J Algebr Comb (2012) 36:389–401
DOI 10.1007/s10801-011-0340-2

On the nullspace of arc-transitive graphs over finite fields

Primož Potočnik · Pablo Spiga · Gabriel Verret

Received: 12 February 2011 / Accepted: 5 December 2011 / Published online: 16 December 2011

Abstract Let A be the adjacency matrix of a graph Γ. The nullity of A (that is, the dimension of the nullspace of A), when viewed as a matrix over a field of prime characteristic p, is called the p-*nullity* of Γ. We present several families of arc-transitive graphs with arbitrarily large p-nullity. We also show that the p-nullity of a vertex-transitive graph of order a power of p is zero, provided that the valency of the graph is coprime to p.

Keywords Arc-transitive graphs · Graph-restrictive groups · Spectral graph theory · Finite fields

1 Introduction

Spectral graph theory is a well-developed area of research with fascinating applications in other areas of graph theory. In view of the vast amount of work done in this field, it is somewhat surprising that the spectrum of a graph is almost exclusively studied over a field of characteristic zero. There are at least two exceptions. Namely, in [3, 4] and [12], the rank of the adjacency matrix of a graph over the field of order 2 is used to bound its chromatic number. Furthermore, in the theory of association schemes and coherent configurations, the adjacency matrix of graphs and designs is

P. Potočnik
Faculty of Mathematics and Physics, University of Ljubljana, Ljubljana, Slovenia

P. Spiga (✉)
Dipartimento di Matematica ed Applicazioni, University of Milano-Bicocca, Via Cozzi 53, 20125 Milano, Italy
e-mail: pablo.spiga@unimib.it

P. Potočnik · G. Verret
Institute of Mathematics, Physics, and Mechanics, Jadranska 19, 1000 Ljubljana, Slovenia

studied in detail over an arbitrary field to deduce some important facts about special families of graphs, for example strongly regular graphs. For this remarkable aspect of spectral graph theory, we refer the reader to [2, 6] and to the excellent recent survey article [5].

Our original motivation for this investigation was a seemingly unrelated question about the order of vertex-stabilisers in arc-transitive graphs [10]. The proof of a critical result required the existence of certain families of arc-transitive graphs with adjacency matrices having arbitrary large nullity over the field with p elements. However, whilst searching for such graphs, the authors became fascinated by the topic and its plentiful connections with other areas of mathematics, ranging from projective geometry to number theory. The aim of this paper is thus two-fold; first, to convey some of our fascination and perhaps initiate further research in this area and, second, to construct a family of graphs solving our original problem. Before stating the main results, let us first introduce some notation which will be used throughout the paper.

Unless otherwise noted, graphs are finite and simple. Let Γ be such a graph. An *s-arc* of Γ is a sequence $\alpha = (v_0, \dots, v_s)$ of $s+1$ vertices of Γ such that each two consecutive vertices are adjacent and each three consecutive vertices in the sequence are pairwise distinct. A 1-arc is simply called an arc.

Let $G \leq \mathrm{Aut}(\Gamma)$ be a group of automorphisms of Γ. We say that Γ is G-vertex-transitive or G-arc-transitive if G acts transitively on the vertices or the arcs of Γ, respectively. Similarly, we say that Γ is *(G, s)-arc-transitive* if G acts transitively on the set of s-arcs of Γ. We also say that Γ is *(G, s)-arc-regular* if G acts regularly on the set of s-arcs of Γ. When $G = \mathrm{Aut}(\Gamma)$, the prefix G in the above definitions is usually omitted.

Let p be a prime, let $\mathbb{F}$ be a field of characteristic p and let A be an integer-valued matrix. Taking A over $\mathbb{F}$ simply means reducing the entries of A modulo p. Note that this does not depend on the choice of $\mathbb{F}$. The rank of A over $\mathbb{F}$ will be called the *p-rank* of A. Define the *p-rank of a graph* to be the p-rank of its adjacency matrix. Recall that the *nullity* of a matrix is the dimension of its nullspace. In an analogous manner as above, we define the *p-nullity* of an integer-valued matrix and of a graph.

Definition 1 Let p be a prime and let $\mathcal{F}$ be a class of graphs. If, for every integer M, there exists a graph Γ of $\mathcal{F}$ with p-nullity at least M, we say that $\mathcal{F}$ has *unbounded p-nullity*.

In this paper, we exhibit a few interesting such classes of graphs, which are summarised in the following theorem.

Theorem 2 *Let $d \geq 3$ be an integer and let p be a prime. The following families have unbounded p-nullity.*

(1) *connected 4-arc-transitive graphs*,
(2) *connected 4-arc-transitive 3-valent graphs, for $p = 2$*,
(3) *connected arc-transitive graphs of valency d*,
(4) *the class of connected 3-valent graphs for which there exists a 2-arc-regular group of automorphisms containing a 1-arc-regular subgroup.*

Here are a few comments on the above theorem. First, note that part (3) improves part (1) for the class of arc-transitive graphs. Similarly, part (2) improves parts (1) and (3) but only for $p = 2$ and $d = 3$, respectively. Part (4) is the result needed to solve the problem which originally motivated our investigation. Let us briefly present this problem and its connection with the above theorem.

