Combinatorics, Probability and Computing (2014) 23, 449–459.
doi:10.1017/S0963548313000655

On the Diameters of Commuting Graphs Arising from Random Skew-Symmetric Matrices

PETER HEGARTY[1,2] and DMITRII ZHELEZOV[1,2]

[1]Mathematical Sciences, Chalmers, 41296 Gothenburg, Sweden
(e-mail: hegarty@chalmers.se, zhelezov@chalmers.se)
[2] Mathematical Sciences, University of Gothenburg, 41296 Gothenburg, Sweden

Received 15 September 2012; revised 2 December 2013; first published online 4 February 2014

We present a two-parameter family $(G_{m,k})_{m,k\in\mathbb{N}_{\geqslant 2}}$, of finite, non-abelian random groups and propose that, for each fixed k, as $m \to \infty$ the commuting graph of $G_{m,k}$ is almost surely connected and of diameter k. We present heuristic arguments in favour of this conjecture, following the lines of classical arguments for the Erdős–Rényi random graph. As well as being of independent interest, our groups would, if our conjecture is true, provide a large family of counterexamples to the conjecture of Iranmanesh and Jafarzadeh that the commuting graph of a finite group, if connected, must have a bounded diameter. Simulations of our model yielded explicit examples of groups whose commuting graphs have all diameters from 2 up to 10.

2010 *Mathematics subject classification*: Primary 20P05

1. Introduction

Let G be a non-abelian group. The *commuting graph* of G, denoted by $\Gamma(G)$, is usually defined as the graph whose vertices are the non-central elements of G, and such that $\{x, y\}$ is an edge if and only if $xy = yx$. For most purposes, one can just as well define the graph to have as its vertices the non-identity cosets of $Z(G)$, with $\{Zx, Zy\}$ an edge if and only if $xy = yx$. This is the definition we will adopt henceforth. Commuting graphs of groups were first mentioned in the seminal paper of Brauer and Fowler [3], which was concerned with the classification of the finite simple groups. Interest in commuting graphs in their own right is often traced back to a question posed by Erdős, and answered by Neumann [10], who showed that if the commuting graph of a group has no infinite independent set, then it cannot have arbitrarily large finite independent sets either. In this paper, we are only concerned with finite groups.

If Γ is any finite, connected graph, the *diameter* of Γ, denoted $\mathrm{diam}(\Gamma)$, is defined to be the maximum of the distances between pairs of vertices in Γ. Here, the distance between vertices x and y is the minimum number of edges in a path from x to y. If Γ

is disconnected, one sets $\mathrm{diam}(\Gamma) := \infty$. The following interesting conjecture was made in [7].

Conjecture 1.1. *There is a natural number b such that if G is a finite, non-abelian group with $\Gamma(G)$ connected, then* $\mathrm{diam}(\Gamma(G)) \leqslant b$.

This may seem like a very surprising conjecture at first sight, but in [7] the authors provided some supporting evidence by proving that, for $n \geqslant 3$, the commuting graph of the full symmetric group S_n is connected if and only if neither n nor $n-1$ is prime, and in that case $\mathrm{diam}(\Gamma(S_n)) \leqslant 5$. Previously, Segev and Seitz [12] had shown that if G is a finite simple classical group over a field of size at least 5, then either $\Gamma(G)$ is disconnected or $\mathrm{diam}(\Gamma(G)) \leqslant 10$ (it is not known if the upper bound is sharp).

Conjecture 1.1 has attracted considerable attention. A recent paper of Giudici and Pope [5] includes a comprehensive summary of existing partial results. Indeed, every paper published thus far on this topic, including theirs, seems to take the viewpoint that Conjecture 1.1 is probably true and seeks to provide evidence to support it.[1] Most of the evidence has come from groups which are structurally 'very far' from being abelian, as in, for example, the results mentioned in the previous paragraph. The intuition here is clear: *a priori*, the more 'non-abelian' a group is, the larger we would expect the diameter of its commuting graph to be. There is, of course, the risk that the graph becomes disconnected. But in many cases it turns out that the graphs are, in fact, connected, and when that is the case the diameter is bounded and small.

Giudici and Pope provided the first evidence in support of Conjecture 1.1 coming from p-groups. If x, y are two elements of a group G, then we define[2] their *commutator* $[x, y]$ to be the group element $x^{-1}y^{-1}xy$. The *commutator subgroup* of G is the subgroup generated by all the commutators and is denoted by G'. If $G' \subseteq Z(G)$ one says that G is of *nilpotence class* 2. The following result, Theorem 1.4 in [5], is particularly striking.

Theorem 1.2. *If G is of nilpotence class 2 and $|Z(G)|^3 < |G|$, then* $\mathrm{diam}(\Gamma(G)) = 2$.

