HAMILTONIAN CYCLES IN THE GENERATING GRAPHS OF FINITE GROUPS

T. BREUER, R. M. GURALNICK, A. LUCCHINI, A. MARÓTI, G. P. NAGY

Abstract. For a finite group G let $\Gamma(G)$ denote the graph defined on the non-identity elements of G in such a way that two distinct vertices are connected by an edge if and only if they generate G. In this paper it is shown that the graph $\Gamma(G)$ contains a Hamiltonian cycle for many finite groups G.

1. Introduction

For a finite group G let $\Gamma(G)$ denote the graph defined on the non-identity elements of G in such a way that two distinct vertices are connected by an edge if and only if they generate G. The graph $\Gamma(G)$ is called the generating graph of G. The generating graph was investigated in [15], [16], and [17]. For example, in [16], it is shown that for a nilpotent by nilpotent finite group G the clique number of $\Gamma(G)$ is equal to the chromatic number of $\Gamma(G)$.

In the literature many deep results about finite simple groups G can equivalently be stated as theorems about $\Gamma(G)$. Three examples are given. Guralnick and Shalev [10] showed that for sufficiently large G the graph $\Gamma(G)$ has diameter at most 2. Guralnick and Kantor [9] showed that there is no isolated vertex in $\Gamma(G)$. Finally, Breuer, Guralnick, Kantor [4] showed that the diameter of $\Gamma(G)$ is at most 2 for all G.

In this paper those finite groups G are considered for which $\Gamma(G)$ contains a Hamiltonian cycle. The following proposition reduces the investigations to those non-solvable groups G for which G/N is cyclic for any non-trivial normal subgroup N of G.

Proposition 1.1. *Let G be a finite solvable group that has at least 4 elements. Then the graph $\Gamma(G)$ contains a Hamiltonian cycle if and only if G/N is cyclic for all non-trivial normal subgroups N of G.*

The three main results of this paper are Theorems 1.2, 1.3, and 1.4.

Theorem 1.2. *For every sufficiently large finite simple group G, the graph $\Gamma(G)$ contains a Hamiltonian cycle.*

Theorem 1.3. *For every sufficiently large symmetric group S_n, the graph $\Gamma(S_n)$ contains a Hamiltonian cycle.*

Theorem 1.4. *For every sufficiently large non-abelian finite simple group S, the graph $\Gamma(S \wr C_m)$ contains a Hamiltonian cycle, where m denotes a prime power.*

---

[1]The second author was partially supported by NSF grant DMS 0653873.

[2]The research of the fourth author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme and partially by grants OTKA T049841 and OTKA NK72523.

[3]Mathematics Subject Classification 2010: 20P05, 05C45

Date: 2nd of December, 2009.

The proofs of Theorems 1.2, 1.3, and 1.4 depend heavily on Liebeck, Shalev [13], Fulman, Guralnick [6], Babai, Hayes [1], and Luczak, Pyber [18].

Theorem 1.5. *Let G be a sporadic simple group or the automorphism group of a sporadic simple group. Then the graph $\Gamma(G)$ contains a Hamiltonian cycle.*

Based on Proposition 1.1, Theorems 1.2, 1.3, 1.4, 1.5, and some computer calculations performed by GAP [8] (see Section 8), the following conjecture is proposed.

Conjecture 1.6. *Let G be a finite group with at least 4 elements. Then the graph $\Gamma(G)$ contains a Hamiltonian cycle if and only if G/N is cyclic for all non-trivial normal subgroups N of G.*

Conjecture 1.6 is related to Conjecture 1.8 (and the following paragraph) of [4]. Indeed, Burness, Guest, and Guralnick [5] are working on the problem of proving that $\Gamma(G)$ has no isolated vertex and indeed has diameter at most 2 if and only if G/N is cyclic for every non-trivial normal subgroup N of G. Moreover, the problem has been reduced to the case where G is almost simple.

Problem 8.5 of The Kourovka Notebook [12] posed by M. R. Vaughan-Lee in 1982 is the following. Prove that if G is a finite group, F is any field, and V is a non-trivial irreducible FG-module then

$$\frac{1}{|G|}\sum_{g\in G}\dim(\mathrm{fix}(g)) \leq \frac{1}{2}\dim(V).$$

This was proved in case $(|G|,|V|)=1$ and also for solvable groups G by Neumann and Vaughan-Lee in [19]. Later, Segal and Shalev [20] showed that, in general, the average dimension of fixed point spaces of elements of G on V is at most $(3/4)\dim(V)$. Finally, Isaacs, Keller, Meierfrankenfeld, Moretó [11] proved, in a slightly more general setting, that the average dimension of fixed point spaces of elements of G on V is at most $((p+1)/(2p))\dim(V)$ where p denotes the smallest prime divisor of $|G|$. In this paper we show the following.

Proposition 1.7. *Let V be an irreducible FG-module of dimension at least 2 for some field F and some finite group G. For an arbitrary element g in G let $d(g)$ denote the dimension of the largest eigenspace of g on V. Suppose that the graph $\Gamma(G)$ contains a Hamiltonian cycle. Then*

$$\frac{1}{(|G|-1)}\sum_{1\neq g\in G} d(g) \leq \frac{1}{2}\dim(V).$$

2. Graphs

A Hamiltonian cycle is a cycle in an undirected simple graph which visits each vertex exactly once. A graph is called Hamiltonian if it contains a Hamiltonian cycle. The problem of determining whether a graph is Hamiltonian is NP-complete and is a special case of the travelling salesman problem.

There are many ways to show that a given graph is Hamiltonian. First of all, sometimes it is possible just to exhibit a Hamiltonian cycle in the graph. This is the case for the graph $\Gamma(G)$ when G is a solvable group of order at least 4 with the property that G/N is cyclic for every non-trivial normal subgroup N of G (see Section 3).

A simple graph with m vertices and list of vertex degrees $d_1 \leq \ldots \leq d_m$ satisfies Pósa's criterion if $d_k \geq k+1$ for all positive integers k with $k < m/2$. By Exercise 10.21 (b) of [14], a graph contains a Hamiltonian cycle if it satisfies Pósa's criterion.

