ISRAEL JOURNAL OF MATHEMATICS **162** (2007), 81–92
DOI: 10.1007/s11856-007-0089-4

ON THE NUMBER OF GENERATORS NEEDED FOR FREE PROFINITE PRODUCTS OF FINITE GROUPS

BY

Miklós Abért*

Department of Mathematics, University of Chicago
5734 University Ave., Chicago, IL 60637, USA
e-mail: abert@math.uchicago.edu

AND

Pál Hegedűs**

Department of Algebra and Number Theory, Eötvös Loránd University
Budapest H-1518, P.O. Box 120, Hungary
e-mail: hegpal@cs.elte.hu

ABSTRACT

We provide lower estimates on the minimal number of generators of the profinite completion of free products of finite groups.

In particular, we show that if $C_1, \ldots, C_n$ are finite cyclic groups then there exists a finite group G which is generated by isomorphic copies of $C_1, \ldots, C_n$ and the minimal number of generators of G is n.

1. Introduction

For a group G let $d(G)$ denote the minimal number of generators for G. If G is a profinite group then we mean topological generation rather than the abstract one. Let $\widehat{G}$ denote the profinite completion of G; trivially $d(\widehat{G}) \leq d(G)$. The first finitely generated residually finite examples where the two quantities are

* The first author's research is partially supported by NSF grant DMS-0701105.
** The second author's research is partially supported by OTKA grant T38059 and the Magyary Zoltán Postdoctoral Fellowship.
Received April 25, 2006

different were found by Noskov [Nos]. His examples were metabelian and he also showed that for these groups we have

$$d(G) \leq (t^2 + 5t + 2)/2 \quad \text{with } t = d(\widehat{G}).$$

An old question Melnikov [Kou, 6.31] raised was whether $d(G)$ is always bounded by a function of $d(\widehat{G})$ for a residually finite, finitely generated group G. This has been recently answered negatively by Wise [Wis] but is still open for linear groups.

Another class of groups where passing to profinite completion may imply a drop in the minimal number of generators is free products of finite groups. Let $G_1, G_2, \ldots, G_n$ be finite groups, let $s = \max_i d(G_i)$ and let

$$\Gamma = G_1 * G_2 * \cdots * G_n$$

be the free product of the G_i. Then the so-called Grushko–Neumann theorem (see [Gru] and [Neu]) says that $d(\Gamma) = \sum_i d(G_i)$. On the other hand, Kovács and Sim [KoS] showed that if the G_i are solvable and have pairwise coprime orders then $d(\widetilde{\Gamma}) \leq n + s - 1$, where $\widetilde{\Gamma}$ denotes the prosolvable completion of Γ. In the language of finite groups this translates to stating that if G is a finite solvable group which is generated by subgroups isomorphic to $G_1, G_2, \ldots, G_n$, then $d(G) \leq n + s - 1$ (see [RiW]).

This was followed by work of Lucchini [Lu1] who, using the Classification of Finite Simple Groups, showed that there exists an absolute constant c such that if the G_i have pairwise coprime orders and $n > 2$ then

$$d(\widehat{\Gamma}) \leq (1 + (4c)/3)(n - 1) + 2s + c.$$

It is conjectured that if the G_i have pairwise coprime orders then in fact

$$d(\widehat{\Gamma}) = n + s - 1.$$

The upper bound $d(\widehat{\Gamma}) \leq n + s$ is proved by Lucchini in [Lu1, Theorem C] in the case when the G_i are p_i-groups for distinct primes p_i.

The aim of this paper is to support general lower bounds for $d(\widehat{\Gamma})$. For some special families of finite groups this has been done by Kovács and Sim [KoS]. The first estimate of this type works for arbitrary finite groups and trivially implies $d(\Gamma) \leq d(\widehat{\Gamma})^2$.

THEOREM 1: *Let $G_1, G_2, \ldots, G_n$ be finite groups and let $\Gamma = G_1 * G_2 * \cdots * G_n$. Then*

$$d(\widehat{\Gamma}) \geq n.$$

In particular, if all the G_i are nontrivial cyclic, then we have the equality $d(\widehat{\Gamma}) = n$, proving the above conjecture for the case $s = 1$. In fact, as Proposition 9 shows, already $d(\widetilde{\Gamma}) = n$.

