Some questions arising from the study of the Product Replacement Algorithm

Andrea Lucchini

Università di Padova, Italy

Giornata dei Rendiconti
Padova, April 19, 2013

The product replacement algorithm (PRA) is a practical algorithm to construct random elements of a finite group.

The algorithm was designed by Leedham-Green and Soicher (1995) to generate efficiently nearly uniform group elements.

Let G be a k-generated finite group and let

$$\Phi_k(G) = \{(g_1, \ldots, g_k) \in G^k \mid \langle g_1, \ldots, g_k \rangle = G\}$$

be the set of all generating k-tuples of G.

Let G be a k-generated finite group and let

$$\Phi_k(G) = \{(g_1, \dots, g_k) \in G^k \mid \langle g_1, \dots, g_k \rangle = G\}$$

be the set of all generating k-tuples of G.

Given a generating k-tuple, a move to another such k-tuple is defined by first uniformly selecting a pair (i, j) with $1 \leq i \neq j \leq k$ and then applying one of the following operations with equal probability:

$$R_{i,j}^{\pm} : (g_1, \dots, g_i, \dots, g_k) \mapsto (g_1, \dots, g_i \cdot g_j^{\pm 1}, \dots, g_k),$$
$$L_{i,j}^{\pm} : (g_1, \dots, g_i, \dots, g_k) \mapsto (g_1, \dots, g_j^{\pm 1} \cdot g_i, \dots, g_k).$$

To produce a random element in G, start with some generating k-tuple, apply the above moves several times, and finally return a random element of the generating k-tuple that was reached.

The moves in the PRA can be conveniently encoded by the PRA graph $\Gamma_k(G)$ whose vertices are the tuples in $\Phi_k(G)$, with edges corresponding to the moves $R^{\pm}_{i,j}, L^{\pm}_{i,j}$.

If k is large enough, then the graph $\Gamma_k(G)$ is connected.

The algorithm consists of running a nearest neighbor random walk on this graph and returning a random component. We refer to this random walk as the product replacement random walk.

The moves in the PRA can be conveniently encoded by the PRA graph $\Gamma_k(G)$ whose vertices are the tuples in $\Phi_k(G)$, with edges corresponding to the moves $R^{\pm}_{i,j}, L^{\pm}_{i,j}$.

If k is large enough, then the graph $\Gamma_k(G)$ is connected.

The algorithm consists of running a nearest neighbor random walk on this graph and returning a random component. We refer to this random walk as the product replacement random walk.

A generating set X of G is said to be minimal if no proper subset of X generates G. We denote by $d(G)$ the minimal number of generators of G, i.e. the smallest size of a minimal generating set of G, and we write $m(G)$ for the largest size of a minimal generating set of G.

A generating set X of G is said to be minimal if no proper subset of X generates G. We denote by $d(G)$ the minimal number of generators of G, i.e. the smallest size of a minimal generating set of G, and we write $m(G)$ for the largest size of a minimal generating set of G.

Diaconis and Saloff-Coste (1998) proved that the random walk on $\Gamma_k(G)$ reaches an uniform distribution in time $|G|^{O(m(G))}k^2 \log k$. Thus an accurate bound for $m(G)$ would be desirable as a means of bounding the time for the algorithm.

Comparing $d(G)$ and $m(G)$

- (J. Whiston, 2000) If $G = \mathrm{Sym}(n)$ with $n \geq 3$, then $d(G) = 2$ and $m(G) = n - 1$.
- (J. Saxl and J. Whiston, 2002) If $G = \mathrm{PSL}(2, p)$ then $d(G) = 2$ and $3 \leq m(G) \leq 4$.
- (P. Apisa and B. Klopsch, 2012) If $d(G) = m(G)$, then $|G|$ is divisible by at most 2 different primes; more precisely one of the following hold:
  1. G is a p-group;
  2. $G = P \rtimes Q$, where P is a p-group and Q is a cyclic q-group for distinct primes $p \neq q$.