It is shown in Sections 4 and 5 that $\Gamma(G)$ satisfy Pósa's criterion for almost all (if not all) finite simple groups G of orders at least 5.

For a simple graph Γ with m vertices let $d(\Gamma, v)$ denote the degree of the vertex v. The closure $\mathrm{cl}(\Gamma)$ of Γ is the graph (on the same set of vertices) constructed from Γ by adding for all non-adjacent pairs of vertices u and v with $d(\Gamma, u) + d(\Gamma, v) \geq m$ the new edge uv. One of the best characterization of Hamiltonian graphs is

Theorem 2.1 (Bondy, Chvátal, [2]). *A graph is Hamiltonian if and only if its closure is Hamiltonian.*

Theorem 2.1 is first applied in Section 6 of this paper.

For a simple graph Γ, let us set $\mathrm{cl}^{(1)}(\Gamma) = \mathrm{cl}(\Gamma)$ and inductively set $\mathrm{cl}^{(i)}(\Gamma) = \mathrm{cl}(\mathrm{cl}^{(i-1)}(\Gamma))$ for every positive integer i larger than 1.

A simple graph with m vertices and list of vertex degrees $d_1 \leq \ldots \leq d_m$ satisfies Chvátal's criterion if whenever k is so that $d_k \leq k < m/2$ it follows that $d_{m-k} \geq m - k$. By Exercise 10.21 (d) of [14], a graph contains a Hamiltonian cycle if it satisfies Chvátal's criterion. In Section 6 it is shown that for every sufficiently large symmetric group S_n the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$ satisfies Chvátal's criterion.

3. Solvable Groups

In this section Proposition 1.1 is shown. Let G be a finite solvable group with at least 4 elements.

If $\Gamma(G)$ contains a Hamiltonian cycle, then there is no isolated vertex in $\Gamma(G)$, hence G/N must be cyclic for all non-trivial normal subgroups N of G. It is sufficient to show the other implication. Suppose that G is a finite group with the property that G/N is cyclic for all non-trivial normal subgroups N of G.

If G is cyclic, then any generator g of G is connected to every other vertex of $\Gamma(G)$ and $g^1, g^2, \ldots, g^{n-1}, g^1$ determines a Hamiltonian cycle in $\Gamma(G)$ where $n = |G|$. Hence we may assume that G is non-cyclic.

If G has two distinct minimal normal subgroups, A and B, then G embeds in $G/A \times G/B$ and so is Abelian. Since G is not cyclic, the Frattini subgroup of G must be trivial. Thus, G is a direct product of cyclic groups of prime order. It follows easily that G is elementary Abelian of order p^2 for some prime p. Then each vertex in $\Gamma(G)$ has degree $p^2 - p$ and so there is a Hamiltonian cycle in $\Gamma(G)$ by Pósa's criterion.

So we may assume that G has a unique minimal normal subgroup M. It follows that M is an elementary Abelian p-group for some prime p and the cyclic group G/M acts faithfully and irreducibly on M. Since the cyclic group G/M acts faithfully and irreducibly on M, the integers $|G/M|$ and $|M|$ are coprime. By the Schur-Zassenhaus Theorem, G is a split extension of M by $H = G/M$ and all complements of M in G are conjugate. Hence H can be considered to be an irreducible subgroup of a Singer cycle on M. It follows that G is a primitive Frobenius group. Put $m = |M|$. Let $H_1, \ldots, H_m$ be the distinct conjugates of H in G. Notice that $m \geq 3$. For each i with $1 \leq i \leq m$ the cyclic group H_i is maximal in G.

Put $n = |H|$ and let h be a generator of H_m. For each k with $1 \leq k \leq m$ let v_k be the unique element of M with ${v_k}^{-1} H_m v_k = H_k$. Let j be an arbitrary positive integer with $1 \leq j \leq m \cdot n$. If j is a multiple of n, then set $g_j = v_k$ where k is such that $k \equiv j \pmod{m}$. Otherwise, if j is not a multiple of n, then set $g_j = {v_k}^{-1} h^i v_k$ where i and k are so that $i \equiv j \pmod{n}$ and $k \equiv j \pmod{m}$. Then $g_{m \cdot n}$ is the identity element of G and $g_1, \ldots, g_{m \cdot n-1}$ are precisely the non-identity elements of G. We claim that the vertices $g_1, \ldots, g_{m \cdot n-1}, g_1$ determine a Hamiltonian cycle in $\Gamma(G)$. To show this claim, let x and y be two consecutive elements in the previous list and set $L = \langle x, y \rangle$. By construction, L projects onto G/M via the natural homomorphism from G to G/M but L is not conjugate to H_1. From this it follows that L cannot be contained in a maximal subgroup containing M (of the form $M \rtimes K$ for K a maximal subgroup of H) and L cannot lie in any complement of M in G. Since G is an affine primitive permutation group with $(|M|, |H|) = 1$, it follows, from the Schur-Zassenhaus Theorem, that L is contained in no maximal subgroup of G, hence $L = G$.

4. Groups of Lie Type

In this section it is shown that the graph $\Gamma(G)$ satisfies Pósa's criterion (and hence contains a Hamiltonian cycle) for every sufficiently large finite simple group G of Lie type.

By a random element of a non-empty finite set S we mean an element chosen uniformly from S. For a finite group G let $P(G)$ be the probability that a random pair of elements of G generate G. For a finite group G and an element $x \in G$, define $P_x(G)$ to be the probability that x and a randomly chosen element y generate G. Note that for a non-identity element x in a non-cyclic finite group G the number $P_x(G)|G|$ is the degree of the vertex in $\Gamma(G)$ corresponding to x in G. Let $m(G)$ denote the minimal index of a proper subgroup in a finite simple group G.

The following two theorems are needed.

