Generating subgroups and an addendum proving subgroups of free groups are free: Lecture 3

Gilbert Baumslag

October 1, 2008

1 Quantum computing and factorization

Marianna Papaleo gave a short lecture on quantum computing and discussed Shor's theorem on the computation of the period of a periodic function. This had applications, in particular, to the problem of factoring large numbers. She also noted that the quantum computer at IBM factored 15.

2 Subgroups of free groups are free

2.1 Coset representatives and subgroup generation

It turns out that there is simple way of finding a set of generators of a subgroup of a group given with a set of generators. We will need the following definition.

Definition 2.1 *Let G be a group, $H \leq G$. Then a complete set of representatives of the right cosets Hg of H in G is a set R consisting of one element from each coset. The element in R coming from the coset Hg is denoted by $\overline{g}$ and is termed the representative of Hg or sometimes the representative of g. If $1 \in R$, R is termed a right transversal of H in G.*

The "difference" between $r \in R$ and $\overline{rx}$, where $x \in X$ is denoted by $\delta(r, x)$ and is defined as follows:

$$\delta(r, x) = \ rx\,(\overline{rx})^{-1} \quad (r \in R, x \in X).$$

The proof of the following lemma is routine.

Lemma 2.2 *1.* $Hg \ = \ H\overline{g}$ $(g \in G)$.

2. $\delta(g,x) \ \in \ H$.

3. $\overline{\overline{g_1}g_2} \ = \ \overline{g_1 g_2}$ $(g_1, g_2 \in G)$.

4. $g \ = \ \delta(g,1)\overline{g}$ $(g \ \in \ G)$

The following observation plays a key role in the way in which O. Schreier proved that subgroups of free groups are free.

Theorem 2.3 *Let G be a group generated by a set X, let $H \leq G$ and let R be a right transversal of H in G. Then*

$$H \ = \ gp\big(\ \delta(r,x) \ = \ rx(\overline{rx})^{-1} \ \big| \ r \in R \,, \, x \in X \ \big) \ .$$

In order to prove this theorem, we begin by defining a homomorphism ρ of G into the group of permutations of the set $H \times R$ as follows:

$$(h,r)(g\rho) = \big(\ h\delta(r,g) \,, \, \overline{rg} \ \big) \ .$$

The claim that ϱ is a homomorphism is nothing more than the observation due to Cayley that every group G has a faithful representation as a group of permutations of the set G. Then we trace out for each $h \in H$ the effect of $h\varrho$ on $(1,1) \in H \times R$. First notice that

$$(h,r)(g\varrho) \ = \ \big(\ h\delta(r,g) \,, \, \overline{rg} \ \big) \ .$$

So if $h \in H$

$$(1,1)(h\varrho) \ = \ \big(\ \delta(1,h) \,, \, \overline{h} \ \big) \ = \ (h,1) \ .$$

Now express h in X-product form

$$h \ = \ {x_1}^{\varepsilon_1} \ldots {x_n}^{\varepsilon_n} \qquad (x_i \in X \,, \, \varepsilon_i = \pm 1) \ .$$

Then

$$\begin{aligned} (1,1)(h\varrho) \ &= \ (1,1)({x_1}^{\varepsilon_1}\varrho) \ldots ({x_n}^{\varepsilon_n}\varrho) \\ &= \big(\ \delta(r_1, {x_1}^{\varepsilon_1}) \ldots \delta(r_n, {x_n}^{\varepsilon_n}) \,, 1 \big) \end{aligned}$$

where the r_i are the elements of R that arise from this computation. This proves that

$$h \ = \ \delta(r_1, {x_1}^{\varepsilon_1}) \ldots \delta(r_n, {x_n}^{\varepsilon_n}) \ .$$

Hence

$$H \ = \ gp\big(\ \delta(r, x^{\pm 1}) \ \big| \ r \in R \,, \, x \in X \ \big) \ .$$

But

$$rx^{-1}\left(\overline{rx^{-1}}\right)^{-1} = \left(\overline{rx^{-1}}x\left(\overline{\overline{rx^{-1}}x}\right)^{-1}\right)^{-1}.$$

This completes the proof of Theorem 2.3.

One of the immediate consequences of Theorem 2.3 is the following

Corollary 2.4 *A subgroup of finite index in a finitely generated group is finitely generated.*

3 Subgroups of free groups

Now suppose that F is a free group, freely generated by the set X. It follows that if $f \in F$, then f can be expressed as a reduced X-product

$$f = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$$

in exactly one way. We term this reduced X-product the *normal form* of f, and define the *length* of f, denoted by $\ell(f)$, to be n:

$$\ell(f) = n .$$

If $f, g \in F$ and if

$$\ell(fg) = \ell(f) + \ell(g)$$

we write

$$f \vartriangle g$$

to express the fact that no cancellation takes place on forming the product fg i.e. the reduced X-product for fg is obtained by concatenating the reduced X-product for g with the reduced X-product for f. If

$$\ell(fg) < \ell(f) + \ell(g)$$

we sometimes write

$$f \sqcup g$$

expressing the fact that the last letter of f cancels the first letter of g.

Now let F be a free group freely generated by some set X, $H \leq F$ and S a right transversal of H in F. We term S a Schreier transversal if

$$x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in S \qquad implies \qquad x_1^{\epsilon_1} \dots x_{n-1}^{\epsilon_{n-1}} \in S$$

i.e. every "initial segment" of a representative is again a representative.