Note that the weaker estimate

$$d(\widehat{\Gamma}) \geq n - \sum_{i=1}^{n} \frac{1}{|G_i|}$$

can be proved in various ways. In particular, it is immediate from the following observation, which may be interesting in itself.

Proposition 2: *Let Γ be a finitely presented residually finite group. Then*

$$d(\widehat{\Gamma}) \geq b_1^{(2)}(\Gamma) + 1,$$

where $b_1^{(2)}(\Gamma)$ denotes the first L_2-Betti number of Γ.

Note that by the definition of L_2-Betti numbers $d(\Gamma) \geq b_1^{(2)}(\Gamma)+1$ for arbitrary groups [Luc].

Our second theorem involves s in the lower estimate in the following form.

Theorem 3: *Let $G_1, G_2, \ldots, G_n$ be finite groups, let $\Gamma = G_1 * G_2 * \cdots * G_n$ and let*

$$s' = \max(d(G_i/G_i')).$$

Then

$$d(\widehat{\Gamma}) \geq n + s' - 1.$$

In particular, if all the G_i are nilpotent then $d(\widehat{\Gamma}) \geq n + s - 1$ which sets the conjectured lower bound. Moreover, if the G_i are p_i-groups for distinct primes p_i, then using Lucchini's upper bound we get

$$n + s - 1 \leq d(\widehat{\Gamma}) \leq n + s.$$

For groups of pairwise coprime order where the minimal number of generators is not witnessed by the abelianization, we are unable to set the conjectured lower bound in general, but in the case $s = 2$ we can show that it is the best possible one can hope for.

Theorem 4: *For every n there exist solvable groups $G_1, G_2, \ldots, G_n$ of pairwise coprime order such that $d(G_i) = 2$, G_i/G_i' is cyclic $(1 \leq i \leq n)$ and for $\Gamma = G_1 * G_2 * \cdots * G_n$ we have $d(\widehat{\Gamma}) \geq n + 1$.*

2. Proofs

First we prove Proposition 2. Note that this is independent of the rest of the paper and it provides a weaker bound than the one obtained with our main method. However, it is readily generalized to all classes of groups where we can compute the first L_2 Betti number, e.g., to amalgamated products.

Proof of Proposition 2: Let $N_1 \lhd \Gamma$ be a normal subgroup of finite index such that $d(\widehat{\Gamma}) = d(\Gamma/N)$. Let

$$\Gamma = N_0 \geq N_1 \geq N_2 \geq \cdots$$

be an infinite chain of normal subgroups of Γ of finite index such that $\bigcap_i N_i = 1$. Let $K_i = N_i' N_i^2$, where N_i' denotes the derived subgroup and N_i^2 is the normal subgroup generated by all squares in N_i $(i \geq 0)$. Let $G_i = \Gamma/N_i$ and let $H_i = \Gamma/K_i$ $(i \geq 0)$. Let d_i denote the torsion-free rank of the abelianization of N_i (or in other words, the first homology of N_i). Using a theorem of Lück [Luc], we have

$$b_1^2(\Gamma) = \lim_{n\to\infty} d_n/|G_n|.$$

Now N_i/K_i, is an elementary abelian 2-group and

$$d(N_i/K_i) \geq d_i \quad i \geq 0.$$

The index of N_i/K_i in H_i is $|G_i|$ and so using the Nielsen–Schreier theorem we have

$$d(N_i/K_i) \leq (d(H_i) - 1)|G_i| + 1 \quad i \geq 0$$

which gives us

$$d(H_i) \geq \frac{d(N_i/K_i) - 1}{|G_i|} + 1 \geq \frac{d_i - 1}{|G_i|} + 1 \quad i \geq 0.$$

Since $\bigcap_i K_i \leq \bigcap_i N_i = 1$ and $|G_n| \to \infty$, we have

$$d(\widehat{\Gamma}) = \lim_{n\to\infty} d(H_i) \geq \lim_{n\to\infty} \frac{d_n - 1}{|G_n|} + 1 = b_1^2(\Gamma) + 1.$$

The proposition holds. ∎

Now we start building towards Theorem 1 and Theorem 3.