The groups in this theorem, being nilpotent of class 2, are certainly 'very close to abelian' in a structural sense, so that now we have evidence in support of Conjecture 1.1 coming from 'both extremes', so to speak.

Our purpose in this paper is to explain why we think Conjecture 1.1 is false. We will describe a family of groups which we believe violates the conjecture, and present some evidence that such is the case, though not a rigorous proof. Though we came upon our idea independently of Giudici and Pope, their work also gives strong hints where one might look for counterexamples. In addition to Theorem 1.2 above, they also proved (Theorem 1.5 in [5]) that if $(G : Z(G))$ is a product of three not necessarily distinct primes, then $\Gamma(G)$ is disconnected. Putting their two results together suggests that one should look at groups of nilpotence class 2 in which the centre is neither too large nor

[1] But see Remark 1.3.

[2] Some books define the commutator of x and y to be $xyx^{-1}y^{-1}$, which in our notation would be $[x^{-1}, y^{-1}]$.

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

too small. This is exactly what we shall do. Another natural reason to look at groups of nilpotence class 2 is that is it easier to 'keep track of' the commutator relations in such groups, since the maps $g \mapsto [x, g]$ are additive, for every $x \in G$. In particular, suppose G is a p-group with $Z(G)$ and $G/Z(G)$ both elementary abelian, that is, abelian of exponent p. Then we may consider $G/Z(G)$ as a vector space over $\mathbb{F}_p$, of dimension d say, and the full set of commutator relations is determined by the choice of a basis for this space and a skew-symmetric $d \times d$ matrix taking entries in $Z(G)$, the latter also being a vector space over $\mathbb{F}_p$. The groups to be considered below have this structure.

In Section 2 we will present in detail a family of 2-groups whose commuting graphs are expected to achieve every finite diameter greater than or equal to two. The construction involves two parameters, m and k, where m represents the dimension of $G/Z(G)$, as a vector space over $\mathbb{F}_2$. The idea is to choose the skew-symmetric matrix defining the commutator relations uniformly at random from among all such $m \times m$ matrices taking values in $Z(G)$ and then show that, as $m \to \infty$ for fixed k, the resulting random group almost surely has a commuting graph of diameter k. Having dealt with some technicalities involved in the construction (Propositions 2.1–2.3), our precise claim about the resulting commuting graphs is formulated in Conjecture 2.4. The remainder of Section 2 consists of heuristic arguments in its favour. These involve analogies with the Erdős–Rényi random graph $G(n, p)$, and reveal the source of inspiration for our construction. For any $\epsilon > 0$, if $p = n^{-1+\epsilon}$ then $\mathrm{diam}(G(n, p))$ is well known to concentrate on $\lceil 1/\epsilon \rceil$. This was first proved by Klee and Larman [8], and in a much sharper form by Bollobás [2]. It can be shown by a standard path-counting argument, involving a second moment calculation and an application of a strong concentration result such as Janson's inequality. Our heuristic follows the same lines but fails at the last step since, as we shall see, it is not clear what kind of strong concentration result can be obtained in the random group setting. While disappointing from the point of view of the group-theoretic application, this difficulty may make our conjecture more interesting in its own right, as a problem in probabilistic combinatorics. Resolving it would also open the way to pushing the analogy with $G(n, p)$ into other ranges of the various parameters involved, since there is an extensive literature on the diameter of $G(n, p)$, for different ranges of the parameter p: see, for example, [11]. We will return to this in Section 3, which very briefly summarizes possibilities for future work.

Remark 1.3. Since this paper was submitted for publication, there have been a number of significant developments. In [4], Giudici and Parker provide explicit examples of finite groups whose commuting graphs are connected and of unbounded diameter, thus disproving Conjecture 1.1. Their construction is based on and inspired by the random groups presented here. They have checked by computer that their model produces examples of commuting graphs of every diameter between 3 and 15, though it appears to remain open whether every positive integer diameter is achievable. As a remarkable counterpoint to their result, Morgan and Parker [9] have proved that if G has trivial centre then every connected component of $\Gamma(G)$ has diameter at most 10. Note that this condition specifically excludes nilpotent groups. In contrast to these purely group-theoretic advances,

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

we are not aware of any further progress having been made on the analysis of the random groups described below.

2. The random group model

For positive integers m, r, let $V = V_m$ and $H = H_r$ be vector spaces over $\mathbb{F}_2$ of dimensions m and r respectively, and let $\phi : V \to H$ be a bilinear map. Set $G := V \times H$ and define a multiplication on G by

$$(v_1, h_1) \cdot (v_2, h_2) := (v_1 + v_2, h_1 + h_2 + \phi(v_1, v_2)). \tag{2.1}$$

We have the following basic facts.

Proposition 2.1.