Theorem 4.1 (Liebeck, Shalev, [13]). *There exists a universal constant c_1 so that $1 - (c_1/m(G)) < P(G)$ for an arbitrary finite simple group G.*

Theorem 4.2 (Fulman, Guralnick, [6]). *There exists a universal positive constant c_2 so that $c_2 < P_x(G)$ for an arbitrary non-identity element x in a finite simple group G of Lie type.*

Let G be a finite simple group of Lie type. Let $m+1$ be the order of G and let $d_1 \leq \ldots \leq d_m$ be the list of vertex degrees of the graph $\Gamma(G)$. Let t be the largest index (with $1 \leq t \leq m$) for which $d_t < (m+1)/2$. (We may assume that such a t exists for otherwise $\Gamma(G)$ satisfies Pósa's criterion and so there exists a Hamiltonian cycle in $\Gamma(G)$.) Then

$$(m+1)^2 P(G) = \sum_{i=1}^{m} d_i < t(m+1)/2 + (m-t)(m+1).$$

¿From this inequality and Theorem 4.1 we see that t must satisfy

$$t < \frac{2c_1(m+1)}{m(G)}$$

where c_1 is as in Theorem 4.1. Hence, if G is sufficiently large, then we have

$$t < c_2(m+1).$$

From this and Theorem 4.2 we find that $\Gamma(G)$ satisfies Pósa's criterion and hence contains a Hamiltonian cycle for G sufficiently large.

5. Alternating Groups

In this section it is shown that for every sufficiently large alternating group A_n the graph $\Gamma(A_n)$ satisfies Pósa's criterion (and hence contains a Hamiltonian cycle). This result together with the result of the previous section provides a proof for Theorem 1.2.

Let G be a subgroup of S_n.

Theorem 5.1 (Babai, Hayes, [1]). *For every $\epsilon > 0$ there exists $\delta > 0$ and a threshold n_0 such that for every $n \geq n_0$, if $G \leq S_n$ has fewer than $[\delta n]$ fixed points then the probability that G and a random element $\sigma \in S_n$ generate A_n or S_n is at least $1 - \epsilon$.*

The following direct consequence of Theorem 5.1 is also indicated in [1]. Let π be a permutation in A_n.

Corollary 5.2. *For every $\epsilon > 0$ there exists $\delta > 0$ and a threshold n_0 such that for every $n \geq n_0$, if $\pi \in A_n$ has fewer than $[\delta n]$ fixed points then the probability that π and a random element $\sigma \in A_n$ generate A_n is at least $1 - \epsilon$.*

In this section, let δ and n_0 be positive numbers which fulfill the statement of Corollary 5.2 for $\epsilon = 1/2$. Also, in this section, assume that $n \geq n_0$. Let $A(n)$ be the set of those even permutations of degree n which fix fewer than $[\delta n]$ points and let $B(n)$ be $A_n \setminus A(n)$. Clearly, $|B(n)| \leq n!/([\delta n])!$.

Theorem 5.3. *Let $n \geq 8$. The degree of every vertex in $\Gamma(A_n)$ is at least $n!/(10n^3)$.*

Proof. This follows from the proof of Proposition 7.1 of [9]. □

By Corollary 5.2, our choice of ϵ, and Theorem 5.3, the graph $\Gamma(A_n)$ satisfies Pósa's criterion provided that n is at least $\max\{8, n_0\}$ and satisfies the inequality

$$n!/(10n^3) \geq (n!/([\delta n])!) + 1 \geq |B(n)| + 1.$$

Hence $\Gamma(A_n)$ is indeed Hamiltonian for sufficiently large n.

6. Symmetric Groups

In this section Theorem 1.3 is proved.

Let $\Gamma(G)$ be defined as usual. If $G = S_n$, let $\Gamma_b(G)$ denote the bipartite subgraph of $\Gamma(G)$ obtained by throwing out edges between elements that are not in $H := A_n$. Using a variation on the ideas in [4, §6], we prove:

Theorem 6.1. *Assume that $n > 15$. Then the minimal degree of any vertex in $\Gamma_b(G)$ is at least $n!/n^3$.*

Proof. First suppose that $n = 2m$ is even. Let C be the conjugacy class of products of two cycles of lengths $m+1$ and $m-1$ if m is even and of lengths $m+2$ and $m-2$ if m is odd. If $s \in G \setminus H$, then the probability that a random element of C and s generate G is greater than $1/2$ [4, Lemma 6.4]. Since $|C| \geq (n!)/m^2$, it follows that the vertex degree of s is at least $n!/n^2$.

Let C be a conjugacy class (of G) consisting of three cycles of lengths $d_1 < d_2 < d_3$ with $d_1 = [n/3] - 1$. More precisely, if $n = 3m$ then let $d_1 = m - 1$, $d_2 = m$, $d_3 = m + 1$; if $n = 3m + 1$ then let $d_1 = m - 1$, $d_2 = m$, $d_3 = m + 2$; and if $n = 3m + 2$ then let $d_1 = m - 1$, $d_2 = m + 1$, $d_3 = m + 2$. Note that no element of C lies inside an imprimitive transitive subgroup. Note also that the elements of C have the property that some specific power of any given element of C moves exactly d_2 points and in fact is a cycle of precisely that size. By a result of Williamson [21], it follows that no element of C lies inside a primitive subgroup of G. Hence we conclude that the only maximal subgroups of G containing an element of C are the obvious intransitive subgroups.

Let $1 \neq h \in H$. We want to show that the number of edges in $\Gamma_b(G)$ connecting h and an element of C is at least $n!/n^3$ whenever $n > 15$. Clearly, we can replace h by a power of h and assume that h has prime order. If $h = h_1 h_2$ is a product of two disjoint permutations both in H then the number of edges from h_1 to an element of C is at most the number of edges from h to an element of C. (This is because if $x \in C$ then $\langle h_1, x\rangle$ is transitive implies that $\langle h, x\rangle$ is transitive.) So we may assume that h is either a p-cycle with p an odd prime or a product of two disjoint transpositions. The probability that a random element of C and such an h is intransitive is roughly at most $3(2/3)^3$ and is always less than 0.9. Thus, the probability that h and a random element of C generate G is at least 0.1. Thus, the degree of the vertex h is at least $|C|/10 \geq n!/n^3$ (note that for $x \in C$, we have $|C_G(x)| < (n/3)^3$).