Let Γ be a finitely generated group and H a finite group. Let $\mathrm{Hom}(\Gamma, H)$ denote the set of homomorphisms from Γ to H. Then $\mathrm{Hom}(\Gamma, H)$ is finite. Let

$$h(\Gamma, H) = \frac{\log|\mathrm{Hom}(\Gamma, H)|}{\log|H|}$$

The number $h(\Gamma, H)$ will be the key notion of this paper. Let

$$K(\Gamma, H) = \bigcap_{\varphi \in \mathrm{Hom}(\Gamma, H)} \ker \varphi$$

and let the quotient group

$$G(\Gamma, H) = \Gamma / K(\Gamma, H).$$

Since $K(\Gamma, H)$ can be obtained as a finite intersection of subgroups of finite index, $G(\Gamma, H)$ is a finite image of Γ. Also, each homomorphism from Γ to H factors through $K(\Gamma, H)$, so we have

$$|\operatorname{Hom}(\Gamma, H)| = |\operatorname{Hom}(G(\Gamma, H), H)|$$

implying

$$h(G(\Gamma, H), H) = h(\Gamma, H).$$

The following two basic lemmas are needed later.

Lemma 5: *Let Γ_i $(1 \leq i \leq n)$ be finitely generated groups and let H be a finite group. Then*

$$h(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n, H) = \sum_{i=1}^{n} h(\Gamma_i, H)$$

Proof: By the definition of a free product, for every set of homomorphisms $\varphi_i \in \operatorname{Hom}(\Gamma_i, H)$ $(1 \leq i \leq n)$ there exists a unique homomorphism $\varphi \in \operatorname{Hom}(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n, H)$ such that the restriction of φ to Γ_i equals φ_i $(1 \leq i \leq n)$. Hence

$$|\operatorname{Hom}(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n, H)| = \prod_{i=1}^{n} |\operatorname{Hom}(\Gamma_i, H)|$$

implying

$$h(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n, H) = \frac{\log |\operatorname{Hom}(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n, H)|}{\log |H|} = \frac{\sum_{i=1}^{n} \log(|\operatorname{Hom}(\Gamma_i, H)|)}{\log |H|} = \sum_{i=1}^{n} h(\Gamma_i, H)$$

as claimed. ∎

Lemma 6: *Let* Γ *be a finitely generated group and let* H *be a finite group. Then*

$$h(\Gamma, H^n) = h(\Gamma, H)$$

for all natural numbers n.

Proof: A function $\varphi\colon \Gamma \to H^n$ is a homomorphism if and only if all the coordinate functions of φ are homomorphisms into H. Thus $|\operatorname{Hom}(\Gamma, H^n)| = |\operatorname{Hom}(\Gamma, H)|^n$ which implies the statement. ∎

The following lemma establishes a connection between the function h and the minimal number of generators for the profinite completion.

Lemma 7: *Let* G_i *be finite groups* ($1 \le i \le n$) *and let*

$$\Gamma = G_1 * G_2 * \cdots * G_n.$$

Then

$$d(\widehat{\Gamma}) \geq \sum_{i=1}^{n} h(G_i, H)$$

for any finite group H.

Proof: If G is an arbitrary homomorphic image of Γ then $\operatorname{Hom}(G, H) \le \operatorname{Hom}(\Gamma, H)$ and so we have $h(G, H) \le h(\Gamma, H)$ as well. In particular, for $d = d(G)$ we have

$$h(G, H) \le h(F_d, H) = \frac{\log|\operatorname{Hom}(F_d, H)|}{\log|H|} = \frac{\log(|H|^d)}{\log|H|} = d.$$

Using this and Lemma 5 we have

$$d(\widehat{\Gamma}) \geq d(G(\Gamma, H)) \geq h(G(\Gamma, H), H) = h(\Gamma, H) = \sum_{i=1}^{n} h(G_i, H),$$

as claimed. ∎

So in order to obtain a lower bound on $d(\widehat{\Gamma})$ we have to find a target group H, such that all the G_i have many homomorphisms into H. Note that if we choose the target group to be a large symmetric group or a large dimensional general linear group over a fixed finite field, we get the estimate

$$d(\widehat{\Gamma}) \geq n - \sum_{i=1}^{n} \frac{1}{|G_i|}$$

already established by Proposition 2. It turns out that the best target groups for our purposes will be produced from semisimple G_i-modules over finite fields.

