The Schreier-Sims algorithm

Petr Nižnanský

Department of Algebra
Faculty of Mathematics and Physics
Charles University in Prague

25. 3. 2012 / Spring School of Algebra

Outline

Notation

- Ω is finite set
- $G = \langle\, T \,\rangle$ is group and T is generating set
- $B = \{\, \beta_1, \ldots, \beta_k \,\}$ is base ($G_{(\beta_1,\ldots,\beta_k)} = 1$)
- $G^{[i]} = G_{(\beta_1,\ldots,\beta_{i-1})}$ is stabilizer ($G^{[1]} = G$)
- S is strong generating set (SGS) if

$$\left\langle\, S \cap G^{[i]} \,\right\rangle = G^{[i]},$$

for $i = 1, \ldots, k+1$

Lemma

Let $B = \{ \beta_1, \ldots, \beta_k \} \subseteq \Omega$ *and* $G \leq Sym(\Omega)$. *For* $1 \leq j \leq k+1$, *let* $S_j \subseteq G_{(\beta_1,\ldots,\beta_{j-1})}$ *such that* $\langle S_j \rangle \geq \langle S_{j+1} \rangle$ *holds for* $j \leq k$. *If* $G = \langle S_1 \rangle$, $S_{k+1} = \emptyset$, *and*

$$\langle S_j \rangle_{\beta_j} = \langle S_{j+1} \rangle \tag{1}$$

holds for all $1 \leq j \leq k$ *then* $B = (\beta_1, \ldots, \beta_k)$ *is a base for* G *and* $S = \bigcup_{j=1}^{k} S_j$ *is an SGS for* G *relative to* B.

Proof.

- induction on $|\Omega|$
- $|\Omega| = 1$ trivial case $G = \{ e \}$
- inductive hypothesis: $S^* = \bigcup_{j=2}^{k} S_j$ is an SGS for $\langle S_2 \rangle$, $B^* = (\beta_2, \ldots, \beta_k)$ is relative base
- we have to check $\langle S \cap G^{[i]} \rangle = G^{[i]}$ holds for $i = 2, \ldots, k+1$
- for $i = 2$ we use (1) with $j = 1$, we obtain $G_{\beta_1} = \langle S_2 \rangle \leq \langle S \cap G_{\beta_1} \rangle$ and reverse inequality is obvious
- for $i > 2$ note that $S^* \cap G_{(\beta_1,\ldots,\beta_{i-1})}$ generates $\langle S_2 \rangle_{(\beta_1,\ldots,\beta_{i-1})}$
- $G^{[i]} \geq \langle S \cap G_{(\beta_1,\ldots,\beta_{i-1})} \rangle \geq \langle S^* \cap G_{(\beta_1,\ldots,\beta_{i-1})} \rangle = \langle S_2 \rangle_{(\beta_1,\ldots,\beta_{i-1})} = (G_{\beta_1})_{(\beta_2,\ldots,\beta_{i-1})}$

$\square$

Notation for algorithm

- $G = \langle T \rangle$ group with generation set T
- $B = (\beta_1, \dots, \beta_m)$ is already known elements of base
- S_i is an approximation for a generator set of stabilizer $G_{(\beta_1, \dots, \beta_{i-1})}$
- we always maintain the property $\langle S_i \rangle \geq \langle S_{i+1} \rangle$ for all i

Definition

We say that the data structure is *up to date below level j* (UTDB) if

$$\langle S_i \rangle_{\beta_i} = \langle S_{i+1} \rangle$$

holds for all $i = j, \dots, m$.

The Schreier-Sims algorithm

Algorithm

INPUT: T - set of generators of G
OUTPUT: S - strong generation set

(1) Set $S_1 := T$, choose $\beta_1 \in \Omega$ that is moved by at least one generator, UTDB $j = 1$

(2) while $j \neq 0$ do

- compute R_j transversal $\langle S_j \rangle$ mod $\langle S_j \rangle_{\beta_j}$
- compute Schreier generators (SG) for $\langle S_j \rangle_{\beta_j}$
- if $g \in \langle S_{j+1} \rangle$ for all SG then $j = j - 1$
  else add siftee of g to S_{j+1} and $j = j + 1$
- if $j = m$ then add a new base point β_{m+1} to B

Correctness is from Lemma.

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

Compute SGS for $G = \langle (123), (124) \rangle = A_4$. UTDB will be j.

