Graphical Frobenius representations of non-abelian groups[*]

Gábor Korchmáros [ID]

Dipartimento di Matematica, Informatica ed Economia, Università della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy

Gábor P. Nagy [ID]

Department of Algebra, Budapest University of Technology and Economics, Egry József utca 1, H-1111 Budapest, Hungary, and
Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary

Abstract

A group G has a Frobenius graphical representation (GFR) if there is a simple graph Γ whose full automorphism group is isomorphic to G acting on the vertices as a Frobenius group. In particular, any group G with a GFR is a Frobenius group and Γ is a Cayley graph. By very recent results of Spiga, there exists a function f such that if G is a finite Frobenius group with complement H and $|G| > f(|H|)$ then G admits a GFR. This paper provides an infinite family of graphs that admit GFRs despite not meeting Spiga's bound. In our construction, the group G is the Higman group $A(f, q_0)$ for an infinite sequence of f and q_0, having a nonabelian kernel and a complement of odd order.

Keywords: Cayley graph, Frobenius group, Suzuki 2-group, Frobenius graphical representation.

Math. Subj. Class. (2020): 20B25, 05C25

1   Introduction

Graphs and their automorphism groups have intensively been investigated especially for vertex-transitive (and hence regular) graphs. Many contributions have concerned vertex-transitive graphs with large automorphism groups compared to the degree of the graph, and have in several cases relied upon deep results from group theory, such as the classification of primitive permutation groups.

On the other end, the smallest vertex-transitive automorphism groups of graphs occur

E-mail addresses: gabor.korchmaros@unibas.it (Gábor Korchmáros), nagyg@math.bme.hu (Gábor P. Nagy)

when the group is regular on the vertex-set. A group is said to have a graphical regular representation (GRR) if there exists a graph whose (full) automorphism group is isomorphic to G acting regularly on the vertex-set. Actually, almost all finite groups have GRRs. In fact, all the few exceptions were found in the 1970-80s by a common effort of G. Sabidussi, W. Imrich, M. E. Watkins, L. A. Nowitz, D. Hetzel, C. D. Godsil, and L. Babai, see [2, Section 1]. Since regular automorphism groups of a graph are those which are vertex transitive but contain no non-trivial automorphism fixing a vertex, a natural next choice as a small vertex-transitive automorphism group of a graph may be a Frobenius group on the vertex-set: an automorphism group of a graph that is vertex-transitive but not regular and only the identity fixes more than one vertex. It is well known that any group may be a Frobenius group in at most one way. Furthermore, each graph Γ with a (sub)group G of automorphisms acting regularly on the vertex-set is a Cayley graph $\mathrm{Cay}(G, S)$.

All these give a motivation for the study of Frobenius groups G which have a graphical Frobenius representation (GFR), that is, there exists a graph whose (full) automorphism group is isomorphic to G acting on the vertex-set as a Frobenius group. The systematic study of the GFR problem was initiated by J. K. Doyle, T. W. Tucker and M. E. Watkins in their recent paper [2]. As pointed out by those authors, the GFR problem is largely not analogous to the GRR problem since all groups have a regular representation whereas Frobenius groups have highly restricted algebraic structures. Nevertheless, they conjectured that like the GRR-case, "all but finitely many Frobenius groups with a given Frobenius complement have a GFR". Very recently Spiga [9, 10] was able to prove that conjecture for Cayley graphs and Cayley digraphs (digraphical Frobenius representations, or DFRs). Spiga combined combinatorial properties of Cayley graphs with some deeper results on the 1-point stabilizers of primitive permutation groups to obtain a function $f \colon \mathbb{N} \to \mathbb{N}$ such that if G is a finite Frobenius group with complement H satisfying $|G| > f(|H|)$, then G admits a GFR; see [10, Theorem 1.1], [9, Theorem 1], and Section 9.

It is apparent from Spiga's work and from the results, examples and classification of smaller groups with GFRs in [2], see in particular [2, Theorem 5.3 and Remark 5.4], that an interesting open problem is the explicit constructions of GFR for Frobenius groups G which do not meet Spiga's bound and whose kernel H is a non-abelian 2-group.

In this paper we provide such a construction. Our choice of Frobenius groups is influenced by Higman's classification of Suzuki 2-groups [5], as we take for G the group $A(f, q_0)$ from Higman's list where q_0 and $q = 2^f$ are 2-powers. The group $A(f, q_0)$ is a subgroup of G of $\mathrm{GL}(3, \mathbb{F}_q)$ whose main properties are recalled in Section 2. We build a Cayley graph Γ_u on the Frobenius kernel K of G, with a certain inverse closed subset S of K as connecting set, constructed from an element $u \in \mathbb{F}_q$. We show that G has GFR on Γ_u provided that $q = 2^f$, q_0 and u are carefully chosen.

Our notation and terminology are standard. For the definitions and known results on Frobenius groups which play a role in the present paper, the reader is referred to [2].

2   The group $A(f, q_0)$

Let $\mathbb{F}_q$ be the finite field of order $q = 2^f$ with $f \geq 4$, and let $q_0 = 2^{f_0}$ be another power of 2 smaller than q. For $a, c \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^*$, we write

$$\Phi_{a,c} = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ c & a^{q_0} & 1 \end{bmatrix}, \qquad \Psi_\lambda = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^{q_0+1} \end{bmatrix}.$$

We define the groups

$$K = \{\Phi_{a,c} \mid a, c \in \mathbb{F}_q\},$$
$$H = \{\Psi_\lambda \mid \lambda \in \mathbb{F}_q^*\}.$$