Take a chief series $1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$.

$$d(G) = \sum_{1 \le i \le t} d_i, \quad m(G) = \sum_{1 \le i \le t} m_i,$$

with $d_i = d(G/G_i) - d(G/G_{i-1}), m_i = m(G/G_i) - m(G/G_{i-1})$.

Take a chief series $1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$.

$$d(G) = \sum_{1 \le i \le t} d_i, \quad m(G) = \sum_{1 \le i \le t} m_i,$$

with $d_i = d(G/G_i) - d(G/G_{i-1}), m_i = m(G/G_i) - m(G/G_{i-1})$.

	G_0	
$d(G/G_1)$		$m(G/G_1)$
	G_1	
$d(G/G_2) - d(G/G_1)$		$m(G/G_2) - m(G/G_1)$
	G_2	
	$\vdots$	
	G_{i-1}	
$d(G/G_i) - d(G/G_{i-1})$		$m(G/G_i) - m(G/G_{i-1})$
	G_i	
	$\vdots$	
	G_{t-1}	
$d(G/G_t) - d(G/G_{t-1})$		$m(G/G_t) - m(G/G_{t-1})$
	G_t	

- $d_1 = 1$ if G/G_1 is abelian, $d_1 = 2$ otherwise.
- If $i > 1$, then $d_i \leq 1$ (AL 1995).
- If $i > 1$, then $d_i = 1$ only if $d(G/G_{i-1})$ is “small” and “many” of the factors G_{j-1}/G_j with $j < i$ are "equivalent" to G_{i-1}/G_i (Detomi, AL 2003).
- $d_i = 0$ if G_{i-1} is contained in every maximal subgroup of G containing G_i (i.e. G_{i-1}/G_i is a Frattini chief factor of G).

- $d_1 = 1$ if G/G_1 is abelian, $d_1 = 2$ otherwise.
- If $i > 1$, then $d_i \leq 1$ (AL 1995).
- If $i > 1$, then $d_i = 1$ only if $d(G/G_{i-1})$ is “small” and “many” of the factors G_{j-1}/G_j with $j < i$ are "equivalent" to G_{i-1}/G_i (Detomi, AL 2003).
- $d_i = 0$ if G_{i-1} is contained in every maximal subgroup of G containing G_i (i.e. G_{i-1}/G_i is a Frattini chief factor of G).

- $m_1 = 1$ if G/G_1 is abelian, $m_1 \geq 3$ otherwise.
- $m_i = 0$ iff G_{i-1}/G_i is a Frattini chief factor of G (AL 2013).
- If G_{i-1}/G_i is a non Frattini chief factor, then $m_i = 1$ if and only if G_{i-1}/G_i is abelian (AL 2013).
- m_i depends only on the structure of G_{i-1}/G_i as a G-group, but not on its “multiplicity”(AL 2013).

- $d_1 = 1$ if G/G_1 is abelian, $d_1 = 2$ otherwise.
- If $i > 1$, then $d_i \leq 1$ (AL 1995).
- If $i > 1$, then $d_i = 1$ only if $d(G/G_{i-1})$ is “small” and “many” of the factors G_{j-1}/G_j with $j < i$ are "equivalent" to G_{i-1}/G_i (Detomi, AL 2003).
- $d_i = 0$ if G_{i-1} is contained in every maximal subgroup of G containing G_i (i.e. G_{i-1}/G_i is a Frattini chief factor of G).

- $m_1 = 1$ if G/G_1 is abelian, $m_1 \geq 3$ otherwise.
- $m_i = 0$ iff G_{i-1}/G_i is a Frattini chief factor of G (AL 2013).
- If G_{i-1}/G_i is a non Frattini chief factor, then $m_i = 1$ if and only if G_{i-1}/G_i is abelian (AL 2013).
- m_i depends only on the structure of G_{i-1}/G_i as a G-group, but not on its “multiplicity”(AL 2013).

