Bases and Strong Generating Sets

Daniel Rogers

June 13, 2014

Motivating Question

Given (finite) groups $G = \langle X \rangle \leq H$ and $h \in H$, how can we decide algorithmically whether $h \in G$?
Algorithms which solve this problem and, if they are successful, write h as a word in X, the generators of G, are known as constructive membership tests.

Bases

Let G be a group acting on a set Ω.

Bases

Let G be a group acting on a set Ω.

Definition

A base for G is a sequence $B = [b_1, ..., b_m] \subset \Omega$ such that the only element of G which stabilizes each b_i is the identity.

Strong Generating Sets

Let G be a group acting on a set Ω and $B = [b_1, ..., b_m] \subset \Omega$ a base.

Definition

The basic stabilizer chain associated with a base B is a chain of pointwise stabilizers of the form

$$G = G^{(0)} \geq G^{(1)} \geq ... \geq G^{(m)} = 1$$

where $G := G^{(0)}$ and $G^{(i)} := G_{(b_1,...b_i)}$ is the group of all elements of G which stabilize the first i base points.

Strong Generating Sets

Let G be a group acting on a set Ω and $B = [b_1, ..., b_m] \subset \Omega$ a base.

Definition

The basic stabilizer chain associated with a base B is a chain of pointwise stabilizers of the form

$$G = G^{(0)} \geq G^{(1)} \geq ... \geq G^{(m)} = 1$$

where $G := G^{(0)}$ and $G^{(i)} := G_{(b_1,...b_i)}$ is the group of all elements of G which stabilize the first i base points.

Definition

A strong generating set for G is a subset $S \subset G$ such that S contains generators for each of the groups $G^{(i)}$ for $0 \leq i \leq m$.

Strong Generating Sets

Let G be a group acting on a set Ω and $B = [b_1, ..., b_m] \subset \Omega$ a base.

Definition

The basic stabilizer chain associated with a base B is a chain of pointwise stabilizers of the form

$$G = G^{(0)} \geq G^{(1)} \geq ... \geq G^{(m)} = 1$$

where $G := G^{(0)}$ and $G^{(i)} := G_{(b_1,...b_i)}$ is the group of all elements of G which stabilize the first i base points.

Definition

A strong generating set for G is a subset $S \subset G$ such that S contains generators for each of the groups $G^{(i)}$ for $0 \leq i \leq m$.

Definition

A BSGS is a pair (B, S) of a base and a strong generating set.

Constructive Membership Testing

We return to the motivating question: suppose we have groups $G \leq H$ (both acting on the same set Ω) and $h \in H$, and suppose additionally that $B = [b_1, ..., b_m]$ and S are a BSGS for G (so in particular $G = \langle S \rangle$). We describe a simple method for performing constructive membership testing in this case.

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i - 1$ base points.

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i - 1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i-1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.
- Determine whether $\alpha \in b_i^{G^{(i-1)}}$ (in other words, whether there is an element of G which stabilizes the first $i-1$ base points and also maps b_i to α).

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i-1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.
- Determine whether $\alpha \in b_i^{G^{(i-1)}}$ (in other words, whether there is an element of G which stabilizes the first $i-1$ base points and also maps b_i to α).
  - If $\alpha \notin b_i^{G^{(i-1)}}$, then $t_{i-1} \notin G^{(i-1)}$, and so $h \notin G$.

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i-1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.
- Determine whether $\alpha \in b_i^{G^{(i-1)}}$ (in other words, whether there is an element of G which stabilizes the first $i-1$ base points and also maps b_i to α).
  - If $\alpha \notin b_i^{G^{(i-1)}}$, then $t_{i-1} \notin G^{(i-1)}$, and so $h \notin G$.
  - If $\alpha \in b_i^{G^{(i-1)}}$, then find $g_i \in G^{(i-1)}$ such that $b_i^{g_i} = \alpha$. (It is easy to find such a g_i as a word in our strong generating set S).

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i-1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.
- Determine whether $\alpha \in b_i^{G^{(i-1)}}$ (in other words, whether there is an element of G which stabilizes the first $i-1$ base points and also maps b_i to α).
  - If $\alpha \notin b_i^{G^{(i-1)}}$, then $t_{i-1} \notin G^{(i-1)}$, and so $h \notin G$.
  - If $\alpha \in b_i^{G^{(i-1)}}$, then find $g_i \in G^{(i-1)}$ such that $b_i^{g_i} = \alpha$. (It is easy to find such a g_i as a word in our strong generating set S). Define $t_i := t_{i-1} g_i^{-1}$; then t_i stabilizes $b_1, \ldots, b_i$.

The Algorithm

Begin by defining $t_0 := h$. We proceed through each base point b_i ($i \geq 1$) in turn, assuming at each stage that $t_{i-1} = hg$ for some $g \in G$, and t_{i-1} stabilizes the first $i-1$ base points.

- Compute $\alpha := b_i^{t_{i-1}}$.
- Determine whether $\alpha \in b_i^{G^{(i-1)}}$ (in other words, whether there is an element of G which stabilizes the first $i-1$ base points and also maps b_i to α).
  - If $\alpha \notin b_i^{G^{(i-1)}}$, then $t_{i-1} \notin G^{(i-1)}$, and so $h \notin G$.
  - If $\alpha \in b_i^{G^{(i-1)}}$, then find $g_i \in G^{(i-1)}$ such that $b_i^{g_i} = \alpha$. (It is easy to find such a g_i as a word in our strong generating set S). Define $t_i := t_{i-1} g_i^{-1}$; then t_i stabilizes $b_1, \ldots, b_i$.
- Iterate.

The Algorithm

If we complete this process for all base points, then we have $h \in G \iff t_m = 1$, and moreover in this case we have $h = g_m g_{m-1} \ldots g_1$ has been expressed as a product of words in S.