Then, K is a 2-group of order q^2 and H is a cyclic group of order $q - 1$. Moreover, H normalizes K, and its action fixes no nontrivial element in K. Their closure group is HK, and denoted by $A(f, q_0)$ in Higman's paper [5]. For brevity, we write G in place of $A(f, q_0)$. With this change $G = HK$. Since $H \cap H^g = 1$ holds for any $g \in G \setminus H$, G is a Frobenius group in its action on the set G/H of right cosets of H. The point stabilizer is H and K is a regular normal subgroup. It may be noticed that when $q = 2q_0^2$ then G is similar to the 1-point stabilizer of the Suzuki group $\mathrm{Sz}(q)$ in its double transitive action on $q^2 + 1$ points. A straightforward computation shows that the H-orbits on K are

$$\Omega_u = \{\Phi_{a,ua^{q_0+1}} \mid a \in \mathbb{F}_q^*\}, \qquad u \in \mathbb{F}_q, \tag{2.1}$$

and

$$\Omega_\infty = \{\Phi_{0,c} \mid c \in \mathbb{F}_q^*\}.$$

3   A Cayley graph arising from G

For every $u \in \mathbb{F}_q$, we may build a Cayley graph in the usual way:

$$\Gamma_u = \mathrm{Cay}(K, \Omega_u \cup \Omega_{u+1}).$$

Since $\Omega_u \cup \Omega_{u+1}$ is H-invariant, the group G induces automorphisms of Γ_u. This allows us to look at (the matrix group) G as a Frobenius group on $K = V(\Gamma_u)$. Our aim is to show that if q, q_0 and $u \in \mathbb{F}_q$ are carefully chosen then $\mathrm{Aut}(\Gamma_u)$ coincides with G. Define the set $\mathscr{U}_{q,q_0}$ of elements $u \in \mathbb{F}_q$ which satisfy both conditions:

(U1) $u = (1 + \eta^{q_0})/(\eta + \eta^{q_0})$ for some primitive element η of $\mathbb{F}_q$;

(U2)   the polynomial $X^{q_0+1} + uX^{q_0} + (u+1)X + 1$ has no roots in $\mathbb{F}_q$.

Then such an appropriate choice of the triple (q, q_0, u) is given in the following theorem.

Theorem 3.1. *Assume that $q - 1$ and $q_0^2 - 1$ are relatively prime. Then*

  (i) Γ_u is connected Cayley graph.

  (ii) If, in addition, $u \in \mathscr{U}_{q,q_0}$, then $\mathrm{Aut}(\Gamma_u) = G$, that is, G has a graphical Frobenius representation on Γ_u.

The question whether Theorem 3.1 provides an infinite family is also answered positively.

Theorem 3.2. *For infinitely many 2-powers q it is true that whenever the 2-power q_0 satisfies $\gcd(q - 1, q_0^2 - 1) = 1$, the set $\mathscr{U}_{q,q_0}$ is not empty.*

Computer calculations show that for many $u \notin \mathscr{U}_{q,q_0}$, the graph Γ_u is still a GFR for G. Hence, the conditions (U1) and (U2) are only needed for our proofs. However, $\mathscr{U}_{q,q_0} = \emptyset$ implies $\varphi(q)/q \leq 3$, which happens extremely rarely for $q = 2^f$, f odd; see Section 5.

4   Some more properties of the abstract structure of the group G

Lemma 4.1. *The following hold in K:*

(i) $\Phi_{a,c}^2 = \Phi_{0,a^{q_0+1}}$ and $\Phi_{a,c}^{-1} = \Phi_{a,c+a^{q_0+1}}$.

(ii) $\Phi_{a,c}^{-1}\Phi_{b,d}^{-1}\Phi_{a,c}\Phi_{b,d} = \Phi_{0,a^{q_0}b+ab^{q_0}}$.

(iii) Ω_∞ consists of central involutions of K.

(iv) For each $u \in \mathbb{F}_q$, we have $\Omega_u^{-1} = \Omega_{u+1}$.

Proof. Straightforward matrix computation. □

Lemma 4.2. *Assume that* $\gcd(q_0^2 - 1, q - 1) = 1$. *Then the following hold:*

(i) $K' = Z(K) = \{1\} \cup \Omega_\infty$.

(ii) K' and K/K' are elementary abelian 2-groups of order q.

(iii) For $u \in \mathbb{F}_q$, the set Ω_u generates K.

(iv) H acts transitively (hence irreducibly) on the nontrivial elements of K' and K/K'.

(v) The subgroup H is maximal in HK', which is maximal in G.

Proof. By the assumption, the map $a \mapsto a + a^{q_0}$ has kernel $\mathbb{F}_2$, and, $a \mapsto a^{q_0+1}$ is a bijection of $\mathbb{F}_q^*$. Hence, any element of $\mathbb{F}_q$ can be written in the form $a^{q_0}b + ab^{q_0}$, which implies (i). For $a \in \mathbb{F}_q^*$, we have $\Phi_{a,ua^{q_0+1}}^2 = \Phi_{0,a^{q_0+1}}$. Thus, $\Omega_\infty \subseteq \langle \Omega_u \rangle$ and (iii) follows. The rest is straightforward computation. □

Notice that Lemma 4.2(iii) yields Theorem 3.1(i).

5   On Conditions (U1) and (U2)

A natural key question regarding the applicability of Theorem 3.1 is the existence of some q such that $\mathscr{U}_{q,q_0}$ is not empty, that is, $\mathbb{F}_q$ contains an element u satisfying both Conditions (U1) and (U2). Theorem 3.2 states that infinitely many such q exist and we are going to show how to prove it using Euler's phi function and the Möbius function. For this purpose, we need some algebraic preparatory results stated in the next lemmas.