COROLLARY

$$m(G_1 \times G_2) = m(G_1) + m(G_2).$$

If G is a finite soluble group, then G_{i-1}/G_i is a G-module.
For any irreducible G-module A let

- $\phi_G(A) = \dim_{\mathrm{End}_G(A)} A$,
- $\zeta_G(A) = 1$ if A is a nontrivial G-module, $\zeta_G(A) = 0$ otherwise,
- $\delta_G(A)$ the number of the non-Frattini factors G-isomorphic to A in an arbitrary chief series of G.

$$d(G) = \max_A \left(\left[\frac{\delta_G(A) - 1}{\phi_G(A)} \right] + 1 + \zeta_G(A) \right), m(G) = \sum_A \delta_G(A)$$

where A ranges over the set of non isomorphic complemented chief factors of G.

Bias

Question

Is there bias in the output of the PRA algorithm? Are all group elements equally represented in generating k-tuples?

Let U denote the uniform distribution over G. The bias of the distribution P is the variation distance between P and U:

$$\|P - U\|_{tv} = \max_{B \subseteq G} |P(B) - U(B)| = \frac{1}{2} \sum_{g \in G} \left| P(g) - \frac{1}{|G|} \right|.$$

Even if the graph $\Gamma_k(G)$ is connected, even if the product replacement random walk mixes rapidly, the resulting distribution of the output can still be biased.

Even if the graph $\Gamma_k(G)$ is connected, even if the product replacement random walk mixes rapidly, the resulting distribution of the output can still be biased.

Let Q^k denote the probability distribution on G of the first component of k-uples chosen uniformly from $\Phi_k(G)$.

Babai and Pak, 2000

Let $G = \mathrm{Alt}(n)^m$ where $m = n!/8$. It can be proved that $d(G) = 2$ if n is sufficiently large. On the other hand

$$\|Q^k - U\|_{tv} \to 1 \text{ as } n \to \infty$$

assuming $k \geq 4$ and $k = o(n)$.

Even if the graph $\Gamma_k(G)$ is connected, even if the product replacement random walk mixes rapidly, the resulting distribution of the output can still be biased.

Let Q^k denote the probability distribution on G of the first component of k-uples chosen uniformly from $\Phi_k(G)$.

BABAI AND PAK, 2000

Let $G = \mathrm{Alt}(n)^m$ where $m = n!/8$. It can be proved that $d(G) = 2$ if n is sufficiently large. On the other hand

$$\|Q^k - U\|_{tv} \to 1 \text{ as } n \to \infty$$

assuming $k \geq 4$ and $k = o(n)$.

However, for each k-generated finite group G,

$$\|Q^k - U\|_{tv} \leq 1 - \mathrm{Prob}_G(k)$$

where $\mathrm{Prob}_G(k) = \frac{|\Phi_G(k)|}{|G|^k}$ is the probability of generating G with k elements.

To avoid strong bias we should choose k so that $\text{Prob}_G(k)$ is large enough.

A conjecture of I. Pak

Given a real number $0 < \alpha < 1$ there exists an absolute constant β_α such that $\text{Prob}_G(k) \geq \alpha$ for any finite group G and any integer $k \geq \beta_\alpha d(G) \log\log|G|$.

Theorem (E. Detomi and al, 2003)

Given a real number $0 < \alpha < 1$, there exists a constant c_α such that for any finite group G

$$\text{Prob}_G([d(G) + c_\alpha(1 + \log \lambda(G)]) \geq \alpha,$$

where $\lambda(G)$ denotes the number of non-Frattini factors in a chief series of G.

Methods of the proof

- Philip Hall observed that the probability of generating a given finite group G by a random k-tuple of elements is given by

$$P_G(k) = \sum_n \frac{a_n}{n^k} \text{ where } a_n = \sum_{|G:H|=n} \mu_G(H).$$

Here μ_G is the Möbius function of the subgroup-lattice of G.