For a G-arc-transitive graph Γ and a vertex $v \in V(\Gamma)$, let $G_v^{\Gamma(v)}$ be the permutation group induced by the action of the stabiliser G_v on the neighbourhood $\Gamma(v)$ of the vertex v. A transitive permutation group L is said to be *graph-restrictive* [11, Definition 2] provided that there exists a constant $c(L)$ such that, if Γ is a connected G-arc-transitive graph with $G_v^{\Gamma(v)}$ permutation isomorphic to L and (u, v) is an arc of Γ, then $|G_{uv}| \le c(L)$. By the classical result of Tutte on 3-valent arc-transitive graphs [15], transitive permutation groups of degree 3 are graph-restrictive (and the constant $c(L)$ can be chosen to be 16). Similarly, it is well known that, with the exception of the dihedral group D_4 of degree 4, all transitive permutation groups of degree 4 or 5 are graph-restrictive (see [16] for example). When trying to extend the classification of graph-restrictive groups to permutation groups of degree 6, some key cases are: (i) the action of the alternating group A_4 on the six unordered pairs of a 4-set, (ii) the action of the symmetric group S_4 on the same six pairs and, (iii) the action of S_4 on the cosets of a cyclic subgroup of order 4. We are able to reduce the problem of proving that these permutation groups are not graph-restrictive to the problem of proving part (4) of Theorem 2 (see [10] for details).

Here is a brief summary of this paper. In Sects. 2 and 3 we give two simple constructions of 4-arc-transitive graphs proving parts (1) and (2) of Theorem 2. In Sect. 4, we set up some useful notation for graphs admitting a semiregular group of automorphisms. This is then used in Sects. 5 and 6 to prove, respectively, parts (3) and (4) of Theorem 2. Finally, in Sect. 7, we prove a remarkable result relating the p-nullity of a graph Γ to the p-nullity of the quotient of Γ by a semiregular group of automorphisms. As an application, we show that vertex-transitive graphs of valency d and order a power of p have trivial p-nullity if $\gcd(p, d) = 1$.

2 Incidence graphs of projective planes

If there is no restriction on the valency, then it is not hard to exhibit examples of arc-transitive graphs with large p-nullity. Here is a well-studied example.

Proof of part (1) of Theorem 2 Let $a \in \mathbb{N}$, let $q = p^a$, and consider the incidence graph Γ_a of the projective plane $\mathrm{PG}(2, q)$. The vertices of Γ_a are the points and the lines of $\mathrm{PG}(2, q)$, with a point P incident to a line l in Γ_a if and only if P lies on l. It is known that Γ_a is connected, is 4-arc-transitive (see [3, Sect. 5.3]) and its p-rank is $2(\binom{p+1}{2}^a + 1)$ (see [13]). Note that $\binom{p+1}{2}^a + 1 \le q^2$. Since Γ_a has $2(q^2 + q + 1)$ vertices, it follows that Γ_a has p-nullity at least $2(q + 1)$. In particular, $\{\Gamma_a \mid a \in \mathbb{N}\}$ has unbounded p-nullity, proving part (1) of Theorem 2. □

3 4-arc-transitive 3-valent graphs

In this section, we study the 2-nullity of some arc-transitive 3-valent graphs. Our first observation is that this is always even. This follows from the fact that the number of vertices of a 3-valent graph is even and the 2-rank of a graph is even. Indeed, the adjacency matrix of a graph over a field of characteristic 2 can be viewed as the matrix of an alternating bilinear form, which is well known to have even rank (see [3, Theorem 8.10.1]).

We prove part (2) of Theorem 2, that is, that the class of connected 4-arc-transitive 3-valent graphs has unbounded 2-nullity. We will require the following lemma, which is well known (see [12, Theorem 22]). We include a proof for completeness.

Lemma 3 *Let A be the adjacency matrix of a graph Γ and let μ be the number of perfect matchings of Γ. Then* $\det A$ *has the same parity as μ.*

Proof Let n be the number of vertices of Γ and write $A = (a_{ij})_{i,j}$. We have $\det A = \sum_\sigma \mathrm{sgn}(\sigma) a_{11^\sigma} \cdots a_{nn^\sigma}$. Since we are only interested in the parity of $\det A$, we can omit $\mathrm{sgn}(\sigma)$. Moreover, σ does not contribute to the sum unless $a_{11^\sigma} \cdots a_{nn^\sigma} = 1$. Since A is symmetric, if $a_{11^\sigma} \cdots a_{nn^\sigma} = 1$, then $a_{11^{\sigma^{-1}}} \cdots a_{nn^{\sigma^{-1}}} = 1$. In particular, if $\sigma \neq \sigma^{-1}$, then the contributions of σ and σ^{-1} to $\det A$ cancel each other. Therefore, we only need to consider the permutations σ such that $\sigma^2 = 1$ and $a_{11^\sigma} \cdots a_{nn^\sigma} = 1$. Clearly, each such permutation σ gives rise to the perfect matching $\{\{i, i^\sigma\}\}_i$ of Γ. Conversely, each perfect matching of Γ yields an involution σ with $a_{11^\sigma} \cdots a_{nn^\sigma} = 1$. This completes the proof of the lemma. □

We also need the following simple result.

Lemma 4 *Let Γ be a connected 3-arc-transitive graph of valency $d \geq 2$ and let μ be the number of perfect matchings of Γ. Then $d(d-1)$ divides μ. In particular, μ is even.*

Proof Let (u, v, w, x) be a 3-arc of Γ. We first consider the degenerate case when $u = x$. By the 3-arc-transitivity of Γ, each 3-arc of Γ is a 3-cycle and hence Γ is a complete graph on 3 vertices, which admits no perfect matching. In particular, $\mu = 0$ and the lemma follows. We may thus assume that $u \neq x$. Let μ_1 be the number of perfect matchings containing (u, v) and let μ_2 be the number of perfect matchings containing both (u, v) and (w, x). In a perfect matching containing (u, v), the vertex w must be matched to any of its remaining $d - 1$ neighbours. Since Γ is 3-arc-transitive, each such choice leads to the same number of perfect matchings and hence $\mu_1 = (d-1)\mu_2$. Similar arguments show that $\mu = d\mu_1$. Hence $\mu = d(d-1)\mu_2$ and $d(d-1)$ divides μ. □

Combining the above two lemmas, we get the following corollary.