Now suppose that n is odd. Let C be the conjugacy class of n-cycles. If $s \in G \setminus H$ is not a transposition, then the probability that a random element of C and s generate G is greater than $2/3$ [4, Proposition 6.8]. Thus, the vertex degree of s is at least $2|C|/3 = 2(n!)/3n$. Suppose that s is a transposition. If $x \in C$, then $\langle x, s\rangle = G$ unless $\langle x, s\rangle$ is imprimitive.

We reverse the computation. Fix $x \in C$. Take it to be $(1, 2, \ldots, n)$. Note that x fixes a unique partition with block size d for each divisor of n. Let $s = (1j)$. Then $\langle x, s\rangle = G$ if and only if $\gcd(n, j-1) = 1$. So the probability that a random transposition and x generate G is at least $1/n$, whence the probability that s and a random element of C generate G is at least $1/n$. Thus, the degree of the vertex s is at least $|C|/n = (n!)/n^2$.

Now suppose that $1 \neq h \in H$. Let C be the conjugacy class of elements that are a product of an m-cycle and an $m+1$-cycle where $n = 2m+1$. Then the probability that a random element of C and s generate G is greater than $1/2$ [4, Lemma 6.5]. Thus, the degree of the vertex s is at least $(n!)/(2n^2)$. □

Two direct consequences of Theorem 5.1 are

Corollary 6.2. *For every $\epsilon_1 > 0$ there exists $\delta_1 > 0$ and a threshold n_1 such that for every $n \geq n_1$, if $\pi \in S_n \setminus A_n$ has fewer than $[\delta_1 n]$ fixed points then the probability that π and a random element $\sigma \in S_n$ generate S_n is at least $1 - \epsilon_1$.*

Corollary 6.3. *For every $\epsilon_2 > 0$ there exists $\delta_2 > 0$ and a threshold n_2 such that for every $n \geq n_2$, if $\pi \in A_n$ has fewer than $[\delta_2 n]$ fixed points then the probability that π and a random element $\sigma \in S_n$ generate S_n is at least $(1/2) - \epsilon_2$.*

Let δ_1, n_1 and δ_2, n_2 be positive numbers satisfying the statements of Corollaries 6.2 and 6.3 for $\epsilon_1 = 1/5$ and $\epsilon_2 = 1/5$ respectively. Let δ be the minimum of δ_1 and δ_2 and let m_0 be the maximum of n_1 and n_2. Unless otherwise stated assume that $n \geq m_0$. Let $A_1(n)$ and $A_2(n)$ be the set of elements of $S_n \setminus A_n$ and A_n respectively fixing less than $[\delta n]$ points. Let $B_1(n)$ and $B_2(n)$ be $(S_n \setminus A_n) \setminus A_1(n)$ and $A_n \setminus (A_2(n) \cup \{1\})$ respectively. Clearly,

$$|B_i(n)| \leq \frac{n!}{2([\delta n])!}$$

for $i = 1, 2$.

Lemma 6.4. *For sufficiently large n, the set $S_n \setminus A_n$ spans a complete subgraph in the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$. Moreover, for n sufficiently large, every vertex in $A_1(n)$ is connected to every other vertex and every vertex in $B_1(n)$ is connected to at least $(n!/2) - 1 + (n!/n^3)$ other vertices in the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$.*

Proof. Let $n \geq \max\{m_0, 15\}$. Set $\Gamma_0 = \Gamma(S_n)$. We claim that in the graph $\Gamma_1 = \mathrm{cl}(\Gamma(S_n))$ the set $A_1(n)$ spans a complete subgraph and every vertex in $A_1(n)$ is connected to every vertex in $A_2(n)$.

For the first claim notice that for any u, v in $A_1(n)$ we have

$$d(\Gamma_0, u) + d(\Gamma_0, v) > (8/5)(n! - 1) > n! - 1.$$

For the latter claim let $u \in A_1(n)$ and $v \in A_2(n)$. Then

$$d(\Gamma_0, u) + d(\Gamma_0, v) > (11/10)(n! - 1) > n! - 1.$$

Now we claim that, for sufficiently large n, in the graph $\Gamma_2 = \mathrm{cl}^{(2)}(\Gamma(S_n))$ every vertex in $A_1(n)$ is connected to every other vertex in the graph. Let $u \in A_1(n)$ and let $v \in B_1(n) \cup B_2(n)$ be arbitrary. Then, by Theorem 6.1 and by the observation made before the statement of the lemma,

$$d(\Gamma_1, u) + d(\Gamma_1, v) > n! - 2 - |B_1(n) \cup B_2(n)| + n!/n^3 > n! - 1.$$

Next we claim that, in the graph $\Gamma_3 = \mathrm{cl}^{(3)}(\Gamma(S_n))$, every vertex in $B_1(n)$ is connected to every other vertex in $B_1(n)$. Let u and v be two arbitrary elements from $B_1(n)$. Then, again by Theorem 6.1 and by the observation made before the statement of the lemma,

$$d(\Gamma_2, u) + d(\Gamma_2, v) \geq 2|A_1(n)| + (2n!)/(n^3) > n! - 1.$$

Finally, it follows from the above and from Theorem 6.1 that every vertex in $B_1(n)$ is connected to at least $(n!/2) - 1 + (n!/n^3)$ other vertices in the graph Γ_3. □

By Theorem 2.1, the following lemma finishes the proof of Theorem 1.3.

