 1 + g + ag, 1 + g)$. This means that the element of H encoded $[g, a]$ takes the vertex u onto the vertex $[1 + ag, 1 + g + ag, 1 + g]$ of $B^*(q)$. Since the neighbours of u in $B^*(q)$ have the form $[0, 1, s]$ for $s \in F$, $s \neq 1$, the elements of H taking u to the neighbours of u are encoded by pairs $[t^{-1}, t]$ for $t \in F^*$. The generating set X of H thus consists, in our representation, of all the pairs $[t^{-1}, t]$, where $t \in F^*$. Composition with the mapping ψ introduced earlier finally establishes the isomorphism from the Cayley graph $Cay(H, X)$ onto the Cayley graph $Cay(G_q, Y_q)$ of [14]. □

5 Remarks

Adjacency in polarity graphs $B(q)$ has been defined by means of the standard dot product. For odd q the standard dot product is just a special case of a symmetric non-singular bilinear form. What happens if one uses a more general form instead? Following [2], for an odd prime power q let Q be a non-singular quadratic form over F^3 where $F = FG(q)$, and let $\beta(x, y) = Q(x + y) - Q(x) - Q(y)$ be the corresponding non-singular symmetric bilinear form. We now may let $B_\beta(q)$ be the graph on the same vertex set as $B(q)$, but with two distinct vertices $[a]$ and $[b]$ adjacent if $\beta(a, b) = 0$. It is known, however (see e.g. [2, 8]), that in dimension 3 and for odd q, all non-singular quadratic forms are equivalent and their equivalence is induced by linear transformations (i.e., by change of bases). It follows that for odd q all such graphs $B_\beta(q)$ are isomorphic to $B(q)$, with isomorphisms being provided by the corresponding linear transformations. Of course, such a correspondence between quadratic forms and bilinear forms fails in characteristic 2.

Another way of generalizing polarity graphs is to define them on more general finite projective planes. Recall that a *finite projective plane* $\mathcal{P}$ is a collection of a finite number of points and lines such that every two points are incident with a unique line, every two lines are incident with a unique point, and there are four points no three of which are incident with a line. It is well known that for any such $\mathcal{P}$ there is an integer n such that any line is incident with precisely $n + 1$ points and, dually, any point is incident with exactly $n + 1$ lines. One then speaks about a projective plane of *order* n, and it is then easy to show that the number of points and the number of lines are both equal to $n^2 + n + 1$. (An outstanding conjecture in finite geometry is that the order of a finite projective plane must be a prime power.)

Suppose now that $\mathcal{P}$ has a *polarity*, that is, a bijection π from the point set onto the line set of $\mathcal{P}$ with the property that for every two points A and B, A is incident with $\pi(B)$ if and only if B is incident with $\pi(A)$. We may then define the *generalized polarity graph* $B_{\mathcal{P},\pi}$ with vertex set equal to the point set of $\mathcal{P}$ and with two distinct points A and B adjacent if A is incident with $\pi(B)$. This graph obviously has diameter 2 by the properties of the projective plane. Observe that if $\mathcal{P} = \mathrm{PG}(2, q)$ is the standard projective plane as introduced in Section 2 and if one considers the standard polarity π interchanging projective vectors with their transposes, then the graph $B_{\mathcal{P},\pi}$ coincides with the polarity graph $B(q)$. It is of interest to point out that if $\mathcal{P}$ is a (general) finite projective plane of order n with a polarity π, then, by [1], the number $m(\pi)$ of self-conjugate points (those incident with their π-images) satisfies $m(\pi) \geq n+1$, and if $m(\pi) > n+1$ then n is a square and every prime divisor of n divides $m(\pi) - 1$. Since the corresponding generalized polarity graph $B_{\mathcal{P},\pi}$ has exactly $m(\pi)$ vertices of degree n and all the remaining vertices have degree $n + 1$ it follows that for $n = q$, where q is an even power of a prime, the graph $B_{\mathcal{P},\pi}$ need not be isomorphic to $B(q)$. Investigation of such a generalization of polarity graphs may lead to interesting results.

We conclude by commenting on vertex-transitive extensions of polarity graphs. In general, by a *vertex-transitive closure* of a graph G we will understand any vertex-transitive supergraph of G on the same vertex set. We may then define $d_{vt}(G)$ to be the smallest degree of a vertex-transitive closure of G. In this terminology, our Theorem 4.1 says that $d_{vt}(B_q) \geq q + 5$ for any odd prime power $q \geq 37$. Determining or at least estimating $d_{vt}(G)$ for arbitrary graphs G appears to be an interesting problem on its own.

Acknowledgement. The authors would like to thank an anonymous referee for carefully reading the manuscript, suggesting important improvements and providing geometric insight into the groups used in Section 4.

The second author acknowledges support from the VEGA Research Grants 1/0871/11, 1/0065/13 and 1/0007/14, the APVV Research Grants 0223-10 and 0136-12, as well as the APVV support as part of the EUROCORES Programme EUROGIGA, project GREGAS, ESF-EC-0009-10, financed by the European Science Foundation.

References

[1] R. Baer, Polarities in finite projective planes, *Bull. Amer. Math. Soc.* **52** (1946), 77–93.

[2] S. Ball and Z. Weiner, An Introduction to Finite Geometry, Preprint (2011).

[3] W. G. Brown, On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.* **9** (1966), 281–285.

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

[5] P. Erdős, S. Fajtlowicz and A. J. Hoffman, Maximum degree in graphs of diameter 2, *Networks* **10** (1980), 87–90.

[6] P. Erdős and A. Rényi, On a problem in the theory of graphs, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **7** (1962), 623–641.

[7] P. Erdős, A. Rényi and V. T. Sós, On a problem of graph theory, *Studia Sci. Math. Hungar.* **1** (1966), 215–235.

[8] J. Hirschfeld, *Projective geometries over finite fields*, Oxford University Press, 1998.

[9] A. J. Hoffman and R. R. Singleton, On Moore graphs with diameter 2 and 3, *IBM J. Res. Develop.* **4** (1960), 497–504.

[10] B. Huppert, *Endliche Gruppen 1*, Springer, 1967.

[11] M. Miller and J. Širáň, Moore graphs and beyond: A survey of the degree-diameter problem, *Electronic J. Combin.* (2013), Dynamic survey DS14.

[12] T. D. Parsons, Graphs from projective planes, *Aequat. Math.* **14** (1976), 167–189.

[13] J. De Saedeleer and D. Leemans, On the rank two geometries of the groups $PSL(2,q)$: part I, *Ars Math. Contemp.* **3** (2010), 177–192.

[14] J. Šiagiová and J. Širáň, Approaching the Moore bound for diameter two by Cayley graphs, *J. Combin. Theory Ser. B* **102** (2012), 470–473.

[15] J. Širáň, J. Šiagiová and M. Ždímalová, Large graphs of diameter two and given degree, in: *Proc. IWONT 2010*, Univ. Politecnica de Catalunya, 2011, 347–359.