(i) $(G, \cdot)$ *is a group of order* 2^{m+r}, *with identity element* $(0, 0)$.
(ii) *Let* $\mathcal{H} := \{(0, h) : h \in H\}$. *Then* $\mathcal{H}$ *is a subgroup of* G *and* $G/\mathcal{H} \cong V$, *as an abelian group.*
(iii) $G' \subseteq \mathcal{H} \subseteq Z(G)$.
(iv) G *is abelian if and only if* ϕ *is symmetric.*

Proof. Part (i) is easily checked and part (ii) is obvious. One also easily verifies the commutator formula

$$[(v_1, h_1), (v_2, h_2)] = (0, \phi(v_1, v_2) - \phi(v_2, v_1)), \tag{2.2}$$

from which parts (iii) and (iv) follow. □

Given a bilinear map $\phi : V \times V \to H$ and a basis $\{v^1, \ldots, v^m\}$ for V, we can form the $m \times m$ matrix $A = (\phi(v^i, v^j))$. Then (2.2) says that the commutator relations in G are determined by the entries in the skew-symmetric matrix $A - A^T$.

Now let $k \geqslant 2$ be an integer, and let

$$\delta \in \left(0, \frac{1}{2k(k-1)}\right)$$

be a real number. There is a choice of real number $\delta_1 > 0$ such that the following holds. For each positive integer m, if we set

$$r := \lfloor (1 - \delta_1)m \rfloor, \quad p := 2^{-r}, \quad n := 2^m - 1, \tag{2.3}$$

then, for all m sufficiently large,

$$1 + \log_n p \in \left(\frac{1}{k} + \delta, \frac{1}{k-1} - \delta\right). \tag{2.4}$$

The parameters k, δ, δ_1 should be considered fixed for the remainder of this section. For each $m \in \mathbb{N}$, with r as in (2.3), let the bilinear map $\phi : V_m \to H_r$ be chosen uniformly at random from among all $2^{m^2 r}$ such maps. We denote by $G_{m,k}$ the corresponding random group of order 2^{m+r} in which multiplication is given by (2.1).

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

To simplify the presentation to follow, subscripts involving k, m, r will often be suppressed. We shall also abuse notation in the following ways. For each $v \in V$, the element $(v, 0)$ of $G = V \times H$ will be denoted simply by v. Then, for a subset $W \subseteq V$, we denote by W' the subset of G' consisting of all commutators $[w_1, w_2]$, for $w_1, w_2 \in W$. In particular, $G' = V'$ in this notation. Similarly, we shall not distinguish between the vector space H and the subgroup $\mathcal{H}$ of G in Proposition 2.1(ii). We shall denote the group operation in G multiplicatively, while thinking of V and H as additive vector spaces. Hence, the identity element $(0, 0)$ of G will be denoted by $1 = 1_G$. Hopefully, no confusion will arise from these choices.

A uniformly random bilinear map from V to H can be realized by fixing a basis $\{v^1, \ldots, v^m\}$ for V and then choosing the m^2 elements $\phi(v^i, v^j)$, $1 \leqslant i, j \leqslant m$, uniformly and independently at random. The choice of basis is clearly immaterial: if ϕ is a uniformly random bilinear map, then so is $\psi^{-1} \circ \phi \circ \psi$, for any linear automorphism ψ of V. These considerations lead to our first proposition concerning the random group $G = G_{m,k}$.

Proposition 2.2.

(i) *For any two distinct elements $v_1, v_2 \in V$, the commutator $[v_1, v_2]$ is a uniformly random element of H. In particular, $\mathbb{P}([v_1, v_2] = 1) = 2^{-r}$.*

(ii) *Let W be a subspace of V, $v \in V \backslash W$ and w_1, w_2 distinct elements of W. Then the commutator $[v, w_1]$, as an H-valued random variable, is independent of the set $W' \cup \{[v, w_2]\}$ of commutators. In particular, $[v, w_1]$ is independent of W'.*

Proof. Choose a basis $\{v^1, \ldots, v^m\}$ for V. For part (i), by the considerations in the previous paragraph we can assume, without loss of generality, that $v_1 = v^1$ and $v_2 = v^2$. Then, by (2.2), the random variable $[v^1, v^2]$ is the difference between two independent, H-uniform random variables, hence also H-uniform. This proves (i). For part (ii), suppose $\dim(W) = l$, for some $2 \leqslant l < m$. By the same reasoning as before, we can assume without loss of generality that W is spanned by $v^1, \ldots, v^l$, $w_1 = v^1$, $w_2 = v^2$ and $v = v^{l+1}$. Since the elements $\phi(v^i, v^j)$, $1 \leqslant i, j \leqslant m$, are chosen independently, it is then clear that the commutator $[v^{l+1}, v^2]$ is independent of all those in $W' \cup \{[v^{l+1}, v^1]\}$. □

Proposition 2.3. *As $m \to \infty$, $\mathbb{P}(G' = Z(G) = H) \to 1$.*

Proof. From Proposition 2.1(iii), we already know that $G' \subseteq H \subseteq Z(G)$, so it remains to prove that the reverse inclusions hold almost surely, as $m \to \infty$. We fix a choice of a basis $\{v^1, \ldots, v^m\}$ for V.