Lemma 6.5. *For sufficiently large n the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$ satisfies Chvátal's criterion. In particular, the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$ contains a Hamiltonian cycle.*

Proof. Put $\Gamma_3 = \mathrm{cl}^{(3)}(\Gamma(S_n))$. Let $d_1 \leq \ldots \leq d_{n!-1}$ be the list of vertex degrees of the graph Γ_3. Let k be a positive integer at most $n!/2$. It is sufficient to show that $d_{n!-1-k} \geq n! - 1 - k$. Since every vertex in $A_1(n)$ has maximum possible degree in Γ_3 by Lemma 6.4, the claim is clear for positive integers k satisfying

$$k \leq \frac{n!}{2} - \frac{n!}{2([\delta n])!}.$$

We may now assume that

$$\frac{n!}{2} - \frac{n!}{2([\delta n])!} < k < \frac{n!}{2}.$$

But then by Theorem 6.1 and Lemma 6.4, we have

$$d_{n!-1-k} \geq \frac{n!}{2} - 1 + \frac{n!}{n^3} > n! - 1 - \frac{n!}{2} + \frac{n!}{2([\delta n])!} \geq n! - 1 - k.$$

□

7. Wreath Products

Let S be a non-abelian finite simple group and let C_m be the cyclic subgroup of S_m generated by the cyclic permutation $\sigma = (1, 2, \ldots, m)$, with $m = p^t$ a prime power. Consider the wreath product $G = S \wr C_m$. Denote the base subgroup of G by $N = S_1 \times \cdots \times S_m$ and let $\pi_i : N \to S_i$ be the projection on the i-th factor. Moreover let $A = \mathrm{Aut}(S)$, $r = p^{t-1}$, $u = r + 1$ and Λ the set $\{1 + ri \mid 0 \leq i \leq p - 1\}$.

Lemma 7.1. *A subgroup H of G coincides with G if the following properties are satisfied:*

(1) $HN/N \cong C_m$;
(2) $\pi_i(H \cap N) \cong S$ for some i;
(3) there exists $(y_1, \dots, y_m) \in H \cap N$ and $a, b \in \Lambda$ such that y_a and y_b are not A-conjugate.

Proof. If H satisfies the first two conditions, then $H \cap N$ is a subdirect product of $N = S_1 \times \cdots \times S_m$. If $H \neq G$ then $H \cap N \leq \prod_j D_j$ where $D_j = \{(s, s^{b_2}, \dots, s^{b_v}) \in \prod_{i \in B_j} S_i \mid s \in S, b_i \in A\}$ is a diagonal subgroup of $\prod_{i \in B_j} S_i$ and the subsets B_j form a system of blocks for the action of C_m on $\{1, \dots, m\}$, with $|B_j| \neq 1$. To conclude note that for any choice of B_j's, a and b belong to the same block. □

Lemma 7.2. *Let i be an integer not divisible by p, $\rho = \sigma^i$, $\tau = \sigma^r$, and $g = (x_1, \dots, x_m)\tau \in G$ where $(x_1, \dots, x_m) \in N$. The probability that there is an edge in $\Gamma(G)$ between g and a randomly chosen element in the coset ρN is at least η, where η is the probability that two randomly chosen elements from S generate S and are not A-conjugate.*

Proof. It is not restrictive to assume that $x_i = 1$ for each $i > r$ (just substitute g with a conjugate g^x for a suitable choice of $x \in N$). Now consider $h = \rho(y_1, \dots, y_m)$. There exists $k < m$ and $(h_1, \dots, h_m) \in N$ such that

$$h^k = (\rho(y_1, \dots, y_m))^k = \tau^{-1}(h_1, \dots, h_m).$$

Let H be the subgroup generated by g and h (which clearly satisfies the first condition of Lemma 7.1). Notice that $H \cap N$ contains $w = (x_1h_1, \dots, x_rh_r, h_u, \dots, h_m)$ and w^g. Notice also that $\pi_u(w^g) = h_1x_1$. In particular the second and third condition of Lemma 7.1) are satisfied if h_u, h_1x_1 are not A-conjugate and generate S. Hence there are $\eta|S|^2$ possible choices for (h_1, h_u). Now notices that there exists two distinct subsets X_1 and X_u of $\{1, \dots, m\}$, of cardinality k such that, for $i \in \{1, u\}$, h_i is the product of the k elements y_j with $j \in X_i$ (in a suitable order); take $a \in X_1 \setminus X_u$ and $b \in X_u \setminus X_1$: to obtain a prescribed value for h_1, h_u, we can choose y_i as we like for $i \notin \{a, b\}$, then choose y_a and y_b in order to get the wanted values. So we find $\eta|N|$ suitable choices for the elements y_i. □

Corollary 7.3. *If $g \in G \setminus N$, then the degree of g as a vertex of $\Gamma(G)$ is at least $\phi(m)|N|\eta = p^{t-1}(p-1)|N|\eta$.*

With similar arguments it can be proved that we have at least $\eta|G|$ edges from the elements that generate G modulo N.

Lemma 7.4. *Let $g = (x_1, \dots, x_m)\sigma \in G$. The probability that there is an edge in $\Gamma(G)$ between g and a randomly chosen element of G is at least η.*

Proof. It is not restrictive (by substituting g with a suitable conjugate) to assume that $x_1 = \cdots = x_{m-1} = 1$. Take an arbitrary element $x = (y_1, \dots, y_m)\sigma^i \in G$; there exist $k \in \mathbb{N}$ and $(z_1, \dots, z_m) \in N$ with $g^k = \sigma^{-i}(z_1, \dots, z_m)$. Clearly $\langle g, x \rangle = G$ if and only if $\langle g, (y_1z_1, \dots, y_mz_m) \rangle = G$: in particular $\langle g, x \rangle = G$ if we choose y_1, y_u so that y_1z_1 and y_uz_u are not A-conjugate and generate S. □

We need now some information on the behavior of $P_n(G)$ when $n \in N$.

Lemma 7.5. *Assume that $n = (x_1, \dots, x_m) \in N$, with $n \neq 1$. Choose $i \in \{1, \dots, m\}$ with the property that $P_{x_i}(S) \geq P_{x_j}(S)$ for each $1 \leq j \leq m$ and let $x = x_i$. Given* *a generator τ of $C_m = \langle \sigma \rangle$, the number of edges connecting n with elements of the coset $N\tau$ is at least $|N|\mu$ with*

$$\mu = \max\left(P_x(S) - \frac{|C_A(x)|}{|S|}, \frac{P_x(S)|C_S(x)|}{|S|}\rho_x\right),$$

with $\rho_x = 1$ if $C_A(x)S = A$ and $\rho_x = 0$ otherwise.