The proof then of Schreier's subgroup theorem goes as follows:

1. There always exist Schreier transversals.
2. If S is a Schreier transversal then H is free on

$$Y \;=\; \{\, \delta(s,x) \;=\; sx(\overline{sx})^{-1} \;\neq\; 1 \;\big|\; s \in S,\, x \in X \,\}\ .$$

We already know that Y generates H. It remains to check that Y freely generates H.

Proof. The scheme of the proof is very simple.

1. If $\delta(s,x) \neq 1$, then we prove

$$\delta(s,x) \;=\; s_\triangle x_\triangle (\overline{sx})^{-1}$$

and so

$$\big(\delta(s,x)\big)^{-1} \;=\; \overline{sx}_\triangle x^{-1}{}_\triangle s^{-1}\ .$$

2. If $\delta(s,x) \neq 1$, then

$$\delta(s,x) \;=\; \delta(t,y) \qquad only\ if \qquad s \;=\; t \qquad and \qquad x \;=\; y\ .$$

3. If

$$\pi \;=\; \delta(s_1,x_1)^{\varepsilon_1} \ldots \delta(s_n,x_n)^{\varepsilon_n}$$

is a reduced Y-product in the symbols $\delta(s,x)$ (which by (ii) are distinct elements if the symbols are distinct) then on expanding we find

$$\pi \;=\; \bullet_\triangle {x_1}^{\varepsilon_1}{}_\triangle \bullet \ldots \bullet_\triangle\, {x_n}^{\varepsilon_n}{}_\triangle \bullet$$

i.e., the x and x^{-1} in the middle of $\delta(s,x)$ and $\big(\delta(s,x)\big)^{-1}$ respectively never cancel on computing the reduced X-product form of π.

The proof goes as follows:

1. Suppose $s_\sqcup x$. Then

$$s \;=\; t_\triangle x^{-1}$$

and since S is a Schreier transversal $t \in S$ i.e. $\bar{t} = t$. Now

$$sx\,\left(\overline{sx}\right)^{-1} \;=\; tx^{-1}x\left(\overline{tx^{-1}x}\right)^{-1} \;=\; t\,t^{-1} \;=\; 1\ .$$

Similarly if $x_\sqcup\big(\overline{sx}\big)^{-1}$ (or equivalently $\overline{sx}_\sqcup x^{-1}$ – note here $\overline{\overline{sx}\,x^{-1}} \;=\; s$).

2. By (1) $s_\triangle x_\triangle \big(\overline{sx}\big)^{-1} \;=\; t_\triangle y_\triangle \big(\overline{ty}\big)^{-1}$. If $l(s) = l(t)$, $s = t$, $x = y$ and we are home. If $l(s) < l(t)$, sx is an initial segment of t. So $\overline{sx} = sx$ and therefore $sx\big(\overline{sx}\big)^{-1} = 1$!

3. Note that on computing any of the reduced Y-products

$$\big(\delta(s,x)\big)^{\pm 1}\big(\delta(t,y)\big)^{\pm 1}$$

we get the four possibilities

$$\ldots \triangle\; x \;\triangle\; \ldots \;\triangle\; y \;\triangle\; \ldots$$

$$\ldots \triangle\; x \;\triangle\; \ldots\triangle y^{-1}{}_\triangle\; \ldots$$

$$\ldots \;{}_\triangle x^{-1}{}_\triangle \ldots \;\triangle\; y \;\triangle\; \ldots$$

$$\ldots \;{}_\triangle x^{-1}{}_\triangle \ldots\triangle y^{-1}{}_\triangle \ldots$$

This establishes the form of π. The rest of the proof follows along the same lines.

Finally we need the following lemma.

Lemma 3.1 *Let F be a free group on the set X, $H \leq F$. Then there exists a Schreier transversal S of H in F.*

Define the length $\ell(Hf)$ of the right coset Hf of H in F by

$$\ell(Hf) \;=\; \min\{\, l(hf) \;\big|\; h \in H \,\}\,.$$

We choose the elements of S in stages. First choose $1 \in S$. Now we proceed by induction. Suppose representatives have been chosen for all cosets of length at most n in such a way that an initial segment of a representative is again a representative. For the right cosets of length $n+1$ suppose that

$$\ell(Hf) \;=\; n+1\ .$$

So there exists in Hf an element

$$b_1 \ldots b_{n+1}$$

of length $n+1$. Consider the coset

$$Hb_1 \ldots b_n.$$

Then

$$\ell(Hb_1 \ldots b_n) \;\leq\; n$$

so has a representative already, say

$$a_1 \ldots a_m \ (m \leq n) \ .$$

Consider

$$a_1 \ldots a_m b_{n+1} \ .$$

Notice

$$Ha_1 \ldots a_m b_{n+1} \ = \ Hb_1 \ldots b_n b_{n+1} \ .$$

So

$$l(a_1 \ldots a_m b_{n+1}) \ = \ n+1$$

i.e., $m = n$ and in particular

$$a_1 \ldots a_n \triangle \ b_{n+1} \ .$$

We take

$$a_1 \ldots a_n b_{n+1}$$

to be the representative of Hf. It is clear that every initial segment of $a_1 \ldots a_n b_{n+1}$ is again a representative, as desired.

To sum up then, suppose the group F is free on the set X, $H \leq F$. If we choose a right transversal S of H in F closed under initial segments, i.e. a Schreier transversal, then H is freely generated by

$$Y \ = \ \{ \ \delta(s,x) \ = \ sx(\overline{sx})^{-1} \ \neq \ 1 \ \big| \ s \in S \, , \ x \in X \ \} \ .$$