First consider G'. There are $2^r - 1$ codimension-one subspaces of H. List them in any order and, for each $\xi = 1, \ldots, 2^r - 1$, let B_ξ be the event that all the commutators $[v^i, v^j]$ lie in the ξth subspace. From Proposition 2.2 and its proof we see that each of the events B_ξ has the same probability, namely $2^{-\binom{m}{2}}$. We have $G' = H$ if and only if none of the events B_ξ occur. By a union bound, the probability of this is at least $1 - (2^r - 1)2^{-\binom{m}{2}}$. Since $m \geqslant r$, this expression obviously goes to one as $m \to \infty$.

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

Next consider $Z(G)$. For each non-zero element v of V, let B_v denote the event that $v \in Z(G)$. We need to show that, as $m \to \infty$, almost surely none of these events occur. By Proposition 2.2 and its proof, each of the events B_v has the same probability. Since there are $2^m - 1$ of them it suffices, by a union bound, to show that $\mathbb{P}(B_{v^1}) = o(2^{-m})$. But B_{v^1} occurs if and only if $[v^1, v^j] = 1$ for each $j = 2, \ldots, m$. These $m - 1$ events are independent, and each occurs with probability 2^{-r}. Hence $\mathbb{P}(B_{v^1}) = 2^{-(m-1)r}$, which is $o(2^{-m})$, since $r = \Theta(m)$. □

Proposition 2.3 implies that, as $m \to \infty$, the group $G = G_{m,k}$, of order 2^{m+r}, almost surely has the following two properties.

(I) It is nilpotent of class 2.

(II) $G' = Z(G)$ is of order 2^r and $G/Z(G)$ is of order 2^m. Both groups are elementary abelian.

Hence the commuting graph $\Gamma(G_{m,k})$ almost surely consists of $n = 2^m - 1$ vertices, one for each non-zero element v of V. By Proposition 2.2, each edge of this graph is present with probability $p = 2^{-r}$. By (2.4), our choice of parameters ensures that $p = p(n) = n^{-1+\epsilon_n}$, where

$$\epsilon_n \in \left(\frac{1}{k} + \delta, \frac{1}{k-1} - \delta \right).$$

Hence, by analogy with Erdős–Rényi graphs, we expect that the following holds.

Conjecture 2.4. *As $m \to \infty$, $\Gamma(G_{m,k})$ is almost surely connected and of diameter k.*

We have been unable to prove this assertion, but we would be amazed if at least the first part of it, namely the claim that $\Gamma(G_{m,k})$ is almost surely connected, were false. Note that even that much would suffice to disprove Conjecture 1.1 since, as we will see below, it is easy to prove that the diameter of $\Gamma(G_{m,k})$ is almost surely at least k. The obvious line of attack for Conjecture 2.4 is to try to imitate, and modify where necessary, a proof of the corresponding assertion for the Erdős–Rényi random graph $G(n, p)$, with n and p as in (2.3). Obviously, some modification is necessary since, unlike in $G(n, p)$, the edges of $\Gamma(G_{m,k})$ are not chosen independently of one another. Indeed, given a basis $\{v^1, \ldots, v^m\}$ for V, the graph is completely specified by the values of the $\binom{m}{2}$ commutators $[v^i, v^j]$, $1 \leqslant i < j \leqslant m$. Our heuristic argument for Conjecture 1.1 will involve showing that the first and second moments of the number of paths[3] between a pair of vertices of $\Gamma(G_{m,k})$ can be computed as in the Erdős–Rényi setting, modulo some technical modifications. To prove this rigorously requires some work, which we now perform.

Henceforth, all statements about $G_{m,k}$ are conditioned on properties (I) and (II) on the previous page holding. In particular, the vertices of the commuting graph are assumed to be in one-to-one correspondence with the non-zero elements of $V = V_m$. Fix a positive

[3] Hereafter we assume all paths are simple.