Lemma 5.1. *Let $q = 2^f$ be a power of 2 with odd exponent f. There exist at least $2(q+1)/3$ elements $u \in \mathbb{F}_q$ such that $X^{q_0+1} + uX^{q_0} + (u+1)X + 1$ has no roots in $\mathbb{F}_q$.*

Proof. Define the rational function

$$U(x) = \frac{x^{q_0+1} + x + 1}{x^{q_0} + x}.$$

Clearly, 0 and 1 are never roots of $X^{q_0+1} + uX^{q_0} + (u+1)X + 1$. Moreover, $X^{q_0+1} + uX^{q_0} + (u+1)X + 1$ has a root in $\mathbb{F}_q$ if and only if $u = U(x)$ for some $x \in \mathbb{F}_q \setminus \{0,1\}$. Since $U(0) = U(1) = \infty$ and

$$U(x) = U\left(\frac{x+1}{x}\right) = U\left(\frac{1}{x+1}\right)$$

identically, we have $|U(\mathbb{F}_q \setminus \{0,1\})| \le (q-2)/3$. Here we use the fact that $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_q$ and x, $(x+1)/x$, $1/(x+1)$ are distinct elements of $\mathbb{F}_q$. □

Lemma 5.2. *For infinitely many odd integers n, inequality $\varphi(2^n - 1)/(2^n - 1) > 1/3$ holds.*

Proof. The claim follows from the asymptotic formula of [7, Theorem 3]

$$\frac{1}{M} \sum_{1 \le m \le M} \frac{\varphi(2^m - 1)}{2^m - 1} = \mu + O(M^{-1} \log M),$$

with μ is given by the absolute convergent series

$$\mu = \sum_{d \text{ odd}} \frac{\mu(d)}{dt_d} \approx 0.73192,$$

where t_d is the multiplicative order of 2 modulo d, and $\mu(d)$ is the Möbius function; see [11, Theorem 4.1].

We give a second, elementary proof based on Fermat's Little Theorem. We show that for primes p, $\varphi(2^p - 1)/(2^p - 1) \to 1$. Let $r_1, \ldots, r_k$ be the different prime factors of $2^p - 1$. For $i = 1, \ldots, k$, let m_i be the order of 2 modulo r_i. Then $m_i \mid p$ and $p = m_i$. Moreover, $2^{r_i-1} \equiv 1 \pmod{r_i}$ implies $p \mid (r_i-1)$. In fact, $p \mid (r_i-1)/2$ and $r_i = 2s_i p + 1$ holds for some integer $s_i \ge 1$. This implies

$$k < \log_{2p}(2^p - 1) < \frac{p}{\log_2 p}.$$

Hence,

$$1 > \frac{\varphi(2^p - 1)}{2^p - 1} = \prod_{i=1}^{k} \left(1 - \frac{1}{r_i}\right) > \left(1 - \frac{1}{2p}\right)^{\frac{p}{\log_2 p}},$$

where the latter term converges to 1. This proves our claim. □

Remark 5.3. As pointed out in [8], much more is true: [7] implies that given any $\varepsilon > 0$, there is a $c > 0$ such that $\varphi(2^n - 1)/(2^n - 1) > c$ apart from a set of n with upper density $< \varepsilon$.

We are in a position to prove Theorem 3.2. By Lemma 5.2, it suffices to show that for an arbitrary odd integer f with $\varphi(2^f - 1)/(2^f - 1) > 1/3$, $q = 2^f$ fulfills the conditions of Theorem 3.2. Fix such an f and choose an arbitrary integer f_0, coprime to f. Then $q_0 = 2^{f_0}$ satisfies $\gcd(q - 1, q_0^2 - 1) = 1$. By the choice of f, $\mathbb{F}_q$ has more than $(q - 1)/3$ primitive elements. In our case, $x \mapsto x^{q_0-1}$ is bijective in $\mathbb{F}_q$, hence the maps

$$\eta \mapsto \eta' = \frac{1 + \eta^{q_0}}{\eta + \eta^{q_0}}, \qquad u \mapsto u' = 1 + \left(\frac{u}{u+1}\right)^{\frac{1}{q_0-1}}$$

are well-defined inverses to each other. Now, the claim follows from Lemma 5.1.

6 Incidences

Recall that Γ_u denotes the Cayley graph $\mathrm{Cay}(K, \Omega_u \cup \Omega_{u+1})$, where the vertices of Γ_u are the elements of K and Ω_u is defined in (2.1). The identity $\Phi_{0,0}$ of K will also be denoted by ε. The group $G = HK$ acts on K, the action is induced as follows: The elements of

K act in the right regular action and the elements of H act by conjugation. In the sequel, we identify G with its permutation action on K, whereby some caution is required since for a subset X of K, the point-wise stabilizer of X in G and the centralizer of X in G are in general different. As a permutation group, G is a subgroup of the automorphism group $\mathrm{Aut}(\Gamma_u)$, and H is its cyclic subgroup of order $q - 1$, fixing ε and preserving both Ω_u and Ω_{u+1}. Formally, ε is viewed as an element of $\mathrm{Aut}(\Gamma_u)$; nevertheless, we will also use the notation id to denote the trivial automorphism of $\mathrm{Aut}(\Gamma_u)$.

For any two elements $\Phi_{a,c}, \Phi_{b,d} \in K$ with $\Phi_{a,c}\Phi_{b,d}^{-1} \in \Omega_u$, we introduce the directed edge notation $\Phi_{a,c} \xrightarrow{u} \Phi_{b,d}$ in Γ_u and we refer to it as a u-edge. It should be noticed that our notation is not the usual one for Cayley digraphs, where the arrows point in the opposite direction. An obvious observation is that the following are equivalent:

(i) $\Phi_{a,c} \xrightarrow{u} \Phi_{b,d}$,

(ii) $\Phi_{a,c}\Phi_{b,d}^{-1} \in \Omega_u$,

(iii) $c + d = (a + b)^{q_0}(ua + (u + 1)b)$,

(iv) $c + d = u(a + b)^{q_0+1} + a^{q_0}b + b^{q_0+1}$.

Now we collect some incidences in Γ_u which play a role in our proof.