Proof. It is not restrictive to assume that $i = 1$ and $\tau = \sigma$. First we claim that the number of edges connecting n with elements of the coset $N\sigma$ is at least $|N|\mu_1$ with

$$\mu_1 = P_x(S) - \frac{|C_A(x)|}{|S|}.$$

It suffices to prove that, for any $y_2, \ldots, y_m \in S^{m-1}$, there exist at least $\mu_1|S|$ choices for y_1 such that if $g = (y_1, \ldots, y_m)\sigma$ then $\langle n, g\rangle = G$. We have $g^m = (h_1, \ldots, h_m)$ with $h_1 = y_1 y_2 \cdots y_m$. In particular the second condition of Lemma 7.1 is satisfied if x and h_1 generate S and there are at least $|S|P_x(S)$ choices for y_1 for which this is ensured. If there exist $\lambda \in \Lambda$ with x_1 and x_λ not A-conjugate, then the third condition is automatically satisfied and we are done. Otherwise for each $1 \le i \le p-1$ there exist $\alpha_i \in A$ with $x_{ir+1} = x^{\alpha_i}$. In this case to be sure that $H = \langle g, n\rangle = G$ we need an extra condition on y_1 to avoid that $\pi_\Lambda(H \cap N) = (s, s^{\beta_1}, \ldots, s^{\beta_{p-1}})$ with $\beta_i \in A$. Assume that this is the case. Since $(x, x_{r+1}, \ldots, x_{r(p-1)+1}) = \pi_\Lambda(n)$, we must have $\beta_i \in C_A(x)\alpha_i$. Let $g^r = (k_1, \ldots, k_m)\sigma^r$ and let ϵ be the p-cycle $(1, r+1, \ldots, r(p-1))$. Since g^r normalizes $H \cap N$, we have that $(k_1, k_{r+1}, \ldots, k_{r(p-1)+1})\epsilon$ normalizes $\pi_\Lambda(H \cap N) = (s, s^{\beta_1}, \ldots, s^{\beta_{p-1}})$. In particular, setting $z = \beta_{p-1}k_{r(p-1)+1}$, we have $z\beta_1 = k_1$ and $z\beta_i = \beta_{i-1}k_{(i-1)r+1}$ for each $2 \le i \le p-1$ and consequently

$$z^p = k_1 k_{r+1} \cdots k_{r(p-1)+1} = h_1.$$

Since $k_{r(p-1)+1}$ depends only on $y_2, \ldots, y_n$, the set $\Delta = \{(t\alpha_{p-1}k_{r(p-1)+1})^p \mid t \in C_A(x)\}$ is independent from y_1. If we choice y_1 such that $\langle x, h_1\rangle = S$ and $h_1 \notin \Delta$, then $\langle g, n\rangle = G$. Clearly the number of y_1 for which h_1 satisfies the two previous conditions is at most

$$|S|\left(P_x(S) - \frac{|C_A(x)|}{|S|}\right).$$

This concludes the proof of the first claim. Now we want to show that the number of edges connecting n with elements of the coset $N\sigma$ is at least $|N|\mu_2$ with

$$\mu_2 = \frac{P_x(S)|C_S(x)|}{|S|}\rho_x.$$

Note that there are at least $\mu_2|N|$ choices of $(y_1, \ldots, y_m)$ so that $\langle h_1, x\rangle = S$ and $k_{r(p-1)+1} \in \alpha_{p-1}^{-1}C_A(x)$. We claim that for any of these choices, $g = (y_1, \ldots, y_m)\sigma$ generates G together with n. By the argument that we have used above, and under the same notations, it suffices to prove that $z^p \ne h_1$. Notice that $z = \beta_{p-1}k_{r(p-1)+1} \in \beta_{p-1}\alpha_{p-1}^{-1}C_A(x) \le C_A(x)$, hence $z^p = h_1$ would imply $[h_1, x] = 1$, against $\langle h_1, x\rangle = S$. □

Lemma 7.6. *Let S be a non-abelian finite simple group and let $c(S)$ be the maximal size of a conjugacy class of S. Then $\lim_{|S|\to\infty}(c(S)|\mathrm{Out}(S)|)/|S| = 0$.*

Proof. If S is a finite simple group of Lie type, then this follows by [7, Theorem 1.4]. If $S = A_n$ for $n > 6$, then $(c(S)|\mathrm{Out}(S)|)/|S| \le 4/n$. □

Lemma 7.7. *Let η be as above. Then $\lim_{|S|\to\infty} \eta = 1$.*

Proof. Let S be a non-abelian finite simple group and let A be the automorphism group of S. Notice that $\eta \geq 1 - p - q$ where p is the probability that a random pair of elements of S does not generate S and q is the probability that a random pair of elements of S is A-conjugate. By Theorem 4.1), p tends to 0 as $|S|$ tends to infinity. Thus, to prove the lemma, it is sufficient to show that q tends to 0 as $|S|$ tends to infinity.

Let k be the number of A-conjugacy classes of elements of S and let $a_1, \ldots, a_k$ be the corresponding orbit sizes with $a_1 \geq \ldots \geq a_k$. We have $q = (\sum_{i=1}^{k} {a_i}^2)/|S|^2$.

Put $a = a_1$, $n = |S|$, and $b = n - [n/a]a$. We claim that $q \leq ([n/a]a^2 + b^2)/n^2$. Before verifying this claim, let us show how our lemma would follow.

Indeed,

$$q \leq \frac{[n/a]a^2 + b^2}{n^2} < \frac{a}{n}\Big(1 + \frac{a}{n}\Big) \leq \frac{c(S)|\mathrm{Out}(S)|}{n}\Big(1 + \frac{c(S)|\mathrm{Out}(S)|}{n}\Big)$$

and, by Lemma 7.6, the right-hand-side of this inequality tends to 0 as n tends to infinity, hence q must tend to 0.

Finally, for the proof of our claim, observe that if x and y are two positive integers with $x \leq y$, then $(x-1)^2 + (y+1)^2 = x^2 + y^2 + 2 + 2(y - x) > x^2 + y^2$. This means that, starting from the list $a = a_1, \ldots, a_k$, we may derive a sequence of lists by replacing two elements x and y of the previous list by $x - 1$ and $y + 1$ in the next list, whenever $1 \leq x \leq y < a$. This way, the last list of non-negative integers will be $a, \ldots, a, b, 0, \ldots, 0$ where $b = n - [n/a]a$. □

We are now in the position to prove Theorem 1.4.