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

integer l. Let a, b be two distinct vertices of $\Gamma(G_{m,k})$, and let

$$P : \gamma_0 = a \to \gamma_1 \to \gamma_2 \to \cdots \to \gamma_{l-1} \to b = \gamma_l \tag{2.5}$$

be a path of length l between a and b in the complete graph K_n on $n = 2^m - 1$ vertices. Let B_P denote the event that P is present in $\Gamma(G_{m,k})$. Further, let V_P denote the subspace of V spanned by $a, \gamma_1, \ldots, \gamma_{l-1}, b$. Since $a \neq b$, we have *a priori* that

$$2 \leqslant \dim(V_P) \leqslant l + 1. \tag{2.6}$$

For each $t \in \{2, \ldots, l+1\}$, let $E_{l,t}$ denote the number of paths P of length l between a and b in K_n for which $\dim(V_P) = t$. Note that this number does not depend on the choice of a and b. If P_1 and P_2 are two paths between a and b, set $V_{P_1,P_2} := \mathrm{Span}\{V_{P_1}, V_{P_2}\}$. *A priori* we have

$$2 \leqslant \dim(V_{P_1,P_2}) \leqslant |P_1 \cup P_2| \leqslant 2l. \tag{2.7}$$

Finally, for each $t \in \{2, \ldots, 2l\}$, let $F_{l,t}$ denote the number of ordered pairs (P_1, P_2) of paths of length l between a and b in K_n for which $\dim(V_{P_1,P_2}) = t$. All the crucial facts we need are contained in the next proposition.

Proposition 2.5. *With notation as above and letting $m \to \infty$ with l fixed, we have the following.*

(i) $\mathbb{P}(B_P) \leqslant p^{\dim(V_P)-1}$, *and we have equality when* $\dim(V_P) = l + 1$.
(ii) *For any two paths,*

$$\mathbb{P}(B_{P_1} \wedge B_{P_2}) \leqslant p^{\dim(V_{P_1,P_2})-1}.$$

Moreover, if $\dim(V_{P_1,P_2}) > l + 1$ *then*

$$\mathbb{P}(B_{P_1} \wedge B_{P_2}) \leqslant p^{\dim(V_{P_1,P_2})}.$$

(iii) *If* $\dim(V_{P_1,P_2}) = 2l$ *then* $\mathbb{P}(B_{P_1} \wedge B_{P_2}) = p^{2l}$ *and the events B_{P_1} and B_{P_2} are independent.*
(iv) $E_{l,t} = \Theta(n^{t-2})$, *for all* $2 \leqslant t \leqslant l + 1$, *and* $F_{l,t} = \Theta(n^{t-2})$ *for all* $2 \leqslant t \leqslant 2l$.

Proof. **(i)** Consider a path as in (2.5). The point is that, as we run through the vertices γ_i, each time the addition of a γ_i increases the dimension of the space V_P by one, the edge corresponding to the commutator $[\gamma_i, \gamma_{i-1}]$ is independent of all the previous edges along the path. This is an immediate consequence of Proposition 2.2(ii). When the dimension of V_P is maximal then all the edges along the path are independent, which gives equality in that case.

(ii), (iii) Given an ordered pair (P_1, P_2) of paths from a to b, we can concatenate P_1 with the reverse of P_2 to form a walk[4] starting and ending at a. If $\mathcal{C}$ is any closed walk in K_n, with a prescribed start/endpoint, we let $V_{\mathcal{C}}$ denote the subspace of V spanned by all the vertices on $\mathcal{C}$, and let $B_{\mathcal{C}}$ denote the event that $\mathcal{C}$ is present in $\Gamma(G_{m,k})$. We let $|\mathcal{C}|$ denote

[4] In contrast to paths, walks are not assumed to be simple in this paper.

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

the length of $\mathcal{C}$, *i.e.*, the total number of edges, including possible repititions. We shall prove the following, which includes part (ii) of Proposition 2.5 as a special case.

Claim. Let $\mathcal{C}$ be a closed walk starting and ending at a which is the concatenation of two paths. Then $\mathbb{P}(B_{\mathcal{C}}) \leqslant p^{\dim(V_{\mathcal{C}})-1}$. Moreover, if $\dim(V_{\mathcal{C}}) > |\mathcal{C}|/2+1$, then $\mathbb{P}(B_{\mathcal{C}}) \leqslant p^{\dim(V_{\mathcal{C}})}$.