Proof of Theorem 1: Recall that $O_p(G)$ denotes the largest normal p-subgroup of G. Let p be a prime such that

$$O_p(G_i) = 1 \quad 1 \le i \le n$$

and let $F = \mathbb{F}_p$ be the field of order p. Let M_i be a nontrivial simple G_i-module over F of dimension $d_i = \dim_F M_i$ $(1 \le i \le n)$. Let l be the least common multiple of the d_i and let V be a vector space over F of dimension l.

Let $1 \le i \le n$. Since d_i divides l, V can be turned into a semisimple G_i-module such that all the simple factors of V under G_i are isomorphic to M_i. Let $L_i \subseteq GL(V)$ denote the linear action of G_i on V. Since M_i is nontrivial, L_i is not the trivial group and since M_i is simple, L_i has no nonzero fixed vector in V.

Let

$$R = \langle L_i \mid 1 \le i \le n \rangle \subseteq GL(V)$$

be the linear group generated by the L_i. Then V is a simple R-module. Let $r = |R|$.

Let m be a natural number and let H be the semidirect product of V^m and R. Then H has order $p^{lm}r$. We want to estimate $|\operatorname{Hom}(G_i, H)|$ from below. It will suffice to consider conjugates of a fixed surjective homomorphism from G_i to L_i. The number of those conjugates equals the size of the conjugacy class of L_i in H. Since L_i has no fixed vector in V, the centralizer $C_H(L_i) \le R$. This implies

$$|\operatorname{Hom}(G_i, H)| \ge \frac{|H|}{|C_H(L_i)|} \ge \frac{|H|}{r} = p^{lm}$$

so

$$h(G_i, H) \ge \frac{\log p^{lm}}{\log(p^{lm}r)} = 1 - \frac{\log r}{m \log p^l + \log r}.$$

Using Lemma 7 gives

$$d(\widehat{\Gamma}) \ge \sum_{i=1}^{n} h(G_i, H) \ge n\Big(1 - \frac{\log r}{m \log p^l + \log r}\Big).$$

Letting m to be arbitrarily large this leads to

$$d(\widehat{\Gamma}) \ge n.$$

The theorem holds. ∎

Now we prove Theorem 3 using the construction above.

Proof of Theorem 3: We can assume that $d(G_n/G_n') = s'$. Let p be a prime such that $p^{s'}$ divides $|G_n/G_n'|$ and let $F = \mathbb{F}_p$ be the field of order p. By permuting the G_i we can also assume that there exists $0 \leq t < n$ such that p does not divide $|G_i/G_i'|$ $(1 \leq i \leq t)$ and p divides $|G_i/G_i'|$ $(t+1 \leq i \leq n)$. Let us define a new list of finite groups H_i $(1 \leq i \leq t+1)$ as follows. For $1 \leq i \leq t$ let

$$H_i = G_i/O_p(G_i)$$

and let

$$H_{t+1} = C_p^{s'+n-t-1}.$$

From here we follow the construction and notation in the proof of Theorem 1 using the H_i $(1 \leq i \leq t)$ and p as prime. This is allowed since $O_p(H_i) = 1$ $(1 \leq i \leq t)$. For m large enough, let H be the target group given by the construction. Then, as before, we have

$$h(H_i, H) \geq 1 - \frac{\log r}{m \log p^l + \log r} \quad 1 \leq i \leq t.$$

Now $\mathrm{Hom}(H_{t+1}, V^m) \subseteq \mathrm{Hom}(H_{t+1}, H)$ implying

$$\begin{aligned} h(H_{t+1}, H) &= \frac{\log |\mathrm{Hom}(H_{t+1}, H)|}{\log |H|} \geq \frac{\log |\mathrm{Hom}(H_{t+1}, V^m)|}{m \log |V| + \log |R|} \\ &= h(H_{t+1}, V^m) \frac{m \log |V|}{m \log |V| + \log |R|} \end{aligned}$$