Corollary 5 *If Γ is a connected 3-arc-transitive graph of valency $d \geq 2$, then Γ has non-zero 2-nullity.*

Proof From Lemma 4, the number of perfect matchings of Γ is even, and hence from Lemma 3, the determinant of the adjacency matrix of Γ is even. □

Proof of part (2) of Theorem 2 We construct an infinite family of connected 4-arc-transitive 3-valent graphs. First, we point out that, by Dirichlet's theorem on primes in arithmetic progression, there exist infinitely many primes congruent to ± 1 mod 16. Let r be such a prime and let $G_r = \mathrm{PSL}(2, r)$.

It is well known that G_r contains a maximal subgroup H isomorphic to S_4 (see [14, Chap. 3, Sect. 6]). Moreover, in its action on the coset space $\Omega = G_r/H$, the group G_r has a self-paired suborbit of size 3. In particular, G_r is a group of automorphisms of an arc-transitive 3-valent graph Γ_r. Since $|H| = 24$, the group G_r acts 4-arc-transitively on Γ_r. As G_r acts primitively on $\mathrm{V}\Gamma_r$, the graph Γ_r is connected.

We claim that the 2-nullity of Γ_r tends to infinity as r tends to infinity. Let V_r be the nullspace of the adjacency matrix A_r of Γ_r over $\mathbb{F}_2$. As G_r acts as a group of automorphisms of Γ_r, we can view V_r as a G_r-module. Since G_r is a simple group, it either centralises or acts faithfully on V_r. If G_r centralises V_r, then, since G_r acts transitively on the vertices of Γ_r, the module V_r must be a subspace of the one dimensional vector space spanned by the all-one vector e. Since Γ_r is a 3-valent graph, we have $A_r e = 3e \neq 0$ and hence $e \notin V_r$. By Corollary 5, we know that $V_r \neq 0$ and hence $V_r \nsubseteq \langle e \rangle$. This shows that G_r acts faithfully on V_r, that is, G_r is isomorphic to a subgroup of $\mathrm{GL}(V_r)$. Since the order of G_r tends to infinity with r, this implies that $\dim V_r$ also tends to infinity as r tends to infinity, as claimed. In particular $\{\Gamma_r \mid r \text{ prime}, r \equiv \pm 1 \mod 16\}$ is a family of connected 4-arc-transitive 3-valent graphs with unbounded 2-nullity. □

4 Graphs with semiregular groups of automorphisms

In this section, we will consider the p-nullity of graphs which admit the action of a *semiregular* group of automorphisms. (A permutation group is said to be semiregular if the stabiliser of each point is trivial.) Note that the much studied family of Cayley graphs is a special case of this situation. The existence of a semiregular group of automorphisms H of a graph Γ allows a more compact representation of the adjacency matrix A of Γ. Rather than considering A as a matrix of dimension $|\mathrm{V}(\Gamma)|$ with coefficients in a field $\mathbb{F}$, we can consider it as a matrix of dimension $|\mathrm{V}(\Gamma)|/|H|$ with coefficients in the group algebra $\mathbb{F}[H]$. (See [7] for a good reference about this approach.)

As an application of this approach, we will prove three results, the first two dealing with the p-nullity of certain Cayley graphs (see Sect. 5 and Sect. 6) and the third dealing with the p-nullity of vertex-transitive graphs with a power of p number of vertices (see Sect. 7). In the last of the three applications, it will prove useful to consider the p-nullity in the setting of multigraphs rather than graphs.

By a *multigraph*, we mean an ordered pair $\Gamma = (V, \mu)$, where V is the set of vertices and $\mu \colon V \times V \to \mathbb{N}$ satisfies $\mu(u, v) = \mu(v, u)$ and is called the *edge-multiplicity* function. The valency of a vertex $v \in V$ is defined by $\sum_{w \in \mathrm{V}} \mu(\{w, v\})$. Note that every graph can be considered as a multigraph by setting $\mu(u, v) = 1$

if $\{u, v\}$ is an edge and $\mu(u, v) = 0$ otherwise. The adjacency matrix of Γ is the $(|V| \times |V|)$-matrix whose rows and columns are indexed by elements of V in which the (u, v)-entry equals $\mu(\{u, v\})$. An automorphism of the multigraph $\Gamma = (V, \mu)$ is a permutation of V which preserves μ.

If $\mathbb{F}[V]$ is the free $\mathbb{F}$-module over V (that is, the vector space of all formal linear combinations of elements in V with coefficients in the field $\mathbb{F}$), then the adjacency matrix A may be viewed as the endomorphism of $\mathbb{F}[V]$ mapping a basis element $v \in V$ to the sum $\sum_{u\in V} \mu(\{v, u\})u$. As in the case of graphs, a permutation g of V is an automorphism of Γ if and only if the induced permutation representation of g on $\mathbb{F}[V]$ commutes with A.