Lemma 6.1. *Assume* $\gcd(q - 1, q_0^2 - 1) = 1$ *and define*

$$\eta = 1 + \left(\frac{u}{u+1}\right)^{\frac{1}{q_0-1}}$$

for $u \in \mathbb{F}_q \setminus \{0, 1\}$. *Then the following hold in* Γ_u *for* $a, b \neq 0$:

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u} \Phi_{b,ub^{q_0+1}} \quad \Longleftrightarrow \quad b = \frac{a}{\eta}, \tag{6.1a}$$

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u+1} \Phi_{b,ub^{q_0+1}} \quad \Longleftrightarrow \quad b = a\eta, \tag{6.1b}$$

$$\Phi_{a,(u+1)a^{q_0+1}} \xrightarrow{u} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow b = a \cdot \frac{\eta}{1+\eta}, \tag{6.1c}$$

$$\Phi_{a,(u+1)a^{q_0+1}} \xrightarrow{u+1} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow b = a \cdot \frac{1+\eta}{\eta}, \tag{6.1d}$$

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow b = \frac{a}{1+\eta}, \tag{6.1e}$$

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u+1} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow \left(\frac{a}{b}\right)^{q_0+1} + u\left(\frac{a}{b}\right)^{q_0} + (u+1)\left(\frac{a}{b}\right) + 1 = 0. \tag{6.1f}$$

Proof. (6.1a): Since Γ_u has no loops, we may assume $a \neq b$.

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u} \Phi_{b,ub^{q_0+1}} \Longleftrightarrow ua^{q_0+1} + ub^{q_0+1} = (a + b)^{q_0}(ua + (u + 1)b)$$
$$\Longleftrightarrow 0 = (u+1)a^{q_0}b + uab^{q_0} + b^{q_0+1}$$
$$\Longleftrightarrow 0 = (u+1)\left(\frac{a}{b}\right)^{q_0} + u\left(\frac{a}{b}\right) + 1$$
$$\Longleftrightarrow 0 = (u+1)\left(\frac{a}{b} + 1\right)^{q_0} + u\left(\frac{a}{b} + 1\right)$$

$$\Longleftrightarrow \left(\frac{a}{b}+1\right)^{q_0-1} = \frac{u}{u+1} = (\eta+1)^{q_0-1}$$
$$\Longleftrightarrow \frac{a}{b} = \eta.$$

Since $(u+1)$-edges are reversed u-edges, we obtain (6.1b) by switching a and b in the computation above. To show (6.1d), we replace u by $u+1$ and use the computation above to obtain

$$\Phi_{a,(u+1)a^{q_0+1}} \xrightarrow{u+1} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow \left(\frac{a}{b}+1\right)^{q_0-1} = \frac{u+1}{u} = \left(\frac{1}{1+\eta}\right)^{q_0-1}$$
$$\Longleftrightarrow \frac{a}{b} = \frac{\eta}{1+\eta}.$$

This proves (6.1c) by switching a and b. For (6.1e):

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow ua^{q_0+1}+(u+1)b^{q_0+1} = (a+b)^{q_0}(ua+(u+1)b)$$
$$\Longleftrightarrow 0 = (u+1)a^{q_0}b + uab^{q_0}$$
$$\Longleftrightarrow \left(\frac{a}{b}\right)^{q_0-1} = \frac{u}{u+1} = (\eta+1)^{q_0-1}$$
$$\Longleftrightarrow \frac{a}{b} = 1+\eta.$$

Finally,

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u+1} \Phi_{b,(u+1)b^{q_0+1}} \Longleftrightarrow ua^{q_0+1}+(u+1)b^{q_0+1} = (a+b)^{q_0}((u+1)a+ub)$$
$$\Longleftrightarrow 0 = a^{q_0+1}+ua^{q_0}b+(u+1)ab^{q_0}+b^{q_0+1}$$
$$\Longleftrightarrow 0 = \left(\frac{a}{b}\right)^{q_0+1}+u\left(\frac{a}{b}\right)^{q_0}+(u+1)\left(\frac{a}{b}\right)+1,$$

which shows (6.1f). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Our next step is to describe the structure of the neighborhood of the vertex ε in Γ_u. For this purpose, we recall the concept of *generalized Petersen graphs* [3]. Let n and k be integers with $1 \le k < n/2$, the vertex set of $\mathrm{GPG}(n,k)$ is $\{c_1,\ldots,c_n,c_1',\ldots,c_n'\}$ and the edge set consists of all pairs of the form

$$c_ic_{i+1}, \qquad c_ic_i', \qquad c_ic_{i+k}', \qquad i \in \{1,\ldots,n\},$$

where all subscripts are to be read modulo n. In order to describe the automorphism group of $\mathrm{GPG}(n,k)$, define the permutations

$$\rho\colon c_i \mapsto c_{i+1}, \quad c_i' \mapsto c_{i+1}',$$
$$\delta\colon c_i \mapsto c_{-i}, \quad c_i' \mapsto c_{-i}',$$
$$\alpha\colon c_i \mapsto c_{ki}', \quad c_i' \mapsto c_{ki}$$

for all $i \in \{1,\ldots,n\}$. By [3, Theorem 1 and 2],

$$\langle \rho,\delta \rangle \le \mathrm{Aut}(\mathrm{GPG}(n,k)) \le \langle \rho,\delta,\alpha \rangle$$

provided that $n \notin \{4, 5, 8, 10, 12, 24\}$. Moreover, the generators ρ, δ, satisfy the relations $\rho^n = \delta^2 = \text{id}$, $\delta\rho\delta = \rho^{-1}$, hence, $\langle \rho, \delta \rangle$ is isomorphic to the dihedral group of order $2n$. Also, $\alpha\delta = \delta\alpha$, $\alpha^2 \in \{\text{id}, \delta\}$, and most importantly $\alpha^{-1}\rho\alpha = \rho^k$. This implies the following lemma:

Lemma 6.2. *Let n be an odd integer, $n \neq 5$, and $1 \leq k < n$. In $\text{Aut}(\text{GPG}(n, k))$, the following properties hold:*

   (i) The elements of odd order form a unique cyclic normal subgroup of order n.