- $S_1 = \{ (123), (124) \}$, $B = \{ 1 \}$, Schreier tree $T_1 = ((), (123), (123), (124))$, $j = 1$
- $\langle S_1 \rangle_1 = \{ (), (234), (243) \}$, transversal $R_1 = \{ (), (12)(34), (13)(24), (14)(23) \}$
- one SG is (234) and is not in $S_2 = \{ () \}$
- $S_2 = \{ (234) \}$, $B = \{ 1, 2 \}$, Schreier tree $T_2 = (*, (), (234), (234))$, $j = 2$
- $\langle S_2 \rangle_2 = \{ () \}$, transversal $R_2 = \{ (), (234), (243) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234))$)
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234))$)
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234)))$
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234))$)
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234)))$
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234)))$
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Example

Example

- all SG obtained from R_2 and S_2 are () and hence contained in $S_3 = \{ () \} \implies j = 1$
- another SG from R_1 and S_1 is (243)
- sifting: we want test if $g = (243) \in \langle S_2 \rangle$, (Schreier tree $T_2 = (*, (), (234), (234)))$
- $g' = g(234) = (243)(234) = ()$ so $\implies (243) \in \langle S_2 \rangle$
- there no other SG from R_1 and S_1, $j = 0$

Result

- base is $B = \{ 1, 2 \}$
- SGS is $S = \{ (123), (124), (234) \}$

Random Schreier-Sims algorithm (1)

Two main possibilities how to randomized (and speed up) the algorithm.

Problem

Given $\langle S_j \rangle$, transversal R_j for $\langle S_j \rangle$ mod $\langle S_j \rangle_{\beta_j}$ and $\langle S_{j+1} \rangle$,

$$\text{decide whether } \langle S_{j+1} \rangle = \langle S_j \rangle_{\beta_j}.$$

Faster (probabilistic) solution

Do not compute all Schreier generators (SG). Test only sample of them.

Random Schreier-Sims algorithm (1)

Algorithm

INPUT: T - set of generators of G
OUTPUT: S - strong generation set

(1) Set $S_1 := T$, choose $\beta_1 \in \Omega$ that is moved by at least one generator, UTDB $j = 1$

(2) while $j \neq 0$ do

- compute R_j transversal $\langle S_j \rangle$ mod $\langle S_j \rangle_{\beta_j}$
- compute Schreier generators (SG) for $\langle S_j \rangle_{\beta_j}$
- if $g \in \langle S_j \rangle_{\beta_j}$ for all SG then $j = j - 1$
  else add siftee of g to S_{j+1} and $j = j + 1$
- if $j = m$ then add a new base point β_{m+1} to B

Random Schreier-Sims algorithm (2)

Lemma

B is a partial base and S is a partial strong generating set for G. Then $|R_1 \cdot \ldots \cdot R_k| = |\beta_1^{\langle S_1 \rangle}| \cdot \ldots \cdot |\beta_k^{\langle S_k \rangle}|$ *divides* $|G|$.

Proof.

$$
\begin{aligned}
|G| &= \prod_{i=1}^{k} |\langle S_i \rangle : \langle S_{i+1} \rangle| \cdot |\langle S_{k+1} \rangle| \\
&= |\langle S_{k+1} \rangle| \prod |\langle S_i \rangle : \langle S_i \rangle_{\beta_i}| \cdot |\langle S_i \rangle_{\beta_i} : \langle S_{i+1} \rangle| \\
&= |\langle S_{k+1} \rangle| \prod |\beta_i^{\langle S_i \rangle}| \cdot |\langle S_i \rangle_{\beta_i} : \langle S_{i+1} \rangle|
\end{aligned}
$$

Random Schreier-Sims algorithm (2)

Corollary

B is a partial base and S is a partial strong generating set for G. Then a random (uniform) $g \in G$ does not sift through the transversal system with probability at least $1/2$.

Problem

Without SGS we can not produce a random element from G.

Random Schreier-Sims algorithm (2)

Algorithm - random

INPUT: T - set of generators of G
OUTPUT: S - strong generation set

(1) Set $S := T$, choose $\beta_1 \in \Omega$ that is moved by at least one generator
(2) while *stopping_condition* = false do
    - let g by a random element of G
    - let g' by the siftee of g
    - if $g' \neq e$ then
        - add g' to S
        - if g' fixed all points of B then add a new point not fixed by g'

Random Schreier-Sims algorithm (2)

Stopping conditions

The tree most common stopping conditions:

(1) R random elements have been considered
(2) C consecutive random elements have all sift to the identity
(3) the product of the lengths of the partial basic orbits has reached L

Note

If the order of the group is known in advance, we can set L to by the order $\implies$ algorithm is deterministic.

Random Schreier-Sims algorithm (2)

Group	$C = 10$		$C = 30$		$C = 50$		$L = \|G\|$
	time	/10	time	/10	time	/10	time
S_{30}	188	3	224	5	270	9	211
S_{50}	1948	1	2824	6	3297	7	3036
S_{63}	8441	1	10418	2	11213	6	10198
A_8	40	10	40	10	42	10	38
M_{11}	10	5	14	9	19	10	10
M_{22}	809	10	850	10	902	10	810
$A_5 \times A_5$	16	10	18	10	20	10	15

Where we can find Schreier-Sims algorithm

software	specialization	Schreier-Sims
GAP	permutation and matrix groups	randomized
Mathematica	-	yes
Pari/GP	computation number theory	no
Sage	-	yes
CoCoA	commutative algebra	no

Thank you for your attention.