Suppose now that Γ admits a group of automorphisms H acting semiregularly on V. Let $P_1, \dots, P_k$ denote the orbits of H and choose a reference vertex $v_i \in P_i$, for each i. The semiregularity of H allows us to identify each P_i with a copy of H (where v_i gets identified with $1 \in H$), in such a way that the regular action of H on P_i is permutation isomorphic to the action of H on itself by right multiplication. This identification, extended by linearity to $\mathbb{F}[V]$, defines an isomorphism ι of the space $\mathbb{F}[V]$ with

$$\mathbb{F}[H]^k = \mathbb{F}[H] \oplus \cdots \oplus \mathbb{F}[H],$$

the direct sum of $k = |V|/|H|$ copies of the group algebra $\mathbb{F}[H]$. The semiregular action of $h \in H$ on $\mathbb{F}[V]$ corresponds to the componentwise multiplication by the scalar $h \in \mathbb{F}[H]$ in $\mathbb{F}[H]^k$. In particular, $\mathbb{F}[V]$ is a free $\mathbb{F}[H]$-module. Also, the isomorphism ι identifies $\mathrm{M}_k(\mathbb{F}[H])$ with a subalgebra of $\mathrm{M}_{|V|}(\mathbb{F})$.

Since the action of the adjacency matrix A on $\mathbb{F}[V]$ commutes with each $h \in H$, the $\mathbb{F}$-endomorphism A of $\mathbb{F}[V]$ is also a $\mathbb{F}[H]$-endomorphism of the $\mathbb{F}[H]$-module $\mathbb{F}[V]$. Thus we can represent A as a $(k \times k)$-matrix over $\mathbb{F}[H]$.

Observe that the A-image of the ith standard basis vector e_i of $\mathbb{F}[H]^k = \mathbb{F}[V]$ is precisely the row of A indexed by the reference vertex $v_i \in P_i$. With respect to the standard basis $(e_i)_{i=1}^k$, the jth component of the ith row of A (as an element of $\mathrm{M}_k(\mathbb{F}[H])$) equals

$$\sum_{h\in H} \mu\bigl(\bigl\{v_i, v_j^h\bigr\}\bigr)h. \qquad (*)$$

More precisely, we have shown the following.

Proposition 6 *Let $\Gamma = (V, \mu)$ be a multigraph admitting a semiregular group of automorphisms H having k orbits on V. For each orbit P_i of H choose a vertex $v_i \in P_i$, and consider the matrix $A \in \mathrm{M}_k(\mathbb{F}[H])$ with the (i, j)-entry being the sum $(*)$ above. Then A is the adjacency matrix of Γ.*

This has the following straightforward consequence for Cayley graphs.

Corollary 7 *Let $\Gamma = \mathrm{Cay}(H, S)$ be a Cayley graph. The adjacency matrix of Γ is $\sum_{s\in S} s \in \mathbb{F}[H]$. Also, the nullity of Γ over $\mathbb{F}$ is the dimension over $\mathbb{F}$ of the right annihilator of the element $\sum_{s\in S} s$ in the group algebra $\mathbb{F}[H]$.*

Proof We use Proposition 6. Since H acts regularly on $\mathrm{V}\Gamma$, the group H has only one orbit on $\mathrm{V}\Gamma$, with reference point 1 say. Since S is the neighbourhood of 1 in Γ, we see that $\sum_{s\in S}\mu(\{1,s\})s=\sum_{s\in S}s$ is the adjacency matrix of Γ. The rest of the corollary follows. □

5 Arc-transitive dihedrants

In this section, we prove part (3) of Theorem 2. Recall that $d\geq 3$ and p is a prime. Let $a=p^k$ for some $k\geq 1$ and let $n=1+a+a^2+\cdots+a^{d-1}$. Denote by D_n the dihedral group of order $2n$ generated by $\{r,t\}$, where r has order n and t has order 2. Let $S=\{rt,r^at,r^{a^2}t,\dots,r^{a^{d-1}}t\}$ and consider the dihedrant $\Gamma_k=\mathrm{Cay}(\mathrm{D}_n,S)$. Clearly, Γ_k is a vertex-transitive graph with $2n$ vertices and valency d.

We claim that Γ_k is arc-transitive. Note that, since $\gcd(n,a)=1$, the function

$$\varphi:\begin{cases} r\mapsto r^a,\\ t\mapsto t\end{cases}$$

extends to an automorphism of D_n (which we still denote by φ) with $\langle\varphi\rangle$ acting transitively on the neighbours of 1 in Γ_k. Therefore $G=\mathrm{D}_n\rtimes\langle\varphi\rangle$ is an arc-transitive group of automorphisms of Γ_k with $G_1=\langle\varphi\rangle\cong\mathbb{Z}_d$ and Γ_k is an arc-transitive dihedrant.

Note that $\langle S\rangle=\langle rt,r^{a-1}\rangle=\langle rt,r^{\gcd(a-1,n)}\rangle$, which has index $\gcd(a-1,n)$ in D_n. This shows that Γ_k has $\gcd(a-1,n)=\gcd(a-1,d)$ connected components. In particular, the number of connected components of Γ_k is at most d. In the rest of the proof, we study the p-nullity of Γ_k.

Proof of part (3) of Theorem 2 We use the dihedrants Γ_k introduced above. Let $\bar{S}=\sum_{s\in S}s\in\mathbb{F}_p[\mathrm{D}_n]$. By Corollary 7, the p-nullity of Γ_k equals the dimension $\dim_{\mathbb{F}_p}(\mathrm{ann}(\bar{S}))$ over $\mathbb{F}_p$ of the right annihilator $\mathrm{ann}(\bar{S})$ of $\bar{S}$ in the group algebra $\mathbb{F}_p[\mathrm{D}_n]$. As t is a unit in the ring $\mathbb{F}_n[\mathrm{D}_n]$, we see that $\mathrm{ann}(\bar{S})=\mathrm{ann}(N)$, where $N=\sum_{l=0}^{d-1}r^{a^l}$.