   (ii) For $k \neq \pm 1$, no involution commutes with the cyclic normal subgroup of order n.   □

Proposition 6.3. *Assume $\gcd(q - 1, q_0^2 - 1) = 1$ and $u \in \mathcal{U}_{q,q_0}$. Then, the neighborhood $\Omega_u \cup \Omega_{u+1}$ of ε in Γ_u is isomorphic to the generalized Petersen graph $\text{GPG}(q - 1, k)$, where $u = (1 + \eta^{q_0})/(\eta + \eta^{q_0})$ and the integer k is defined by $1 + \eta = \eta^{k+1}$.*

Proof. By the choice of u, η is a primitive element of $\mathbb{F}_q$. Define

$$c_i = \Phi_{\eta^i, u\eta^{i(q_0+1)}}, \qquad c_i' = \Phi_{\eta^i/(1+\eta), (u+1)(\eta^i/(1+\eta))^{q_0+1}}.$$

From Lemma 6.1, $c_i c_{i+1}$, $c_i c_i'$ are edges and there are no more edges in Ω_u and between Ω_u and Ω_{u+1}. In Ω_{u+1}, c_i' and c_j' are connected with an u-edge if and only if

$$\frac{\eta^j}{1+\eta} = \frac{\eta^i}{1+\eta} \cdot \frac{1+\eta}{\eta} \iff \eta^{j-i+1} = 1 + \eta = \eta^{k+1} \iff j \equiv i + k \pmod{q-1}.$$

This finishes the proof.   □

Notice that $k = \pm 1$ would imply $\eta = 0$ or $1 + \eta + \eta^2 = 0$, which is not possible if $\gcd(q - 1, q_0^2 - 1) = 1$ and η generates $\mathbb{F}_q^*$.

Corollary 6.4. *Assume $\gcd(q - 1, q_0^2 - 1) = 1$ and $u \in \mathcal{U}_{q,q_0}$. Let A be the permutation group induced by the stabilizer $\text{Aut}(\Gamma_u)_\varepsilon$ on $\Omega_u \cup \Omega_{u+1}$. Then A is solvable, its order is either $(q - 1)$, $2(q - 1)$ or $4(q - 1)$, and it has a unique cyclic normal subgroup of odd order $q - 1$. Moreover, $\text{Aut}(\Gamma_u)_\varepsilon$ either preserves Ω_u and Ω_{u+1}, or it interchanges them.*

Proof. A contains the cyclic subgroup of order $q - 1$ that is induced by H on $\Omega_u \cup \Omega_{u+1}$. Proposition 6.3 and Lemma 6.2 apply.   □

We finish this section with another property of the stabilizer of ε in $\text{Aut}(\Gamma_u)$.

Lemma 6.5. *Assume $\gcd(q - 1, q_0^2 - 1) = 1$ and $u \in \mathcal{U}_{q,q_0}$.*

   (i) Let A be the centralizer of the commutator subgroup K' in $\text{Aut}(\Gamma_u)$. Then $K \leq A$ and $|A : K| \leq 2$. Moreover, any element of $A \setminus K$ interchanges the sets Ω_u and Ω_{u+1}.

   (ii) Let $\alpha \in \text{Aut}(\Gamma)$ be an involution which centralizes H. Then α fixes $\Omega_u \cup \Omega_{u+1}$ point-wise.

Proof. (i): Obviously, $K \le A$ and A is transitive. From the last sentence of Corollary 6.4, an element $\alpha \in A_\varepsilon$ either preserves Ω_u and Ω_{u+1}, or it interchanges them. We show that if α preserves Ω_u then $\alpha = $ id. This will imply $|A_\varepsilon| \le 2$ and $|A| \le 2q^2$. Since α commutes with K' and fixes ε, it fixes all points in the orbit $\varepsilon^{K'} = \{\varepsilon\} \cup \Omega_\infty$. The elements $\Phi_{a,ua^{q_0+1}} \in \Omega_u$ and $\Phi_{0,d} \in K'$ satisfy both relations

$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u} \Phi_{0,d} \iff d = 0,$$
$$\Phi_{a,ua^{q_0+1}} \xrightarrow{u+1} \Phi_{0,d} \iff d = a^{q_0+1}.$$

This means that each element in Ω_u is connected with a unique element in Ω_∞. Hence, α fixes all elements in Ω_u. As each K'-orbit contains a unique element in Ω_u, we see that each K'-orbit is preserved. Once again, α commutes with K' and fixes an element in each K'-orbit. Therefore, α fixes all points in each K'-orbit.

(ii): As ε is the unique fixed point of H, $\varepsilon^\alpha = \varepsilon$ and α leaves the neighborhood $\Omega_u \cup \Omega_{u+1}$ of ε invariant. By Lemma 6.2(ii), the restriction of α to $\Omega_u \cup \Omega_{u+1}$ cannot have order 2, therefore, it must be trivial. □

7   Imprimitivity

In this section we show that an appropriate choice of $u \in \mathbb{F}_q$ ensures that $\mathrm{Aut}(\Gamma_u)$ cannot act primitively on the set of vertices of Γ_u. We recall that a primitive permutation group G is of *affine type* if it has an abelian regular normal subgroup, which is necessarily elementary abelian of order r^n for some prime r. In this case G is embedded in the affine group $\mathrm{AGL}(n, r)$ with the socle being the translation subgroup. Its stabiliser of $0 \in \mathbb{F}_r^n$ is a subgroup of $\mathrm{GL}(n, r)$ which acts irreducibly on $\mathbb{F}_r^n$. For our purpuse, a useful tool is the following result by Guralnick and Saxl.