The first part of the Claim is proved in exactly the same way as part (i) of Proposition 2.5. The meat is in the second statement. To prove it, we proceed by induction on $|\mathcal{C}|$. The statement is vacuous when $|\mathcal{C}| = 2$, since then $\dim(V_{\mathcal{C}})$ cannot *a priori* exceed $|\mathcal{C}| = 2 = |\mathcal{C}|/2+1$. When $|\mathcal{C}| = 3$ then the statement is non-vacuous if and only if $\dim(V_{\mathcal{C}}) = 3$. This happens if and only if $\mathcal{C}$ has the form $a \to c \to d \to a$, where a, c, d are linearly independent in V. But in that case the commutators $[a,c]$, $[c,d]$ and $[d,a]$ are also independent in $G_{m,k}$: this is the simplest case of Proposition 2.2(ii). Thus $\mathbb{P}(B_{\mathcal{C}}) = p^3 = p^{\dim(V_{\mathcal{C}})}$. The same reasoning applies when $|\mathcal{C}| = 4$, since then the statement is still vacuous unless $V_{\mathcal{C}}$ has maximal dimension. Whenever $\dim(V_{\mathcal{C}}) = |\mathcal{C}|$ it means that all $|\mathcal{C}|$ vertices along the walk are linearly independent elements of V. If v is the last vertex before returning to a, then linear independence of vertices already implies that all $|\mathcal{C}|-1$ edges up to v are independent in the random graph. Plus, we can apply Proposition 2.2(ii) to deduce that the edge $\{v,a\}$ is independent of all the previous edges. So all the edges on $|\mathcal{C}|$ are independent in this case and hence $\mathbb{P}(B_{\mathcal{C}}) = p^{|\mathcal{C}|}$. Note that this argument already proves part (iii) of Proposition 2.5.

We still have to complete the induction step for part (ii). So now suppose $|\mathcal{C}| > 4$, and that $\mathcal{C}$ is a concatenation of paths Q_1, Q_2 of lengths l and m respectively, where $l+m = |\mathcal{C}| > 4$. We assume that $\dim(V_{\mathcal{C}}) > (l+m)/2+1$ and must show that $\mathbb{P}(B_{\mathcal{C}}) \leqslant p^{\dim(V_{\mathcal{C}})}$. Write

$$\begin{aligned} Q_1 &: \gamma_0 = a \to \gamma_1 \to \gamma_2 \to \cdots \to \gamma_{l-1} \to c := \gamma_l, \\ Q_2 &: \gamma_l = c \to \gamma_{l+1} \to \gamma_{l+2} \to \cdots \to \gamma_{l+m-1} \to a := \gamma_{l+m}. \end{aligned} \tag{2.8}$$

As in the proof of part (i), we can walk along $\mathcal{C}$ and there must be a final vertex γ_j, $1 \leqslant j \leqslant l+m-1$, at which the dimension of $V_{\mathcal{C}}$ increases. Let $\mathcal{C}_1$ be that part of $\mathcal{C}$ from γ_0 as far as γ_j, and let $B_{\mathcal{C}_1}$ be the event that $\mathcal{C}_1$ is present in $\Gamma(G_{m,k})$. Let W be the subspace of V spanned by $\gamma_0, \ldots, \gamma_{j-1}$. Then $\dim(W) = \dim(V_{\mathcal{C}}) - 1$ and, as in the proof of part (i), we already know that $\mathbb{P}(B_{\mathcal{C}_1}) \leqslant p^{\dim(V_{\mathcal{C}})-1} = p^{\dim(W)}$. It thus suffices to have at least one edge in $\mathcal{C} \backslash \mathcal{C}_1$ which is independent of all the edges in $\mathcal{C}_1$. We consider three cases.

Case 1: $\gamma_{j-1} = \gamma_{j+1}$.

Since each of Q_1 and Q_2 is a path, this can only happen if $j = l$. We let R_1 be the part of Q_1 from γ_0 to γ_{l-1} and let R_2 be the part of Q_2 from γ_{l+1} to γ_{l+m}. Then their concatenation $\mathcal{D}$ is a closed walk, and it is the concatenation of paths of lengths $l-1$ and $m-1$. In particular, $|\mathcal{D}| \geqslant 2$. Since $V_{\mathcal{C}} = \mathrm{Span}\{V_{\mathcal{D}}, \gamma_j\}$, we have

$$\dim(V_{\mathcal{D}}) \geqslant \dim(V_{\mathcal{C}}) - 1 > \frac{(l-1)+(m-1)}{2} + 1.$$

So we can apply the induction hypothesis and conclude that $\mathbb{P}(B_{\mathcal{D}}) \leqslant p^{\dim(V_{\mathcal{D}})}$. If $V_{\mathcal{D}} = V_{\mathcal{C}}$ we are already done. Otherwise, $V_{\mathcal{D}} = W$ and the edge $\{\gamma_{j-1}, \gamma_j\}$ is independent of all the

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

edges on $\mathcal{D}$, so

$$\mathbb{P}(B_{\mathcal{C}}) = \mathbb{P}(B_{\mathcal{D}} \wedge \text{“}[\gamma_{j-1}, \gamma_j] = 1'') = \mathbb{P}(B_{\mathcal{D}}) \cdot \mathbb{P}([\gamma_{j-1}, \gamma_j] = 1) \leqslant p^{\dim(V_{\mathcal{D}})+1} = p^{\dim(V_{\mathcal{C}})}, \quad (2.9)$$

as required.

Case 2: $\gamma_{j+1} \in W$ but $\gamma_{j+1} \neq \gamma_{j-1}$.