Since the group algebra $\mathbb{F}_p[\mathrm{D}_n]$ splits into the direct sum $\mathbb{F}_p[\langle r\rangle]\oplus\mathbb{F}_p[\langle r\rangle]t$, if we let $\mathrm{ann}_{\langle r\rangle}(N)=\mathrm{ann}(N)\cap\mathbb{F}_p[\langle r\rangle]$, then $\mathrm{ann}(N)=\mathrm{ann}_{\langle r\rangle}(N)\oplus\mathrm{ann}_{\langle r\rangle}(N)t$. Hence $\dim_{\mathbb{F}_p}(\mathrm{ann}(N))$ equals twice the dimension of the right annihilator of N in $\mathbb{F}_p[\langle r\rangle]$, which we will now compute.

Identifying the elements of $\langle r\rangle$ with the corresponding matrices in the right regular permutation representation $\langle r\rangle\to\mathrm{GL}(n,\mathbb{F}_p)$, we have to compute the dimension of the kernel of the $(n\times n)$-matrix $N=r+r^a+\cdots+r^{a^{d-1}}$.

Let $p_r(T)$ be the characteristic polynomial of $r\in\mathrm{GL}(n,\mathbb{F}_p)$ over $\mathbb{F}_p$. Clearly, as r has order n, we have $p_r(T)=T^n-1$. Now, since $p_r(T)$ and $p_r'(T)=nT^{n-1}=T^{n-1}$ are coprime, it follows that $p_r(T)$ has n distinct roots in a suitable extension of $\mathbb{F}_p$, that is, r has n distinct eigenvalues in the algebraic closure of $\mathbb{F}_p$.

Note that the set of eigenvalues of $N=\sum_{l=0}^{d-1}r^{a^l}$ is $\{\sum_{l=0}^{d-1}\lambda^{a^l}\mid\lambda \text{ eigenvalue of } r\}$. Namely, if λ is an eigenvalue of r for the eigenvector v, then $\sum_{l=0}^{d-1}\lambda^{a^l}$ is an eigenvalue of N for the eigenvector v. In particular, the p-nullity of N is the number of common roots of $p_r(T)$ and $\sum_{l=0}^{d-1} T^{a^l}$. Write $g(T)=\sum_{l=0}^{d-1} T^{a^l}$ and $\mathrm{null}(N)$ for the p-nullity of N.

Let $f(T)=T^{a^d}-T$. Consider $E=\mathbb{F}_{a^d}$ and $F=\mathbb{F}_a$ the fields with a^d and a elements, respectively. As $|E|=a^d$, the elements of E are exactly the roots of the polynomial $f(T)$. Note that $g(T)^a=T^a+T^{a^2}+\cdots+T^{a^d}$ and hence $g(T)(g(T)^{a-1}-1)=g(T)^a-g(T)=T^{a^d}-T=f(T)$. In particular, the polynomial $g(T)$ divides $f(T)$ and hence the roots of $g(T)$ are elements of E. Moreover, since n divides a^d-1, we find that $p_r(T)$ divides $f(T)$ and hence the roots of $p_r(T)$ lie in E. This shows that the roots of $p_r(T)$ and $g(T)$ are elements of E.

We claim that the common roots of $p_r(T)$ and $g(T)$ are the elements of E of norm 1 and trace 0 in the Galois extension E/F. Indeed, if $x\in E$, then the norm of x in E/F is

$$\mathrm{N}_{E/F}(x)=\prod_{l=0}^{d-1} x^{a^l}=x^{\sum_{l=0}^{d-1} a^l}=x^n$$

and $\mathrm{N}_{E/F}(x)=1$ if and only if $p_r(x)=0$. Similarly, the trace of x in E/F is

$$\mathrm{Tr}_{E/F}(x)=\sum_{l=0}^{d-1} x^{a^l}=g(x)$$

and $\mathrm{Tr}_{E/F}(x)=0$ if and only if $g(x)=0$. Now, Moisio in [9, Sect. 3] obtains tight upper and lower bounds on the number of field elements in the finite extension E/F of norm 1 and trace 0, in particular from [9, Corollary 3.3] we obtain

$$(\dagger)\quad \mathrm{null}(N)\geq \frac{a^{d-1}-1}{a-1}-\gcd(a-1,d)a^{(d-2)/2}.$$

Denote by Γ_k^1 the connected component of Γ_k containing 1 and consider the family $\{\Gamma_k^1 \mid k\in\mathbb{N}\}$. By construction Γ_k^1 is a connected arc-transitive graph of valency d. As Γ_k has $\gcd(a-1,d)$ connected components, from (†) we see that Γ_k^1 has p-nullity at least $\frac{a^{d-1}-1}{\gcd(a-1,d)(a-1)}-a^{(d-2)/2}$. In particular, the p-nullity of Γ_k^1 tends to infinity as k tends to infinity and the proof is complete. □

Remark This proof of part (3) of Theorem 2 depends on deep number theoretic results about Kloosterman sums from [9, Sect. 3]. For $d>3$, it is possible to deduce that the number of common roots of $p_r(T)$ and $g(T)$ tends to infinity as a tends to infinity by using the Stepanov–Schmidt method and a theorem of A. Weil, (see [8] for a general account of the Stepanov–Schmidt method and [8, Theorem 6.61] for our particular application). This yields another proof of part (3) of Theorem 2 (for $d>3$).