Methods of the proof

- Philip Hall observed that the probability of generating a given finite group G by a random k-tuple of elements is given by

$$P_G(k) = \sum_n \frac{a_n}{n^k} \text{ where } a_n = \sum_{|G:H|=n} \mu_G(H).$$

  Here μ_G is the Möbius function of the subgroup-lattice of G.

- If N is a normal subgroup of G, then $P_G(k) = P_{G/N}(k)P_{G,N}(k)$ with $P_{G,N}(k) = \sum \frac{b_n}{n^k}$ and $b_n = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H)$

Methods of the proof

- Philip Hall observed that the probability of generating a given finite group G by a random k-tuple of elements is given by

$$P_G(k) = \sum_n \frac{a_n}{n^k} \text{ where } a_n = \sum_{|G:H|=n} \mu_G(H).$$

Here μ_G is the Möbius function of the subgroup-lattice of G.

- If N is a normal subgroup of G, then $P_G(k) = P_{G/N}(k) P_{G,N}(k)$ with $P_{G,N}(k) = \sum \frac{b_n}{n^k}$ and $b_n = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H)$
- In particular, given a chief series $1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$, we have that $P_G(k) = \prod_i P_{G/G_{i+1}, G_i/G_{i+1}}(k)$

Methods of the proof

- Philip Hall observed that the probability of generating a given finite group G by a random k-tuple of elements is given by

$$P_G(k) = \sum_n \frac{a_n}{n^k} \text{ where } a_n = \sum_{|G:H|=n} \mu_G(H).$$

  Here μ_G is the Möbius function of the subgroup-lattice of G.

- If N is a normal subgroup of G, then $P_G(k) = P_{G/N}(k)P_{G,N}(k)$ with $P_{G,N}(k) = \sum \frac{b_n}{n^k}$ and $b_n = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H)$

- In particular, given a chief series $1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$, we have that $P_G(k) = \prod_i P_{G/G_{i+1},G_i/G_{i+1}}(k)$

- $P_{G/G_{i+1},G_i/G_{i+1}}(k)$ can be estimated using results on the probabilistic generation of finite simple groups.

Connectivity of the PRA graph

Question

For a given G and $k \geq d(G)$, is $\Gamma_k(G)$ connected?

It is quite embarrassing how little is known about this problem. For example, we do not know the answer to the following innocent looking question: is it true that if $\Gamma_k(G)$ is connected, then $\Gamma_m(G)$ is connected for every $m > k$?

It is usually more convenient to look at the extended PRA graph $\Gamma_k^*(G)$, which is obtained from $\Gamma_k(G)$, by adding edges corresponding to the moves:

$$P_{i,j} : (g_1, \dots, g_i, \dots, g_j, \dots, g_k) \mapsto (g_1, \dots, g_j, \dots, g_i, \dots, g_k)$$
$$I_i : (g_1, \dots, g_i, \dots, g_k) \mapsto (g_1, \dots, g_i^{-1}, \dots, g_k).$$

It is usually more convenient to look at the extended PRA graph $\Gamma_k^*(G)$, which is obtained from $\Gamma_k(G)$, by adding edges corresponding to the moves:

$$P_{i,j} : (g_1, \ldots, g_i, \ldots, g_j, \ldots, g_k) \mapsto (g_1, \ldots, g_j, \ldots, g_i, \ldots, g_k)$$

$$I_i : (g_1, \ldots, g_i, \ldots, g_k) \mapsto (g_1, \ldots, g_i^{-1}, \ldots, g_k).$$

Proposition

If $\Gamma_k^*(G)$ is connected and $k \geq d(G) + 1$, then $\Gamma_k(G)$ is also connected.

THEOREM

If $k \geq d(G) + m(G)$, then $\Gamma_k^*(G)$, and consequently $\Gamma_k(G)$, is connected.