and $|\mathrm{Hom}(H_{t+1}, C_p)| = p^{s'+n-t-1}$ implying

$$h(H_{t+1}, V^m) = h(H_{t+1}, C_p) = s' + n - t - 1$$

which gives

$$\sum_{i=1}^{t+1} h(H_i, H) \geq (s' + n - t - 1) \frac{m \log |V|}{m \log |V| + \log |R|} + t\Big(1 - \frac{\log r}{m \log p^l + \log r}\Big)$$

Setting m to be large enough and using Lemma 7 we get

$$d(\widehat{H_1 * \cdots * H_{t+1}}) \geq \sum_{i=1}^{t+1} h(H_i, H) \geq s' + n - 1.$$

On the other hand, H_i is a quotient of G_i $(1 \leq i \leq t)$ and H_{t+1} is a quotient of $G_{t+1} * \cdots * G_n$ which implies that $H_1 * \cdots * H_{t+1}$ is a quotient of Γ, leading to

$$d(\widehat{\Gamma}) \geq d(\widehat{H_1 * \cdots * H_{t+1}}) \geq s' + n - 1.$$

The theorem holds. ∎

For a prime p let $\mathrm{Aff}(p)$ denote the group of affine transformations of $\mathbb{F}_p$. Then $\mathrm{Aff}(p)$ acts on $\mathbb{F}_p$ and so it embeds into the symmetric group $\mathrm{Sym}(\mathbb{F}_p)$.

Lemma 8: *Let $H \leq \mathrm{Aff}(p)$ be a subgroup properly containing the additive subgroup $\mathbb{F}_p$. Then the centralizer $C_{\mathrm{Sym}(\mathbb{F}_p)}(H) = 1$.*

Proof: Since $\mathbb{F}_p$ is abelian and transitive in $\mathrm{Sym}(\mathbb{F}_p)$, $C_{\mathrm{Sym}(\mathbb{F}_p)}(\mathbb{F}_p) = \mathbb{F}_p$, implying $C_{\mathrm{Sym}(\mathbb{F}_p)}(H) \leq \mathbb{F}_p$. Let $h \in H \backslash \mathbb{F}_p$. Then h acts on $\mathbb{F}_p$ as multiplication by a non-identity element, thus $C_{\mathbb{F}_p}(h) = \{0\}$, giving $C_{\mathrm{Sym}(\mathbb{F}_p)}(H) = 1$. ∎

Now we prove Proposition 9. It is again a slight modification of the construction in Theorem 1.

Proposition 9: *Let $G_1, G_2, \ldots, G_n$ be finite cyclic groups and let $\Gamma = G_1 * G_2 * \cdots * G_n$. Then*

$$d(\widetilde{\Gamma}) = d(\widehat{\Gamma}) = n$$

where $\widetilde{\Gamma}$ denotes the prosolvable completion of Γ.

Proof: Obviously $d(\widetilde{\Gamma}) \leq d(\widehat{\Gamma}) \leq n$ holds, so it is enough to show that $d(\widetilde{\Gamma}) \geq n$. Just as before, we can assume that the G_i have prime order p_i $(1 \leq i \leq n)$. Let k be the product of the distinct primes in the sequence $p_1, p_2, \ldots, p_n$ and let p be a prime in the arithmetic progression $kn + 1$ $(n \in \mathbb{N})$ to be chosen later. Then the cyclic group C_k embeds into the multiplicative group $\mathbb{F}_p^*$. Let the target group be $H = \mathbb{F}_p C_k \leq \mathrm{Aff}(p)$. Since the target group is metabelian, the witness group

$$G(\Gamma, H) = \Gamma / K(\Gamma, H) = \Gamma / \bigcap_{\varphi \in \mathrm{Hom}(\Gamma, H)} \ker \varphi \hookrightarrow H^{|\mathrm{Hom}(\Gamma, H)|}$$

embeds into the product of metabelian groups thus it is metabelian itself. Using Lemma 8 and Lemma 7 for a large enough p we get $d(G(\Gamma, H)) \geq n$, finishing the proof. ∎

Now we prove Theorem 4. The background result needed is due to Erdős [Erd] and is purely number-theoretic.