6 2-arc-regular 3-valent generalised dihedrants

This section is devoted to the proof of part (4) of Theorem 2. In particular, we will construct an infinite family of connected 3-valent Cayley graphs Γ, admitting a 2-

arc-regular group of automorphisms A which contains a 1-arc-regular subgroup $\overline{A}$. We will then show that this family has an unbounded p-nullity for each prime p. We will make use of the theory developed in Sect. 4.

Construction 8 Let p be a prime and let n be a natural number. Let G_n be the group $(\langle i\rangle \times \langle j\rangle \times \langle g\rangle) \rtimes \langle h\rangle$, where $|i| = |j| = p^n$, $|g| = 3$, $|h| = 2$, $i^h = i^{-1}$, $j^h = j^{-1}$ and $g^h = g^{-1}$. (Such a group is sometimes called a generalised dihedral group over the abelian group $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n} \times \mathbb{Z}_3$.) Let $S_n = \{h, igh, jg^2h\}$ and let $\Gamma_n = \mathrm{Cay}(G_n, S_n)$.

Note that S_n consists of three involutions and hence Γ_n is a vertex-transitive 3-valent graph with $6p^{2n}$ vertices. It is not hard to see that, if $p \neq 3$, then $G_n = \langle h, igh, jg^2h\rangle$ and Γ_n is connected, whilst if $p = 3$, then Γ_n has 3 connected components.

We claim that Γ_n admits a group of automorphisms A_n acting 2-arc-regularly, and containing a subgroup $\overline{A_n}$ acting arc-regularly.

We leave to the reader to check that the map

$$\alpha : \begin{cases} i \mapsto j, \\ j \mapsto i, \\ g \mapsto g^2, \\ h \mapsto h \end{cases}$$

determines an automorphism of G_n fixing h and swapping igh and jg^2h. Similarly, the map

$$\beta : \begin{cases} i \mapsto i^{-1}j, \\ j \mapsto i^{-1}, \\ g \mapsto g, \\ h \mapsto igh \end{cases}$$

determines an automorphism of G_n acting as a 3-cycle on S_n. Since the automorphisms α and β of G_n fix S_n setwise, the groups $\overline{A_n} = G_n \rtimes \langle \beta\rangle$ and $A_n = G_n \rtimes \langle \alpha, \beta\rangle$ act arc-regularly and 2-arc-regularly on Γ_n, respectively, with $\overline{A_n} \subseteq A_n$, as required.

Proposition 9 *Let p be a prime and let n be a natural number. The p-nullity of the graph Γ_n from Construction 8 is at least $4p^n$.*

Proof Throughout the proof, we use the notation of Construction 8 but we drop the subscript n, writing G for G_n, S for S_n and Γ for Γ_n.

Let $\mathbb{F} = \mathbb{F}_p$ be the field of cardinality p. By a slight abuse of notation, we interpret S as the element $h + igh + jg^2h$ of the group algebra $\mathbb{F}[G]$. In view of Corollary 7, the p-nullity of Γ equals the dimension $\dim_{\mathbb{F}}(\mathrm{ann}_{\mathbb{F}[G]}(S))$ over $\mathbb{F}$ of the right annihilator of S in the ring $\mathbb{F}[G]$. As h is a unit of $\mathbb{F}[G]$, we see that $\mathrm{ann}_{\mathbb{F}[G]}(S) = \mathrm{ann}_{\mathbb{F}[G]}(N)$, where $N = 1 + ig + jg^2 \in \mathbb{F}[G]$.

Let $H = \langle i, j, g\rangle$ and observe that the group algebra $\mathbb{F}[G]$ splits (as a left $\mathbb{F}[H]$-module) into the direct sum $\mathbb{F}[H] \oplus \mathbb{F}[H]h$. Moreover, since $N \in \mathbb{F}[H]$, it follows that $\mathrm{ann}_{\mathbb{F}[G]}(N) = \mathrm{ann}_{\mathbb{F}[H]}(N) \oplus \mathrm{ann}_{\mathbb{F}[H]}(N)h$, and hence the $\mathbb{F}$-dimension of $\mathrm{ann}_{\mathbb{F}[G]}(N)$ equals twice the $\mathbb{F}$-dimension of the right annihilator $\mathrm{ann}_{\mathbb{F}[H]}(N)$ of N in $\mathbb{F}[H]$. To prove the proposition it therefore suffices to show that $\dim_{\mathbb{F}}(\mathrm{ann}_{\mathbb{F}[H]}(N)) \geq 2p^n$.

Write $e = 1 + g + g^2$ if $p \neq 3$ and $e = 0$ if $p = 3$. Since $\mathbb{F}$ has characteristic p and H is abelian, we have

$$N^{p^n} = 1^{p^n} + (ig)^{p^n} + \left(jg^2\right)^{p^n} = 1 + g^{p^n} + g^{2p^n} = e.$$

Hence $\mathrm{ann}_{\mathbb{F}[H]}(N) \subseteq \mathrm{ann}_{\mathbb{F}[H]}(N^{p^n}) = \mathrm{ann}_{\mathbb{F}[H]}(e)$. Thus $\mathrm{ann}_{\mathbb{F}[H]}(N)$ is equal to the kernel of the linear map

$$\tilde{N}\colon \mathrm{ann}_{\mathbb{F}[H]}(e) \to \mathrm{ann}_{\mathbb{F}[H]}(e), \quad \tilde{N}\colon x \mapsto Nx.$$