PROOF.

Let $d = d(G)$. There exist $h_1, \ldots, h_d$ with $G = \langle h_1, \ldots, h_d \rangle$.

$(h_1, \ldots, h_d, 1, \ldots, 1)$ is connected to $(h_1, \ldots, h_d, x_{d+1}, \ldots, x_k)$ in $\Gamma_k(G)$, for every $x_{d+1}, \ldots, x_k \in G$.

Let $(g_1, \ldots, g_k) \in \Gamma_k(G)$: since $k - d \geq m$, up to permutation we have $G = \langle g_{d+1}, \ldots, g_k \rangle$.

It follows that $(g_1, \ldots, g_k)$ is connected to $(h_1, \ldots, h_d, g_{d+1}, \ldots, g_k)$ and $(h_1, \ldots, h_d, g_{d+1}, \ldots, g_k)$ is connected to $(h_1, \ldots, h_d, 1, \ldots, 1)$. $\square$

Conjecture

If $k \geq d(G) + 1$, then $\Gamma_k^*(G)$ is connected.

CONJECTURE

If $k \geq d(G) + 1$, then $\Gamma^*_k(G)$ is connected.

Dunwoody in 1963 proved that $\Gamma_{d(G)+1}(G)$ is connected for any finite soluble group G. However there are examples of finite soluble groups G for which the graph $\Gamma^*_{d(G)}(G)$ is not connected.

Conjecture

If $k \geq d(G)+1$, then $\Gamma_k^*(G)$ is connected.

Dunwoody in 1963 proved that $\Gamma_{d(G)+1}(G)$ is connected for any finite soluble group G. However there are examples of finite soluble groups G for which the graph $\Gamma_{d(G)}^*(G)$ is not connected.

$\Gamma_k^*(G)$ is connected in the following cases:

- $G = PSL(2,p)$, where $p \geq 5$ is prime and $k \geq 3$ is a prime.
- $G = PSL(2,2^m)$, where $m \geq 2$ and $k \geq 3$.
- $G = PSL(2,q)$, where $q = p^e$ is an odd prime power and $k \geq 4$.
- $G = Sz(2^{2m+1})$, where $m \geq 2$ and $k \geq 3$.
- $G = \mathrm{Alt}(n)$, where $6 \leq n \leq 11$ and $k = 3$.

Conjecture

If $k \geq d(G) + 1$, then $\Gamma_k^*(G)$ is connected.

Dunwoody in 1963 proved that $\Gamma_{d(G)+1}(G)$ is connected for any finite soluble group G. However there are examples of finite soluble groups G for which the graph $\Gamma_{d(G)}^*(G)$ is not connected.

$\Gamma_k^*(G)$ is connected in the following cases:

- $G = PSL(2, p)$, where $p \geq 5$ is prime and $k \geq 3$ is a prime.
- $G = PSL(2, 2^m)$, where $m \geq 2$ and $k \geq 3$.
- $G = PSL(2, q)$, where $q = p^e$ is an odd prime power and $k \geq 4$.
- $G = Sz(2^{2m+1})$, where $m \geq 2$ and $k \geq 3$.
- $G = \mathrm{Alt}(n)$, where $6 \leq n \leq 11$ and $k = 3$.

N. Avni and S. Garion, 2008

There is a function $c(r)$ such that for any finite simple group of Lie type, with Lie rank r, the graph $\Gamma_k^*(G)$ is connected for any $k \geq c(r)$.

T_k-SYSTEMS

- F_k=the free group on k-generators, with $k \geq d(G)$.
- $\Phi_k(G)$ can be identified with the set $\mathrm{Epi}(F_k \to G)$.
- $\mathrm{Aut}(F_k) \times \mathrm{Aut}(G)$ acts on $\Phi_k(G)$:

$$(\tau, \sigma) : \phi \to \sigma \circ \phi \circ \tau^{-1}$$

  where $\tau \in \mathrm{Aut}(F_k), \sigma \in \mathrm{Aut}(G), \phi \in \mathrm{Epi}(F_k \to G)$.
- The orbits are called T_k-systems.