Proposition 7.1 (Guralnick and Saxl [4]). *Let G be a primitive permutation group of degree 2^n. Then either G is of affine type, or G has a unique minimal normal subgroup $N = S \times \cdots \times S = S^t$, $t \ge 1$, S is a non-abelian simple group, and one of the following holds:*

(i) *$S = A_m$, $m = 2^e \ge 8$, $n = te$, and the 1-point stabilizer in N is $N_1 = A_{m-1} \times \cdots \times A_{m-1}$, or*

(ii) *$S = \mathrm{PSL}(2, p)$, $p = 2^e - 1 \ge 7$ is a Mersenne prime, $n = te$, and the 1-point stabilizer in N is the direct product of maximal parabolic subgroups each stabilizing a 1-space.*

Lemma 7.2. *Let G be a group acting transitively on the set X. For $x \in X$ and let $H = G_x$ be the stabilizer of x in G.*

(i) *For $y \in X$, choose $g \in G$ such that $y = x^g$. Then the subgroup of H, fixing the H-orbit of y point-wise, coincides with $\cap_{h \in H} H^{gh}$.*

(ii) *If G is 2-transitive on X then $\cap_{h \in H} H^{gh}$ is either H or $\{1\}$, depending upon whether $g \in H$ or $g \notin H$.*

Proof. If $y' \in y^H$, then $y' = y^h = x^{gh}$ for some $h \in H$. Hence, for the stabilizer we have $G_{y'} = G_x^{gh} = H^{gh}$. Therefore, the point-wise stabilizer of y^H is $\cap_{y' \in y^H} G_{y'} = \cap_{h \in H} H^{gh}$. This proves (i). Clearly, if $g \in H$ then $\cap_{h \in H} H^{gh} = H$. If $g \in G \setminus H$ then $x \ne y = x^g$ and $\cap_{h \in H} H^{gh}$ fixes all points in $\{x\} \cup y^H$. The latter set is X if G is 2-transitive. □

Lemma 7.3. *Assume* $\gcd(q - 1, q_0^2 - 1) = 1$ *and* $u \in \mathscr{U}_{q,q_0}$. *If* $\mathrm{Aut}(\Gamma_u)$ *acts primitively on* Γ_u, *then its action is of affine type.*

Proof. Let us assume on the contrary that $\mathrm{Aut}(\Gamma_u)$ is not of affine type. Let N be its unique minimal normal subgroup. With the notation in Proposition 7.1, we have $N = S^t$ where either $S = A_m$, $m \geq 8$, or $S = \mathrm{PSL}(2, p)$, with a Mersenne prime $p = m - 1 \geq 7$. In both cases, S has a 2-transitive action on m points. Moreover, if B is the 1-point stabilizer in S, then the point stabilizer of $\varepsilon = \Phi_{0,0}$ in N is $N_\varepsilon = B^t$. For $(g_1, \ldots, g_t) \in S^t$ take a generic vertex $y = \varepsilon^{(g_1, \ldots, g_t)}$ of Γ_u. Let Y be the B^t-orbit of y. By Lemma 7.2(i) the point-wise stabilizer of Y is

$$(\cap_{b \in B} B^{g_1 b}) \times \cdots \times (\cap_{b \in B} B^{g_t b}).$$

By Lemma 7.2(ii), each factor is either $\{1\}$ or B, depending upon whether $g_i \in B$ or not. Thus, the point-wise stabilizer of Y in B^t is B^{t_0}, where $0 \leq t_0 \leq t$, and $t_0 = t$ occurs if and only if $Y = \{\varepsilon\}$. Therefore, the B^t induces a permutation group on Y which is isomorphic to B^{t_1}, where $t_1 = t - t_0$. Furthermore, $t_1 = 0$ if and only if $Y = \{\varepsilon\}$.

The stabilizer N_ε acts on $\Omega_u \cup \Omega_{u+1}$. Let Y be a nontrivial N_ε-orbit contained in $\Omega_u \cup \Omega_{u+1}$. If $S = A_m$, then N_ε induces a nonsolvable group of automorphisms of $\Omega_u \cup \Omega_{u+1}$. If $S = \mathrm{PSL}(2, p)$, then $|B| = p(p-1)/2$, and N_ε induces a noncyclic group of odd order on $\Omega_u \cup \Omega_{u+1}$. Both possibilities are inconsistent with Corollary 6.4. $\square$

We are now able to prove the imprimitivity of $\mathrm{Aut}(\Gamma_u)$.

Proposition 7.4. *Assume* $\gcd(q - 1, q_0^2 - 1) = 1$ *and* $u \in \mathscr{U}_{q,q_0}$. *Then,* $\mathrm{Aut}(\Gamma_u)$ *acts imprimitively on* Γ_u.

Proof. As before, G is identified with its permutation action on Γ_u. In particular, we consider H, K as subgroups of $\mathrm{Aut}(\Gamma_u)$. At the same time, K is the set of vertices of Γ_u.

Assume on the contrary that $\mathrm{Aut}(\Gamma_u)$ is primitive, hence of affine type by Lemma 7.3. Let N be the unique minimal normal subgroup of $\mathrm{Aut}(\Gamma_u)$. Then N is a regular elementary abelian 2-group. Since H has odd order, N decomposes into the direct product of H-invariant subgroups. For any $1 \neq h \in H$ and $1 \neq n \in N$, h has a unique fixed point, while n has no fixed point. Hence $nh \neq hn$. Therefore $N = A_1 \times A_2$ where A_i is an elementary abelian group of order q and H acts regularly on $A_i \setminus \{1\}$, $i = 1, 2$. Consider the subgroup $M = N_{NK}(K)$. Since NK is nilpotent, we have $K \lneq M$ and $K' \lhd M$. The latter implies $K' \cap Z(M) \neq \{1\}$. Since both K' and $Z(M)$ are H-invariant while H acts regularly on $K' \setminus \{1\}$, we have $K' \leq Z(M)$. By Lemma 6.5, $|M : K| = 2$. On the one hand, $M = (M \cap N)K$. On the other hand, $N \cap K$ is an H-submodule of $M \cap N$. By Maschke's Theorem [1, (10.8)] applied to $M \cap N$, viewed as a $\mathbb{F}_2$-vector space, there is an H-invariant subgroup B in $M \cap N$ such that $M \cap N = B \times (N \cap K)$. Therefore,

$$B \cong (M \cap N)/(N \cap K) \cong (M \cap N)K/K \cong M/K \cong \mathbb{F}_2,$$

that is, the nontrivial element of $B \leq N$ commutes with H, a contradiction. $\square$

8   Proof of the main result Theorem 3.1(ii)

In this section, we complete the proof of Theorem 3.1. As before, G is identified with its permutation action on Γ_u. From Proposition 7.4, we know that $A = \mathrm{Aut}(\Gamma_u)$ acts

imprimitively on Γ_u. We claim that the only nontrivial blocks of imprimitivity of A are the cosets of the commutator subgroup K' of K. Or equivalently, K' is the only nontrivial block containing ε. Let B be an arbitrary nontrivial block of imprimitivity of A which contains ε. Then the stabilizer of the set B in G is a subgroup G_B of G, lying properly between H and G. By Lemma 4.2(v), $G_B = HK'$ and $B = K'$, which proves the claim. The next two lemmas describe the point-wise stabilizer of K' in A.