Now we compute the $\mathbb{F}$-dimension of $\mathrm{ann}_{\mathbb{F}[H]}(e)$. If $p = 3$, then $e = 0$ and hence $\dim_{\mathbb{F}}(\mathrm{ann}_{\mathbb{F}[H]}(e)) = 3p^{2n}$. If $p \neq 3$, then we show that $\dim_{\mathbb{F}}(\mathrm{ann}_{\mathbb{F}[H]}(e)) = 2p^{2n}$. Let $L = \langle i, j\rangle$ and let w be an arbitrary element of $\mathbb{F}[H]$. Then w can be written uniquely as $w = x + yg + zg^2$ for some $x, y, z \in \mathbb{F}[L]$. We have $ew = (1 + g + g^2)(x + yg + zg^2) = (x + y + z) + (x + y + z)g + (x + y + z)g^2$. Since $\mathbb{F}[H] = \mathbb{F}[L] \oplus \mathbb{F}[L]g \oplus \mathbb{F}[L]g^2$, it follows that $w \in \mathrm{ann}_{\mathbb{F}[H]}(e)$ if and only if $x + y + z = 0$. We conclude that $\mathrm{ann}_{\mathbb{F}[H]}(e)$ has $\mathbb{F}$-dimension $2p^{2n}$. Note that in both cases ($p = 3$ and $p \neq 3$), it follows that $\dim_{\mathbb{F}}(\mathrm{ann}_{\mathbb{F}[H]}(e)) \geq 2p^{2n}$.

Notice that $N^{p^n} = e$ implies that $\tilde{N}^{p^n} = 0$ and hence each Jordan block of N has size at most p^n. It follows that the kernel of $\tilde{N}$ has dimension at least $2p^{2n}/p^n = 2p^n$. To conclude the proof, recall that the p-nullity of Γ is twice the $\mathbb{F}$-dimension of $\mathrm{ann}_{\mathbb{F}[H]}(N)$. □

Proof of part (4) of Theorem 2 Using the notation from Construction 8, we already remarked that Γ_n is a 3-valent graph admitting a 2-arc-regular group of automorphisms with a 1-arc-regular subgroup. Moreover, if $p \neq 3$, then Γ_n is connected and hence, from Proposition 9, we see that $\{\Gamma_n \mid n \in \mathbb{N}\}$ is a family of graphs satisfying the hypothesis of part (4) of Theorem 2 and with unbounded p-nullity.

If $p = 3$, then Γ_n has 3 connected components. Denote one of these connected components by Γ_n'. Clearly, Γ_n' also admits a 2-arc-regular group of automorphisms with a 1-arc-regular subgroup. From Proposition 9, we find that Γ_n' has p-nullity at least $(4 \cdot 3^n)/3 = 4 \cdot 3^{n-1}$ and hence $\{\Gamma_n' \mid n \in \mathbb{N}\}$ is a family of graphs satisfying the hypothesis of part (4) of Theorem 2 and with unbounded p-nullity. □

7 Vertex-transitive graphs of prime power order

In contrast to the previous sections, where we were considering families of graphs with large p-nullity, this section is devoted to vertex-transitive graphs with trivial p-nullity. In particular, we will show that the p-nullity of a vertex-transitive graph on a power of p of vertices is zero provided that the valency of Γ is not divisible by p.

The main idea of the proof is based on the fact that such graphs admit a semiregular group of automorphisms of order p. We will use this group to reduce the problem to a smaller (multi)graph with the same properties and then proceed by induction. Besides the theory developed in Sect. 4 we will also need a result concerning quotient multigraphs, which we now briefly describe.

Let H be a group of automorphisms of a multigraph $\Gamma = (V, \mu)$ and let $\mathcal{P} = \{P_1, \dots, P_k\}$ be the partition of V into orbits of H. For each i, choose a reference vertex $v_i \in P_i$. We define the *quotient multigraph* Γ/H as the multigraph with vertex-set $\mathcal{P}$ and the edge-multiplicity of $\{P, Q\}$ in Γ/H is defined as the sum of the multiplicities $\mu(\{u, v\})$, where u is a fixed vertex of P and v runs through the neighbours of u in Q. Note that this sum is independent of the choice of the vertex u in P, and that we get the same value for the edge-multiplicity if we swap the roles of P and Q.

By the definition of the quotient multigraph Γ/H, the adjacency matrix A' of Γ/H is a $(k \times k)$-matrix with rows and columns indexed by the orbits $P_1, \dots, P_k$ of H, where the (P_i, P_j)-entry equals the sum

$$\sum_{u \in P_j} \mu\big(\{v_i, u\}\big) = \sum_{h \in H} \mu\big(\{v_i, v_j^h\}\big).$$

Note that the latter is precisely the value obtained from the (i, j)-entry of A (viewed as an element of $\mathrm{M}_k(\mathbb{F}[H])$) by applying the augmentation homomorphism $\varphi : \mathbb{F}[H] \to \mathbb{F}$, mapping each $h \in H$ to 1. We have thus proved the following interesting fact.

Proposition 10 *Let H be a semiregular group of automorphisms of a multigraph Γ and let A be the adjacency matrix of Γ, viewed as a $(k \times k)$-matrix over $\mathbb{F}[H]$. Then the adjacency matrix of the quotient multigraph Γ/H is the matrix obtained from A by applying the ring homomorphism $\hat{\varphi} : \mathrm{M}_k(\mathbb{F}[H]) \to \mathrm{M}_k(\mathbb{F})$ induced entry-wise by the augmentation homomorphism $\varphi : \mathbb{F}[H] \to \mathbb{F}$.*

Let us now prove the following simple lemma concerning local rings (i.e. rings with a unique maximal ideal).