In this case, Proposition 2.2(ii) immediately implies that the edge $\{\gamma_j, \gamma_{j+1}\}$ is independent of all the edges in $\mathcal{C}_1$, so we are done.

Case 3: $\gamma_{j+1} \notin W$.

By assumption, $V_{\mathcal{C}} = \text{Span}\{W, \gamma_j\}$. Hence $\gamma_{j+1} = w + \gamma_j$ for some non-zero $w \in W$. We cannot have $w = 0$ since $\gamma_{j+1} \neq \gamma_j$. Observe that $[\gamma_{j+1}, \gamma_j] = [w + \gamma_j, \gamma_j] = [w, \gamma_j]$. If $w \neq \gamma_{j-1}$ then we could argue just as in Case 2. Thus we may assume that $\gamma_{j+1} = \gamma_{j-1} + \gamma_j$. Note in particular that $j \leqslant l + m - 2$ since $\gamma_{l+m} = a \in W$. So we can consider the vertex γ_{j+2}.

A priori, $\gamma_{j+2} = w + \epsilon\gamma_j$ for some $w \in W$ and $\epsilon \in \{0, 1\}$. Then, considered as elements of the additive vector space H,

$$[\gamma_{j+2}, \gamma_{j+1}] = [w + \epsilon\gamma_j, \gamma_{j-1} + \gamma_j] = [w, \gamma_{j-1}] + [w^*, \gamma_j], \quad (2.10)$$

where $w^* = w + \epsilon\gamma_{j-1}$ also lies in W. Thus $[\gamma_{j+2}, \gamma_{j+1}] \in W' \oplus [w^*, \gamma_j]$, so if $w^* \neq \gamma_{j-1}$ we can once again argue just as in Case 2, and conclude that the edge $\{\gamma_{j+1}, \gamma_{j+2}\}$ is independent of those in $\mathcal{C}_1$. So we may assume that $w^* = \gamma_{j-1}$, which one readily checks to imply that $\gamma_{j+2} = \gamma_{j-1}$.

Now we are almost in the same situation as in Case 1. This time we must have $j = l$ or $j = l + 1$. In Case 1 we removed a hanging 2-cycle $\gamma_{j-1} \to \gamma_j \to \gamma_{j-1}$ and applied induction to the remaining closed walk $\mathcal{D}$, which was a concatenation of paths of lengths $l - 1$ and $m - 1$. This time we remove the hanging 3-cycle $\gamma_{j-1} \to \gamma_j \to \gamma_{j+1} \to \gamma_{j-1}$ and will be left with a closed walk $\mathcal{D}^*$ which is a concatenation of paths of lengths $l - 1$ and $m - 2$, or $l - 2$ and $m - 1$. Now $\mathcal{C}_1 \subseteq \mathcal{D}^*$ and hence $\dim(V_{\mathcal{D}^*}) \geqslant \dim(V_{\mathcal{C}_1}) \geqslant \dim(V_{\mathcal{C}}) - 1$. Also, $|\mathcal{D}^*| \geqslant 2$ since $|\mathcal{C}| > 4$. Thus induction can validly be applied and the argument goes through exactly as in Case 1. Thus the proof of the Claim, and in particular of part (ii) of Proposition 2.5, is complete.

(iv) We prove the estimate for $E_{l,t}$ only, since the argument for $F_{l,t}$ follows exactly the same lines. Consider paths as in (2.5) again. We must estimate the number of ways we can choose the ordered sequence $(\gamma_1, \ldots, \gamma_{l-1})$ of vertices, so that $\dim(V_P) = t$. We can just as well start with a and b, which span a two-dimensional space, and choose the remaining γ_i in order, so that the dimension increases by $t - 2$ in all. Each time we choose a new γ_i we must decide whether or not to increase the dimension by one. Each time we do the former, there are $(1 - o(1))n$ choices for γ_i. Each time we do the latter, there are certainly no more than $2^l = O(1)$ choices for γ_i. We will get another $O(1)$ factor from the freedom to choose on which $t - 2$ occasions the dimension is to be increased. But clearly the result is that we have $\Theta(1) \cdot n^{t-2}$ choices for the path, as claimed. □

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

Let $X = X_{m,k,l}$ be the random variable denoting the number of paths of a length l from a to b in $G_{m,k}$. Set

$$\mu := \mathbb{E}[X] = \sum \mathbb{P}(B_p), \tag{2.11}$$

the sum being taken over all paths P of length l from a to b. From parts (i) and (iv) of Proposition 2.5 it follows that $\mu = \Theta(n^{l-1}p^l)$. Hence, by (2.4), $\mu = o(1)$ when $l < k$. This already suffices to prove that the diameter of $G_{m,k}$ is almost surely at least k. Let

$$\Delta := \sum \mathbb{P}(B_{P_i} \wedge B_{P_j}), \tag{2.12}$$

where the sum is taken over all ordered pairs (P_i, P_j) of paths of length l from a to b, but such that the events B_{P_i} and B_{P_j} are dependent. The second moment method (see Chapter 4 of [1]) implies that

$$\mathbb{P}(\text{no path of length } l \text{ from } a \text{ to } b) \leqslant \frac{\Delta + \mu}{\mu^2}. \tag{2.13}$$