T_k-SYSTEMS

- F_k=the free group on k-generators, with $k \geq d(G)$.
- $\Phi_k(G)$ can be identified with the set $\mathrm{Epi}(F_k \to G)$.
- $\mathrm{Aut}(F_k) \times \mathrm{Aut}(G)$ acts on $\Phi_k(G)$:

$$(\tau, \sigma) : \phi \to \sigma \circ \phi \circ \tau^{-1}$$

  where $\tau \in \mathrm{Aut}(F_k), \sigma \in \mathrm{Aut}(G), \phi \in \mathrm{Epi}(F_k \to G)$.
- The orbits are called T_k-systems.

If $k \geq 2 \cdot d(G)$ then $\Gamma_k(G)$ and $\Gamma_k^*(G)$ are connected if and only if G has only one T_k-system.

An interesting question is to estimate the number of T_k-systems of G as a function of k and G.

- a k-generated abelian group has only one T_k-system.
- A first example of a nilpotent group G with more than one T_k-system where $k = d(G)$, was given by B.H. Neumann (1955)
- Dunwoody proved that the number of T_k-systems of certain groups is in fact not bounded; i.e. for every k, m and p, one can find a p-group G with $d(G) = k$ such that the number of T_k-systems of G is at least m.

Particular attention was given to T-systems in finite simple groups G. Here $d(G) = 2$ and a conjecture attributed to Wiegold states that for $k \geq 3$ the number of T_k-systems of G is 1. This conjecture was proved for very few families of simple groups. However, the case $k = 2$ seems to be different.

Particular attention was given to T-systems in finite simple groups G. Here $d(G) = 2$ and a conjecture attributed to Wiegold states that for $k \geq 3$ the number of T_k-systems of G is 1. This conjecture was proved for very few families of simple groups. However, the case $k = 2$ seems to be different.

Theorem (S. Garion and A. Shalev, 2009)

Let G be a finite simple group. Then the number of T_2-systems of G tends to infinity as $|G| \to \infty$.

Corollary

Let G be a finite simple group. Then the number of connected components of the PRA graph $\Gamma_2(G)$ tends to infinity as $|G| \to \infty$.

It seems interesting to investigate whether the connectivity is ensured for other graphs obtained by adding further edges to $\Gamma_k(G)$.

For example one can consider a new graph $\Delta_k(G)$ obtained by allowing the "swap moves":

$$(g_1, \dots, g_i, \dots, g_k) \mapsto (g_1, \dots, g_i', \dots, g_k).$$

In other words $(x_1, \dots, x_k), (y_1, \dots, y_k) \in \Phi_k(G)$ are adjacent in the swap graph $\Delta_k(G)$ if and only if they differ only by one entry.

The swap conjecture

The conjecture that $\Delta_k(G)$ is connected if $k \geq d(G)$ (swap conjecture) was proposed by Tennant and Turner in 1992.

THE SWAP CONJECTURE

The conjecture that $\Delta_k(G)$ is connected if $k \geq d(G)$ (swap conjecture) was proposed by Tennant and Turner in 1992.

Tennant and Turner proved that their conjecture holds for various classes of groups: free groups of finite rank, free abelian groups of finite rank, Fuchsian groups, surface groups, finitely-generated abelian groups, certain 1-relator groups, and others.

In 1995 V. A. Roman'kov proved that the free metabelian group of rank 3 does not satisfy this conjecture but no counterexample is known in the class of finite groups.

THEOREM (E. CRESTANI AND AL, 2012)

Let G be an arbitrary finite group. If $k \geq d(G) + 1$, then the swap graph $\Delta_k(G)$ is connected.