Lemma 11 *Let R and S be commutative local rings and let $\varphi : R \to S$ be a surjective ring homomorphism. Let $\hat{\varphi}$ be the homomorphism from $\mathrm{M}_n(R)$ to $\mathrm{M}_n(S)$ induced by φ and let $A \in \mathrm{M}_n(R)$. Then, A is invertible in $\mathrm{M}_n(R)$ if and only if $A^{\hat{\varphi}}$ is invertible in $\mathrm{M}_n(S)$.*

Proof Recall that the set of invertible elements in a local ring is precisely the complement of the maximal ideal. Since a surjective ring homomorphism maps maximal ideals to maximal ideals, this shows that an element $r \in R$ is invertible in R if and only if r^{φ} is invertible in S. To conclude the proof, note that $\det(A^{\hat{\varphi}}) = (\det A)^{\varphi}$ and that a matrix is invertible if and only if its determinant is invertible. □

Finally, we prove the following key result relating the nullity of a multigraph with that of its quotient under an abelian p-group.

Proposition 12 *Let Γ be a vertex-transitive multigraph, let $\mathbb{F}$ be a field of characteristic p and let C be an abelian p-group of automorphisms of Γ, acting semiregularly on the vertices. Then, the adjacency matrix of Γ is invertible over $\mathbb{F}$ if and only if the adjacency matrix of Γ/C is invertible over $\mathbb{F}$.*

Proof Let k be the number of orbits of C on the vertices of Γ, let A be the adjacency matrix of Γ, viewed as a $(k \times k)$-matrix over $\mathbb{F}[C]$, and let A_C be the adjacency matrix of Γ/C. In view of Proposition 10, we have $A_C = A^{\hat{\varphi}}$, where $\hat{\varphi}$ denotes the mapping induced by the augmentation ring homomorphism $\varphi\colon \mathbb{F}[C] \to \mathbb{F}$.

Since C is a p-group and $\mathbb{F}$ has characteristic p, $\mathbb{F}[C]$ is a local ring (see [1, Corollary 3, Chap. I]). Hence, by Lemma 11, $A_C = A^{\hat{\varphi}}$ is invertible if and only if A is invertible. □

We conclude the paper with a nice application of Proposition 12.

Theorem 13 *Let p be a prime and let Γ be a vertex-transitive multigraph of valency d on n vertices. Let $\mathbb{F}$ be a field of characteristic p. If $\gcd(p, d) = 1$ and n is a power of p, then the adjacency matrix of Γ is invertible over $\mathbb{F}$.*

Proof The proof goes by induction on n. If $n = 1$, then Γ consists of a single vertex with d loops and its adjacency matrix is the (1×1)-matrix $[d]$. This matrix is invertible over $\mathbb{F}$ since $\gcd(p, d) = 1$.

We now assume that $n > 1$. Let $G = \mathrm{Aut}(\Gamma)$ and let P be a Sylow p-subgroup of G. Since n is a power of p, the group P acts transitively on the vertices of Γ. Let C be a central subgroup of P with $|C| = p$. Since C is central in P, it must act semiregularly on the vertices of Γ. Consider Γ/C. This is a vertex-transitive multigraph of valency d and $|\mathrm{V}(\Gamma/C)|$ is a strict divisor of n. By the induction hypothesis, the adjacency matrix of Γ/C is invertible over $\mathbb{F}$. Proposition 12 then completes the induction step and the proof. □

Acknowledgements We wish to thank Giuseppe Marino for pointing out and discussing the results in [9]. The second author is supported by UWA as part of the Australian Council Federation Fellowship Project FF0776186.

References

1. Alperin, J.L.: Local Representation Theory. Cambridge Studies in Advanced Mathematics, vol. 11. Cambridge University Press, Cambridge (1986)
2. Brouwer, A.E., van Eijl, C.A.: On the p-rank of the adjacency matrices of strongly regular graphs. J. Algebr. Comb. **1**, 329–346 (1992)
3. Godsil, C., Royle, G.: Algebraic Graph Theory. Graduate Texts in Mathematics, vol. 207. Springer, New York (2001)
4. Godsil, C., Royle, G.: Chromatic number and the 2-rank of a graph. J. Comb. Theory, Ser. B **81**, 142–149 (2001)
5. Haemers, W.H.: Matrices for graphs, designs and codes. In: Crnković, D., Tonchev, V. (eds.) Information Security, Coding Theory and Related Combinatorics, pp. 253–277. IOS Press, Amsterdam (2011)
6. Haemers, W.H., Peeters, R., van Rijckevorsel, J.M.: Binary codes of strongly regular graphs. Des. Codes Cryptogr. **17**, 187–209 (1999)

7. Kovács, I., Malnič, A., Marusič, D., Miklavič, S., Transitive group actions: (im)primitivity and semiregular subgroups. arXiv:math/0701686v1 [math.GR]
8. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, Cambridge (1984)
9. Moisio, M.M.: Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. Acta Arith. **134**, 329–349 (2008)
10. Potočnik, P., Spiga, P., Verret, G.: An explicit method for constructing arc-transitive graphs with unbounded vertex stabilisers (in preparation)
11. Potočnik, P., Spiga, P., Verret, G.: On graph-restrictive permutation groups. arXiv:1101.5186v2 [math.CO]
12. Rotman, J.J.: Projective planes, graphs, and simple algebras. J. Algebra **155**, 267–289 (1993)
13. Smith, K.J.C.: On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry. J. Comb. Theory **7**, 122–129 (1969)
14. Suzuki, M.: Group Theory I. Springer, New York (1982)
15. Tutte, W.T.: A family of cubical graphs. Proc. Camb. Philos. Soc. **43**, 459–474 (1947)
16. Weiss, R.: Presentation for (G,s)-transitive graphs of small valency. Math. Proc. Philos. Soc. **101**, 7–20 (1987)