But from parts (ii)–(iv) of Proposition 2.5 it follows that

$$\Delta = O\left(\sum_{t=2}^{l+1} n^{t-2}p^{t-1} + \sum_{t=l+2}^{2l-1} n^{t-2}p^t\right) = O(n^{l-1}p^l + n^{2l-3}p^{2l-1}). \tag{2.14}$$

Hence, by (2.4), for any $l \geqslant k$ we have

$$\mathbb{P}(\text{no path of length } l \text{ from } a \text{ to } b) = O(n^{-\delta_2}), \tag{2.15}$$

where δ_2 is some positive number, depending on the choice of the parameters δ and δ_1 at the outset of Section 2. From (2.15) and a simple averaging argument, we can deduce the following result.

Proposition 2.6. *There is some $\delta_3 > 0$, depending on the choices of δ and δ_1, such that, as $m \to \infty$, $\Gamma(G_{m,k})$ almost surely has a connected component of size at least $n - n^{1-\delta_3}$.*

But to prove almost sure connectedness of the full graph we need much stronger concentration of the number of a–b paths than that provided by (2.13). For Erdős–Rényi graphs one can apply Janson's inequality, for example, but we cannot do that here. Janson's inequality assumes that there is an underlying set of independent coin tosses such that each event B_P represents the success of a certain subset of these tosses. That requirement is satisfied by $G(n,p)$ but not $\Gamma(G_{m,k})$, since the edges in the latter graph are not placed independently. At this time we do not see how to get around this problem, so Conjecture 2.4 remains open. However, we hope the reader will agree with us that the theoretical evidence in its favour seems strong. We also have some numerical evidence. Simulations of our model yielded examples of groups whose commuting graphs achieve all possible diameters up to 10. More details of these can be found in an earlier version of the paper available on `arXiv` [6]. As m is increased, it rapidly becomes impractical to run simulations, however.

https://doi.org/10.1017/S0963548313000655 Published online by Cambridge University Press

3. Future work

Clearly, some new idea is needed to either prove or disprove Conjecture 2.4. If it is true, then perhaps the analogy with $G(n,p)$ can be pushed even further ? For example, there may be a sharp connectivity threshold for our random commuting graph model and it may or may not be at $p(n) = (\log n)/n$, which is the threshold for $G(n,p)$.

Acknowledgement

We thank the referee for a careful reading of the paper and in particular for observing a gap in the proof of Proposition 2.5. His/her comments helped to improve the presentation.

References

[1] Alon, N. and Spencer, J. (2000) *The Probabilistic Method*, second edition, Wiley.
[2] Bollobás, B. (1981) The diameter of random graphs. *Trans. Amer. Math. Soc.* **267** 41–52.
[3] Brauer, R. and Fowler, K. A. (1955) On groups of even order. *Ann. of Math.* (2) **62** 565–583.
[4] Giudici, M. and Parker, C. W. (2013) There is no upper bound for the diameter of the commuting graph of a finite group. *J. Combin. Theory Ser. A* **120** 1600–1603.
[5] Guidici, M. and Pope, A. (2013) On bounding the diameter of the commuting graph of a group. *J. Group Theory* (1) **17** 131–149.
[6] Hegarty, P. and Zhelezov, D. Can commuting graphs of finite groups have arbitrarily large diameter? Preprint available at `arXiv.org/abs/1204.5456`.
[7] Iranmanesh, A. and Jafarzadeh, A. (2008) On the commuting graph associated with the symmetric and alternating groups. *J. Algebra Appl.* **7** 129–146.
[8] Klee, V. and Larman, D. (1981) Diameters of random graphs. *Canad. J. Math.* **33** 618–640.
[9] Morgan, G. L. and Parker, C. W. (2013) The diameter of the commuting graph of a finite group with trivial centre. *J. Algebra* **393** 41–59.
[10] Neumann, B. H. (1976) A problem of Paul Erdős on groups. *J. Austral. Math. Soc. Ser. A* **21** 467–472.
[11] Riordan, O. and Wormald, N. (2010) The diameter of sparse random graphs. *Combin. Probab. Comput.* **19** 835–926.
[12] Segev, Y. and Seitz, G. M. (2002) Anisotropic groups of type A_n and the commuting graph of finite simple groups. *Pacific J. Math.* **202** 125–225.