Lemma 8.1. *Let E be the point-wise stabilizer of $K' = \{\varepsilon\} \cup \Omega_\infty$ in $\mathrm{Aut}(\Gamma_u)$. Then E is either trivial or it is an elementary abelian 2-group which fixes all pairs $\{\Phi_{a,c}, \Phi_{a,c}^{-1}\}$.*

Proof. The observations made prior to Lemma 6.1 show

$$\Phi_{a,c} \xrightarrow{u} \Phi_{0,d} \iff d = c + ua^{q_0+1}$$

for all $a, c, d \in \mathbb{F}_q$. Thus, any vertex $\Phi_{a,c}$, $a \neq 0$, is u-connected to a unique element Φ_{0,d_1} of K' and $(u+1)$-connected to a unique element Φ_{0,d_2} of K', where $d_1 = c + ua^{q_0+1}$ and $d_2 = c + (u+1)a^{q_0+1}$. If d_1 and d_2 are distinct nonzero elements, then Φ_{0,d_1}, Φ_{0,d_2} are distinct vertices in Ω_∞, whose common neighbors are $\Phi_{a,c}$ and $\Phi_{a,c}^{-1} = \Phi_{a,c+a^{q_0+1}}$, where

$$a = (d_1 + d_2)^{\frac{1}{q_0+1}} \quad \text{and} \quad c \in \{d_1 + ua^{q_0+1}, d_2 + ua^{q_0+1}\}.$$

This shows that any automorphism of Γ_u, which fixes Ω_∞ point-wise, must leave the pair $\{\Phi_{a,c}, \Phi_{a,c}^{-1}\}$ invariant. It follows that E either trivial or has exponent 2 and in the latter case E is elementary abelian. $\qquad\square$

Actually, E is trivial by the following lemma.

Lemma 8.2. *The only automorphism that fixes $\{\varepsilon\} \cup \Omega_\infty$ point-wise is the identity.*

Proof. Let E be defined as in Lemma 8.1. Since HK' preserves the set of vertices in K', HK' normalizes E. Assume on the contrary that $E \neq \{1\}$, then $C_E(K') \neq \{1\}$ is H-invariant. Since K' acts regularly on itself, $E \cap K' = \{1\}$. We apply Lemma 6.5(i) to conclude that $|C_E(K')| = 2$. This means that there is a unique involutory automorphism $\alpha \in A$ which centralizes both K' and H. Now, Lemma 6.5(ii) implies that α fixes $\Omega_u \cup \Omega_{u+1}$ point-wise. Finally, Lemma 6.5(i) yields $\alpha \in K$, a contradiction. $\qquad\square$

Let us now focus on the point stabilizer A_ε of ε in $A = \mathrm{Aut}(\Gamma_u)$. Clearly, A_ε leaves $\Omega_u \cup \Omega_{u+1}$ invariant. Moreover, by the imprimitivity of A, A_ε preserves Ω_∞ as well. Since any element of Ω_u is connected with a unique element of Ω_∞, each automorphism fixing all points in $\{\varepsilon\} \cup \Omega_u \cup \Omega_{u+1}$ fixes all points in Ω_∞. Hence by Lemma 8.2, the action of A_ε on $\Omega_u \cup \Omega_{u+1}$ is faithful and the possibilities for $|A_\varepsilon|$ are $q - 1$, $2(q-1)$ or $4(q-1)$ by Corollary 6.4.

Let S denote the stabilizer of the set K' in A. On the one hand, $HK' \leq S$, hence S is transitive on K'. On the other hand, $A_\varepsilon \leq S$ since K' is a block of imprimitivity. Therefore, $A_\varepsilon = S_\varepsilon$, and

$$|S| = q|A_\varepsilon| \in \{q(q-1), 2q(q-1), 4q(q-1)\}.$$

This implies that S induces a 2-transitive solvable permutation group $\bar{S}$ on K'. Since the order of K' is a power of 2, Huppert's Theorem [6, Theorem XII.7.3] yields that $\bar{S}$ is similar to a subgroup of the group $\mathrm{A\Gamma L}(1, q)$ of all semilinear mappings

$$z \mapsto az^\alpha + b, \qquad a, b \in \mathbb{F}_q, a \neq 0, \alpha \in \mathrm{Aut}(\mathbb{F}_q)$$

on $\mathbb{F}_q$. Here, $|A\Gamma L(1,q)| = fq(q-1)$ for $q = 2^f$. Since $\gcd(q-1, q_0^2 - 1) = 1$, f is odd, and the only possibility for the cardinality of $\bar{S}$ is $q(q-1)$. We apply Lemma 8.2 once more to conclude that $|S| = q(q-1)$, which implies $A_\varepsilon = H$ and $A = HK = G$. This finishes the proof of Theorem 3.1(ii).

Remark 8.3. Since the proof of Lemma 8.2 depends on Huppert's classification of solvable 2-transitive groups of degree $2^h + 1$, a natural question is whether the possibility $|S| \in \{2q(q-1), 4q(q-1)\}$ can be ruled out by purely combinatorial arguments based on the structure of the graph Γ_u rather than by the use of Huppert's classification. We are likely to think that the answer is negative. In fact, the action of an extra-automorphism in case $|S| \in \{2q(q-1), 4q(q-1)\}$ does not seem to produce further useful constraint on the structure of the graph G_u in the case where the kernel K is nonabelian and the complement H has odd order. Actually, as Spiga himself pointed out in [10, Section 1.1], this case is by far the hardest in the GFR problem.