Theorem 10 (Erdős): *Let A be an infinite set of positive integers and let*

$$f_n(A) = |A \cap \{1, \ldots, n\}|.$$

Assume that

1) *$f_n(A)$ increases faster than $n^{(\sqrt{5}-1)/2}$;*
2) *Every arithmetic progression contains at least one integer which is the sum of distinct elements of A.*

Then every sufficiently large integer is a sum of distinct elements of A.

We are ready to prove Theorem 4.

Proof of Theorem 4: Let $p_1, p_2, \ldots, p_n$ be the first n odd primes and let $D = p_1 p_2 \cdots p_n$. For $1 \leq i \leq n$ let $m_i \in \{1, \ldots, D\}$ be the (unique) solution of the congruence system

$$m_i \equiv \begin{cases} 1 (\operatorname{mod} p_j) & \text{if } i = j \\ 2 (\operatorname{mod} p_j) & \text{if } i \neq j \end{cases} \qquad 1 \leq j \leq n$$

and let S_i be the set of primes in the arithmetic progression

$$\{Dx + m_i \colon x \in \mathbb{N}\}.$$

Then the S_i $(1 \leq i \leq n)$ are pairwise disjoint.

We claim that S_i satisfies both assumptions in Theorem 10 $(1 \leq i \leq n)$. The first assumption follows from the asymptotic form of Dirichlet's theorem saying $f_n(S_i) = O(n/\log n)$. For the second assumption let a and r be positive integers; we shall check that the assumption holds for the arithmetic progression $\{ax + r \colon x \in \mathbb{N}\}$. Let $p_j^{o_j}$ be the maximal p_j-power dividing a $(1 \leq j \leq n)$, let

$$b = \prod_{j=1}^{n} p_j^{o_j}$$

and let $a' = a/b$ and let D' be the least common multiple of b and D. Then a' and D' are relatively prime, so there exists a solution m_i' to the congruence system

$$m_i' \equiv m_i (\operatorname{mod} D')$$
$$m_i' \equiv 1 (\operatorname{mod} a')$$

Since m_i' and $D'a'$ are relatively prime, using Dirichlet's theorem, the set

$$S_i' = \{x \in S_i \colon x \equiv m_i' (\operatorname{mod} D'a')\}$$

consists of infinitely many primes. Also there exists t with $m_i' t \equiv r \ (\operatorname{mod} D'a')$. Let $s_1, s_2, \ldots, s_t$ be distinct elements of $S_i' \subseteq S_i$. Then since a divides $D'a'$, we have

$$\sum_{j=1}^{t} s_j \equiv m_i' t \equiv r (\operatorname{mod} a)$$

provides the required sum in the second assumption. The claim holds.

Now Theorem 10 implies that there exists a natural number k that can be obtained as a sum of different elements of the S_i ($1 \le i \le n$). Let $q_{i,j} \in S_i$ ($1 \le i \le n$, $1 \le j \le l_i$) be different primes satisfying the decompositions

$$k = \sum_{j=1}^{l_i} q_{i,j}.$$

Let C_i denote the cyclic group of order p_i. Let $F_{i,j} = \mathbb{F}_{q_{i,j}}$, let

$$V_i = \bigoplus_{j=1}^{l_i} F_{i,j} \quad \text{and} \quad X_i = \bigcup_{j=1}^{l_i} F_{i,j}$$