We divide the vertices of $\Gamma(G)$ into three disjoint subsets:

- V_1 is the set of vertices corresponding to elements $(y_1, \ldots, y_m)\tau$ with $|\tau| = m$;
- V_2 is the set of vertices corresponding to elements $(y_1, \ldots, y_m)\tau$ with $1 < |\tau| < m$;
- V_3 is the set of vertices corresponding to the non trivial elements of the base group N of the wreath product.

Let $\Gamma_0 = \Gamma(G)$ and $\Gamma_i = \mathrm{cl}^{(i)}(\Gamma(G))$ for $i \geq 1$. By Lemma 7.4 and Corollary 7.3, if $u \in V_1$ and $v \in V_1 \cup V_2$, then

$$d(\Gamma_0, u) + d(\Gamma_0, v) \geq \eta|G| + \eta|G|\left(1 - \frac{1}{p}\right) \geq 3\eta|G|/2.$$

Since η tends to 1 as $|S|$ tends to infinity (by Lemma 7.7), we deduce that if $|S|$ is large enough then any vertex in V_1 is connected to any other vertex in $V_1 \cup V_2$ in the first closure Γ_1. But then, if $v_1, v_2 \in V_2$, then

$$d(\Gamma_1, v_1) + d(\Gamma_1, v_2) \geq 2|V_1| = 2\left(1 - \frac{1}{p}\right)|G| \geq |G|$$

which means that Γ_2 induces a complete subgraph on $V_1 \cup V_2$.

To complete the proof we need different arguments for the Lie and alternating cases.

First assume that S is a group of Lie type. By Theorem 4.2 and the fact that $\max_{x \in S, x \neq 1} |C_A(x)|/|S|$ tends to 0 as $|S|$ tends to infinity, we deduce that there exists a positive constant c_3 such that, if S is large enough then, for any $x \in S \setminus \{1\}$,

$$P_x(S) - \frac{|C_A(x)|}{|S|} \geq c_3.$$

By Lemmas 7.4 and 7.5, for any $u \in V_1$ and $u \in V_3$ we have

$$d(\Gamma_0, u) + d(\Gamma_0, v) \geq \eta|G| + c_3|G| \left(1 - \frac{1}{p}\right) = \left(\eta + c_3 \left(1 - \frac{1}{p}\right)\right) |G|.$$

If $|S|$ is large enough, then $\eta + c_3(1 - 1/p) \geq 1$: in this case any vertex in V_1 is connected to any other vertex in V_3 in the first closure Γ_1, and this implies that Γ_2 is a complete graph.

We remain with the alternating groups. In this case we need to use the Babai-Hayes Theorem. Let δ and n_0 be positive numbers which fulfill the statement of Corollary 5.2 for $\epsilon = 1/2$. Let $A(n)$ be the set of those even permutations of degree n which fix fewer than $[\delta n]$ points. We divide V_3 into two disjoint subsets: W_1 is the set of elements $(y_1, \ldots, y_m)$ of N with the property that $y_i \in A(n)$ for some $1 \leq i \leq m$; $W_2 = V_3 \setminus W_1$. Since $P_x(S) \geq 1/2$ for each $x \in A(n)$, arguing as in the case of groups of Lie type we deduce that Γ_2 induces a complete subgraph on $V_1 \cup V_2 \cup W_1$. Let now $w = (y_1, \ldots, y_m) \in W_2$ and assume that $y = y_i$ has the property that $P_{y_i}(S) \geq P_{y_j}(S)$ for each $1 \leq j \leq m$. Let now $p = P_y(S)$ and $c = |C_A(y)|/|S|$ and consider

$$\mu = \max\left(P_y(S) - \frac{|C_A(y)|}{|S|}, \frac{P_y(S)|C_S(y)|}{|S|}\right).$$

If $c \leq p/2$ then $\mu \geq p/2 \geq p^2/4$, otherwise, if $c \geq p/2$, we again have $\mu \geq p^2/4$. Moreover, by Theorem 5.3, $p \geq 1/(5n^3)$, hence, by Lemma 7.5,

$$d(\Gamma_2, w) \geq d(\Gamma_0, w) \geq \frac{(p^t - p^{t-1})|N|}{100n^6}.$$

On the other hand

$$|W_2| \leq |S - A(n)|^m \leq \left(\frac{n!}{[\delta n]!}\right)^m \leq |N| \left(\frac{2}{[\delta n]!}\right)^m$$

so if n is large enough, $d(\Gamma_2, w) > |W_2|$ for each $w \in W_2$. This means that Γ_2 satisfies Pósa's criterion, and hence contains a Hamiltonian cycle.

8. Computer Calculations

The main results of this paper hold for *sufficiently large* groups. In this section, we consider *small* groups and sporadic simple groups. In particular, we get a computational proof of Theorem 1.5. (Currently, we do not know how large the gap between *small* and *sufficiently large* is.)

Using the same computational methods as in [4, Section 2.5], we showed that the generating graphs of the following groups contain Hamiltonian cycles.

- Non-abelian simple groups of orders at most 10^7,
- groups G containing a unique minimal normal subgroup N such that N has order at most 10^6, N is nonsolvable, and G/N is cyclic,
- alternating and symmetric groups on n points, with $5 \leq n \leq 13$,
- sporadic simple groups and automorphism groups of sporadic simple groups.

More specifically, the generating graphs of the simple groups in this list satisfy Pósa's criterion, and for each non-simple group in this list a suitable iterated closure of the generating graph satisfies Pósa's criterion.

For that, we define the *partial vertex degree* of the non-identity element s w. r. t. the conjugacy class C as $d(\Gamma(G), s, C) = |\{x \in C; \langle s, x\rangle = G\}|$. The vertex degree $d(\Gamma(G), s)$ equals $\sum_C d(\Gamma(G), s, C)$, where C runs over the conjugacy classes of G, and a lower bound for $d(\Gamma(G), s, g^G)$ is given by $|g^G| - \sum_{M \in \mathcal{M}(G,s)} |g^G \cap M|$, where $\mathcal{M}(G, s)$ denotes the set of those maximal subgroups of G that contain s.