9 Spiga's bound

To state Spiga's bound we need some notation consistent with that used in [9]. For a Frobenius group $G = N \rtimes H$ with kernel N and complement H, let

$$d_{11}(|N|, |H|) = 1 + \frac{|N| - 1}{|H|} - \left(\frac{\sqrt{|N|}}{4} - (\log_2 |N|)^2 \right);$$

$$d_{12}(|N|, |H|) = 1 + \frac{|N| - 1}{|H|} - \left(\frac{\sqrt{|N|} - 1 - |H|}{|H|(1 + 2|H|)} \log_2 \tfrac{4}{3} - 2\log_2 \sqrt{|N|} + 1 \right);$$

$$d_1(|N|, |H|) = (\log_2 |N|)^2;$$

$$f_1(|N|, |H|) = 2^{d_1(|N|,|H|)} (\tfrac{1}{2}|N| - 1) \max\{ 2^{d_{11}(|N|,|H|)}, 2^{d_{12}(|N|,|H|)} \};$$

$$c_2(|N|, |H|) = \frac{3}{4} \frac{|N|}{|H|} - \frac{1}{2|H|} + \frac{1}{2} + \sqrt{|N|} \frac{|H| - 1}{2|H|} + (\log_2 |N|)^2;$$

$$f_2(|N|, |H|) = 2^{c_2(|(N|,|H|)};$$

$$d_{31}(|N|, |H|) = \left(\frac{2|N|}{|H|} \right)^{\frac{2}{3}} - 2|H|\sqrt{|N|};$$

$$d_{32}(|N|, |H|) = \sqrt{N};$$

$$d_{33}(|N|, |H|) = 4\sqrt{|N|} - 2|H|\sqrt[4]{|N|};$$

$$F_3(|N|, |H|) = \frac{1}{4|H|} \min\{ d_{31}(|N|, |H|), d_{32}(|N|, |H|), d_{33}(|N|, |H|) \};$$

$$c_3(|N|, |H|) = \frac{3}{2} + \frac{|N|}{|H|} + \frac{1}{2|H|} - F_3(|N|, |H|) + (\log_2 |N|)^2;$$

$$f_3(|N|, |H|) = 2^{c_3(|N|,|H|)}.$$

Theorem 9.1 (Spiga's Bound). *If*

$$2^{1+(|N|-1)/|H|} > f_1(|N|, |H|) + f_2(|N|, |H|) + f_3(|N|, |H|)$$

then G admits a GFR.

As stated in [9, Theorem 2], Spiga's bound implies that when $|N|$ is large compared to $|H|$, then a random H-invariant subset S of N gives rise to GFR on $\mathrm{Cay}(N, S)$. Spiga also claimed on his strategy that "Theoretically this strategy is sound, in practice, even for relatively small groups H, the lower bound on $|N|$ is so large that it seems hopeless and infeasible to study the small groups N with a computer."

Proposition 9.2. *For a 2-power $q \geq 2$, let G be a Frobenius group of order $q^2(q-1)$ with nucleus of order q^2 and complement of order $q-1$. Then Spiga's bound does not hold for G.*

Proof. In our case, in the exponent on the left hand side in Spiga's bound we have $q + 2$. On the other hand, for $q = 2^m$,

$$c_2(|N|, |H|) > \frac{3}{4}\frac{q^2}{q-1} + \frac{q(q-2)}{2(q-1)} + 2m \geq \frac{q(5q-4)}{4(q-1)} + 2.$$

A straightforward computation shows that the last number is always bigger than $q + 2$ when the claim follows. $\square$

ORCID iDs

Gábor Korchmáros ⓘ https://orcid.org/0000-0002-2776-5754
Gábor P. Nagy ⓘ https://orcid.org/0000-0002-9558-4197

References

[1] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, AMS Chelsea Publishing, Providence, RI, 2006, doi:10.1090/chel/356.

[2] J. K. Doyle, T. W. Tucker and M. E. Watkins, Graphical Frobenius representations, *J. Algebraic Combin.* **48** (2018), 405–428, doi:10.1007/s10801-018-0814-6.

[3] R. Frucht, J. E. Graver and M. E. Watkins, The groups of the generalized Petersen graphs, *Proc. Cambridge Philos. Soc.* **70** (1971), 211–218, doi:10.1017/s0305004100049811.

[4] R. M. Guralnick and J. Saxl, Monodromy groups of polynomials, in: W. M. Kantor and L. Di Martino (eds.), *Groups of Lie Type and Their Geometries*, Cambridge University Press, Cambridge, volume 207 of *London Mathematical Society Lecture Note Series*, pp. 125–150, 1995, doi:10.1017/cbo9780511565823.012, proceedings of the conference held in Como, June 14 – 19, 1993.

[5] G. Higman, Suzuki 2-groups, *Illinois J. Math.* **7** (1963), 79–96, doi:10.1215/ijm/1255637483.

[6] B. Huppert and N. Blackburn, *Finite Groups III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften*, Springer-Verlag, Berlin-New York, 1982, doi:10.1007/978-3-642-67997-1.

[7] I. E. Shparlinskiĭ, Some arithmetic properties of recurrence sequences, *Mat. Zametki* **47** (1990), 124–131, doi:10.1007/bf01170895.

[8] so-called friend Don (https://mathoverflow.net/users/16510/so-called-friend-don), How often is $2^n - 1$ a number with few divisors?, MathOverflow, version: 19 October 2015, https://mathoverflow.net/q/221269.

[9] P. Spiga, On the existence of Frobenius digraphical representations, *Electron. J. Combin.* **25** (2018), #P2.6 (19 pages), doi:10.37236/7097.

[10] P. Spiga, On the existence of graphical Frobenius representations and their asymptotic enumeration, *J. Comb. Theory Ser. B* **142** (2020), 210–243, doi:10.1016/j.jctb.2019.10.003.

[11] J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht and I. E. Shparlinski, Average order in cyclic groups, *J. Théor. Nombres Bordeaux* **16** (2004), 107–123, doi:10.5802/jtnb.436.