Then p_i divides $q_{i,j} - 1$, so C_i embeds into the multiplicative group of $F_{i,j}$. Let G_i be the semidirect product of V_i and C_i acting diagonally on the components $F_{i,j}$. This action defines an embedding of G_i into $\mathrm{Sym}(X_i)$. Let $G_{i,j}$ denote the action of G_i on $F_{i,j}$. Then $G_{i,j}$ is permutation isomorphic to a subgroup of $\mathrm{Aff}(q_{i,j})$ properly containing $F_{i,j}$ and for $j \neq j'$ the permutation groups $G_{i,j}$ and $G_{i,j'}$ are not permutation isomorphic. Applying Lemma 8, the centralizer

$$C_{\mathrm{Sym}(X_i)}(G_i) = \bigoplus_{j=1}^{l_i} C_{\mathrm{Sym}(F_{i,j})}(G_{i,j}) = 1$$

is trivial. We showed that the G_i ($1 \le i \le n$) have a permutation action on k points with trivial centralizer in the full symmetric group $\mathrm{Sym}(k)$.

It is easy to see that $G_i' = V_i$ and so G_i/G_i' is cyclic. Trivially, G_i is solvable and non-cyclic, so $d(G_i) = 2$. Also

$$|G_i| = p_i \prod_{j=1}^{l_i} q_{i,j}$$

so for $i \neq i'$ the orders of G_i and $G_{i'}$ are relatively prime.

We estimate $d(\widehat{\Gamma})$ using Lemma 7 with $\mathrm{Sym}(k)$ as target group. We have seen that the G_i ($1 \le i \le n$) have an embedding into $\mathrm{Sym}(k)$ with trivial centralizer. Taking into account the trivial permutation representation, this gives

$$|\operatorname{Hom}(G_i, \mathrm{Sym}(k))| \ge |\mathrm{Sym}(k)| + 1,$$

which yields

$$d(\widehat{\Gamma}) \ge \sum_{i=1}^{n} h(G_i, \mathrm{Sym}(k)) \ge n \frac{\log(k! + 1)}{\log k!} > n.$$

The theorem holds. ∎

Remark: The upper estimate $d(\widehat{\Gamma}) \leq n + s - 1$ does not hold in general, even if we assume that all the G_i are perfect. Indeed, let the G_i $(1 \leq i \leq n)$ be isomorphic to A_5, the alternating group on 5 letters. Now $\mathrm{Hom}(A_5, A_5)$ consists of the set of automorphisms and the trivial homomorphism, so

$$h(A_5, A_5) = \frac{\log 121}{\log 60} \approx 1.1713$$

implying

$$d(\widehat{\Gamma}) \geq 1.1713n.$$

References

[Erd] P. Erdős, *On the representation of large integers as sums of distinct summands taken from a fixed set,* Acta Arithmetica **7** (1961/1962), 345–354.

[Gru] I. Gruschko, *Über die Basen eines freien Produktes von Gruppen (Russian. German summary),* Rec. Math. [Mat. Sbornik] N.S **8** (1940), 169–182.

[Kou] *The Kourovka Notebook,* Unsolved Problems in Group Theory (1978).

[KoS] L. G. Kovács and H.S. Sim, *Generating finite soluble groups,* Koninklijke Nederlandse Akademie van Wetenschappen. Indagationes Mathematicae. New Series **2** (1991), 229–232.

[Lu1] A. Lucchini, *On the number of generators of finite images of free products of finite groups,* Journal of Algebra **245** (2001), 552–561.

[Lu2] A. Lucchini, *On the minimal number of generators of free profinite products of profinite groups,* Journal of Group Theory **4** (2001), 53–58.

[Luc] W. Lück, *L_2-Invariants: Theory and Applications to Geometry and K-Theory,* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics 44. Springer-Verlag, Berlin, 2002.

[Neu] B. H. Neumann, *On the number of generators of a free product,* Journal of the London Mathematical Society **18** (1943), 12–20.

[Nos] G. A. Noskov, *The number of generators of a group,* Mathematical Notes **33** (1983), 249–254.

[RiW] L. Ribes and K. Wong, *On the minimal number of generators of certain groups,* in *Groups-St. Andrews 1989, vol. 2*, London Mathematical Society Lecture Note Ser. 160, Cambridge University Press, Cambridge, 1991, pp. 408–421.

[Wis] D. T. Wise, *A residually finite version of Rips's construction,* The Bulletin of the London Mathematical Society **35** (2003), 23–29.