THEOREM (E. CRESTANI AND AL, 2012)

Let G be an arbitrary finite group. If $k \geq d(G) + 1$, then the swap graph $\Delta_k(G)$ is connected.

A crucial ingredient in the proof is the following consequence of the Classification of the Finite Simple Groups, proved in 2000 by R.M. Guralnick and W.M. Kantor: let S be a finite non abelian simple group; for each $1 \neq h \in \mathrm{Aut}(S)$ there exists $s \in \mathrm{Inn}(S)$ such that $\mathrm{Inn}(S) \leq \langle s, h \rangle$.

The case when $k = d(G)$ is much more difficult. In 2012 we proved that the 2-generated finite soluble groups satisfy the swap conjecture.

THEOREM (E. CRESTANI AND AL, 2012)

If G is a 2-generated soluble group, then $\Delta_2(G)$ is connected.

The case when $k = d(G)$ is much more difficult. In 2012 we proved that the 2-generated finite soluble groups satisfy the swap conjecture.

THEOREM (E. CRESTANI AND AL, 2012)

If G is a 2-generated soluble group, then $\Delta_2(G)$ is connected.

We generalized the previous theorem proving a weaker version of the swap conjecture for arbitrary finite soluble groups.

Consider the graph $\Delta_k^*(G)$ whose vertices are the generating k-tuples and in which two vertices $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ are adjacent if and only if there exists $i \in \{1, \ldots, k\}$ such that $x_i = y_i$.

Consider the graph $\Delta_k^*(G)$ whose vertices are the generating k-tuples and in which two vertices $(x_1, \dots, x_k)$ and $(y_1, \dots, y_k)$ are adjacent if and only if there exists $i \in \{1, \dots, k\}$ such that $x_i = y_i$.

We prove that if $k \geq 2$ and G is a k-generated soluble group, then $\Delta_k^*(G)$ is connected.

Actually we prove a slightly stronger result, considering a graph with fewer edges, namely the graph $\Lambda_k(G)$ in which the vertices are the generating k-tuples and in which two vertices $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ are adjacent if and only if there exists $I \subseteq \{1, \ldots, k\}$ such that $|I| \geq [k/2]$ and $x_i = y_i$ for each $i \in I$.

Actually we prove a slightly stronger result, considering a graph with fewer edges, namely the graph $\Lambda_k(G)$ in which the vertices are the generating k-tuples and in which two vertices $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ are adjacent if and only if there exists $I \subseteq \{1, \ldots, k\}$ such that $|I| \geq [k/2]$ and $x_i = y_i$ for each $i \in I$.

THEOREM

Let G be a k-generated finite soluble group, with $k \geq 2$. The graph $\Lambda_k(G)$ is connected.

A problem in linear algebra plays a crucial role in our proof of the previous theorem.

$M_{r\times s}(F)$: $r \times s$ matrices with coefficients over the field F.
a, b, c, d positive integers with $a+b=c+d$ and $a \le \min\{c,d\}$
Consider $A \in M_{a\times c}(F)$, $B \in M_{a\times d}(F)$, with rank $\begin{pmatrix} A & B \end{pmatrix} = a$.

$$\Omega_A := \left\{ C \in M_{b\times c}(F) \mid \text{rank} \begin{pmatrix} A \\ C \end{pmatrix} = c \right\}$$

$$\Omega_B := \left\{ D \in M_{b\times d}(F) \mid \text{rank} \begin{pmatrix} B \\ D \end{pmatrix} = d \right\}$$

We define a bipartite graph $\Gamma = \Gamma(A, B)$ in the following way:

1. the set of vertices of Γ is the disjoint union $\Omega_A \sqcup \Omega_B$;
2. $C \in \Omega_A$ and $D \in \Omega_B$ are adiacent iff $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} \neq 0$.

PROPOSITION

If either $a > 1$ or $a = 1$ and $|F| > 2$, then Γ is connected.