The point is that these lower bounds can be computed easily if the primitive permutation characters of G are known. This is the case when the table of marks of G is available or if the character tables of G and of all its maximal subgroups (and the necessary class fusions) are available, for example if G is a sporadic simple group not equal to the Monster.

Defining partial vertex degrees for the iterated closures of $\Gamma(G)$ in the obvious way, we get $d(\mathrm{cl}(\Gamma(G)), s, g^G) = |g^G|$ if $d(\Gamma(G), s) + d(\Gamma(G), g) \geq |G| - 1$, and $d(\mathrm{cl}(\Gamma(G)), s, g^G) = d(\Gamma(G), s, g^G)$ otherwise.

Note that lower bounds for the partial vertex degrees for the closures of $\Gamma(G)$ can be computed this way from lower bounds for the partial vertex degrees for $\Gamma(G)$.

If the primitive permutation characters of G are not known then computing the (partial) vertex degrees directly, without character-theoretic computations, is usually faster than computing first the character information.

It turned out that this approach was sufficient to prove that Pósa's criterion holds for appropriate closures $\mathrm{cl}^{(i)}(\Gamma(G))$, for all groups G listed above. See [3] for more information.

9. Proof of Proposition 1.7

Let us use the notations and assumptions of Proposition 1.7. Notice that if G is generated by elements x and y then $d(x) + d(y) \leq \dim(V)$. Indeed, if $d(x) + d(y) > \dim(V)$, then any non-trivial subspace of $U \cap W$ is G-invariant contradicting the irreducibility of V where U and W are eigenspaces of x and y on V of dimensions $d(x)$ and $d(y)$, respectively.

Let $n+1$ be the order of G and let $x_1, \ldots, x_n, x_{n+1} = x_1$ be a Hamiltonian cycle in the graph $\Gamma(G)$. Then $d(x_i) + d(x_{i+1}) \leq \dim(V)$ for all i with $1 \leq i \leq n$, hence

$$\sum_{i=1}^{n} d(x_i) = \frac{1}{2} \sum_{i=1}^{n} (d(x_i) + d(x_{i+1})) \leq \frac{n}{2} \dim(V)$$

which is exactly what we wanted.

Acknowledgment. We thank L. Pyber for drawing our attention to [1].

References

[1] Babai, L.; Hayes, T. P. The probability of generating the symmetric group when one of the generators is random. *Publ. Math. Debrecen* **69/3** (2006), 271-280.

[2] Bondy, J. A.; Chvatal, V. A method in graph theory. *Discrete Math.* **15** (1976), 111-136.

[3] Breuer, T. GAP computations concerning Hamiltonian cycles in the generating graphs of finite groups. arXiv:0911.5589.

[4] Breuer, T.; Guralnick, R. M.; Kantor, W. M. Probabilistic generation of finite simple groups, II. *J. Algebra* Vol. 320. **2**, (2008), 443-494.

[5] Burness, T.; Guest, S.; Guralnick, R. M. Finite groups with positive spread, in preparation.

[6] Fulman, J.; Guralnick, R. M. The probability of generating an irreducible subgroup, preprint.

[7] Fulman, J.; Guralnick, R. M. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. arXiv:0902.2238.

[8] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.4*; 2005, (`http://www.gap-system.org`).

[9] Guralnick, R. M.; Kantor, W. M. Probabilistic generation of finite simple groups. *J. Algebra* Vol. 234. **2**, (2000), 743-792.

[10] Guralnick, R. M.; Shalev, A. On the spread of finite simple groups. *Combinatorica* **23** (1) (2003), 73-87.

[11] Isaacs, I. M.; Keller, T. M.; Meierfrankenfeld, U.; Moretó, A. Fixed point spaces, primitive character degrees and conjugacy class sizes. *Proc. Am. Math. Soc.* **134** 11, (2006), 3123-3130.

[12] The Kourovka Notebook. Unsolved problems in group theory. Sixteenth augmented edition, 2006. Edited by V. D. Mazurov and E. I. Khukhro.

[13] Liebeck, M. W.; Shalev, A. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), no. 1, 31–57.

[14] Lovász, L. Combinatorial problems and exercises. North-Holland, Amsterdam, 1979.

[15] Lucchini, A.; Maróti, A. Some results and questions related to the generating graph of a finite group. To appear in *Proceedings of the Ischia Group Theory Conference 2008.*

[16] Lucchini, A.; Maróti, A. On the clique number of the generating graph of a finite group. *Proc. Am. Math. Soc.* **137**, No. 10, (2009), 3207-3217.

[17] Lucchini, A.; Maróti, A. On finite simple groups and Kneser graphs. *J. Algebr. Comb.* **30** No. 4, (2009), 549-566.

[18] Luczak, T.; Pyber, L. On random generation of the symmetric group. *Combinatorics, Probability and Computing* **2** (1993), 505-512.

[19] Neumann, P. M.; Vaughan-Lee, M. R. An essay on BFC groups. *Proc. London Math. Soc.* (3) **35** (1977), 213-237.

[20] Segal, D.; Shalev, A. On groups with bounded conjugacy classes. *Quart. J. Math. Oxford* **50** (1999), 505-516.

[21] Williamson, A. On primitive permutation groups containing a cycle. *Math. Z.* **130** (1973), 159-162.

Thomas Breuer, Lehrstuhl D für Mathematik, RWTH Aachen University, 52065 Aachen, Germany. E-mail address: sam@math.rwth-aachen.de

Robert M. Guralnick, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA. E-mail address: guralnic@usc.edu

Andrea Lucchini, Dipartimento di Matematica Pura ed Applicata, Via Trieste 63, 35121 Padova, Italy. E-mail address: lucchini@math.unipd.it

Attila Maróti, MTA Alfréd Rényi Institute of Mathematics, Budapest, Hungary. E-mail address: maroti@renyi.hu

Gábor Péter Nagy, SZTE Bolyai Institute, Aradi Vértanúk tere 1, Szeged, 6720, Hungary. E-mail address: nagyg@math.u-szeged.hu