# Permutation Basis

hos

2024 年 10 月 11 日

## 1 Schreier の補題

$G$ を群，$S$ を $G$ の生成系とする．$H \leq G$ を部分群，$\sigma\colon G/H \to G$ を標準全射 $G \twoheadrightarrow G/H$ の section であって $\sigma(H) = 1$ を満たすものとする．$R = \sigma(G/H)$ とおく ($R$ は 1 を含む $G/H$ の完全代表系である)．このとき，

$$T = \{\sigma(srH)^{-1}sr \mid r \in R,\, s \in S\}$$

とおくと $H = \langle T \rangle$ となる．

特に，$G$ が有限生成ならば $H$ も有限生成である．

**証明.** まず，

$$T^{-1} = \{\sigma(s^{-1}rH)^{-1}s^{-1}r \mid r \in R,\, s \in S\}$$

を示す．$r \in R$, $s \in S$ をとる．$r' = \sigma(srH) \in R$ とおくと，$\sigma(s^{-1}r'H) = \sigma(s^{-1}srH) = \sigma(rH) = r$ であるから，

$$(\sigma(srH)^{-1}sr)^{-1} = r^{-1}s^{-1}\sigma(srH) = \sigma(s^{-1}r'H)^{-1}s^{-1}r'$$

となるから $T^{-1} \subseteq$ (右辺) である．逆向きも同様.

$H \subseteq \langle T \rangle$ を示す．任意の $h \in H$ は $h \in G = \langle S \rangle$ より $h = s_0 s_1 \cdots s_{k-1}$ ($s_i \in S \cup S^{-1}$) と書ける．

- $0 \leq i \leq k$ に対し $r_i = \sigma(s_i s_{i+1} \cdots s_{k-1}H)$ とおく．
- $0 \leq i \leq k-1$ に対し $t_i = r_i^{-1}s_i r_{i+1}$ とおく．

すると，$r_0 = \sigma(hH) = \sigma(H) = 1$ および $r_k = \sigma(H) = 1$ より $h = t_0 t_1 \cdots t_{k-1}$ であり，$0 \leq i \leq k-1$ に対し

$$\sigma(s_i r_{i+1}H) = \sigma(s_i(s_{i+1} \cdots s_{k-1}H)) = r_i$$

なので $t_i \in T \cup T^{-1}$ である．よって $h \in \langle T \rangle$ となるのでよい.

$H \supseteq \langle T \rangle$ を示す．$r \in R$, $s \in S$ をとる．$\sigma(srH)H = srH$ なので $H = \sigma(srH)^{-1}srH$ となり，$\sigma(srH)^{-1}sr \in H$ が従うのでよい. ■

**注.** $\sigma(H) = 1$ を仮定しない場合は証明に修正が必要．$r_k, t_k$ を $r_k = h^{-1}\sigma(H)h$ によって置き換える ($r_k \in R$ とは限らない) ことで，

$$\sigma(s_{k-1}r_k H) = \sigma(s_{k-1}H) = r_{k-1}$$

および

$$t_0 t_1 \cdots t_{k-1} = r_0^{-1} h r_k = \sigma(H)^{-1} h h^{-1} \sigma(H) h = h$$

が成り立つのでよい.

## 2 Sims filter

$[l, r) := \{l, l+1, \ldots, r-1\}$ 上の対称群を $\mathfrak{S}_{[l,r)}$ で表す. $l' \leq l \leq r \leq r'$ に対し, $\mathfrak{S}_{[l,r)} \leq S_{[l',r')}$ とみなす.

$G \leq \mathfrak{S}_n := \mathfrak{S}_{[0,n)}$ を置換群とし, $G$ の生成系 $S$ が与えられているとする. このとき, $G$ の生成系 $T$ であって, $T \subseteq S$ であり,

> 任意の $0 \leq u < v < n$ に対し, $t \in T$ であって「$t \in \mathfrak{S}_{[u,n)}$ かつ $t(u) = v$ を満たすもの」は高々 1 個である

という条件を満たすもの (特に $|T| \leq \binom{n}{2}$ を満たす) を, 以下のようにして $O(|S|n^2)$ 時間・$O(n^3)$ 空間で得られる:

$T$ の元を管理する配列 $t_{u,v}$ を null で初期化する. 各 $s \in S$ に対し, $u = 0, 1, \ldots, n-1$ の順に以下を行う:

- $t_{u,s(u)}$ が null でない場合, $s \leftarrow t_{u,s(u)}^{-1} s \in \mathfrak{S}_{[u+1,n)}$ とする.
- $t_{u,s(u)}$ が null の場合, $t_{u,s(u)} \leftarrow s$ として break する.

## 3 Schreier–Sims

$G \leq \mathfrak{S}_n$ を置換群とし, $G$ の生成系 $S$ が与えられているとする. $0 \leq u \leq n$ に対し, $G_u = G \cap \mathfrak{S}_{[u,n)}$ とおく. $G = G_0 \geq G_1 \geq \cdots \geq G_{n-1} \geq G_n = 1$ である.

各 $0 \leq u \leq n-1$ に対し, 1 を含む $G_u / G_{u+1}$ の完全代表系 $R_u$ を構成したい.

$0 \leq u \leq n-1$ に対し, $G_u$ の生成系 $S_u$ が与えられたとき, $R_u$ を構成し, さらに $G_{u+1}$ の生成系 $S_{u+1}$ を求めたい.

$G_u$ による $u$ の軌道を $O_u = \{g(u) \mid g \in G_u\}$ とすると, $R_u \to O_u;\ r \mapsto r(u)$ は全単射である:

- 全射性: $v \in O_u$ をとると, $g(u) = v$ なる $g \in G_u$ がとれて, $g = rh$ なる $r \in R_u$, $h \in G_{u+1}$ がとれて, $r(u) = r(h(u)) = g(u) = v$ となる.
- 単射性: $r, r' \in R_u$ が $r(u) = r'(u)$ を満たすと, $r r'^{-1} \in G_{u+1}$ より $r G_{u+1} = r' G_{u+1}$ なので $r = r'$.

$O_u$ を DFS または BFS によって求める. すなわち, 訪問した $v \in O_u$ について, 各 $s \in S_u$ に対し, $s(v)$ が未訪問なら辺 $v \xrightarrow{s} s(v)$ を張って $s(v) \in O_u$ を訪問する (有限群なので $S_u^{-1}$ の元を追加で調べる必要はない). このようにして $u$ を根とする外向木が得られる.

$v \in O_u$ に対し, 根からのパスを $u \xrightarrow{s_0} * \xrightarrow{s_1} \cdots \xrightarrow{s_{k-1}} v$ として, 対応する元を $r_{u,v} = s_{k-1} \cdots s_1 s_0 \in G_u$ と定め, $R_u = \{r_{u,v} \mid v \in O_u\}$ とするとこれが所望の完全代表系である.

その後，Schreier の補題を適用し

$$S_{u+1} = \{\sigma(srG_{u+1})^{-1}sr \mid r \in R_u,\, s \in S_u\} = \{r_{u,s(v)}^{-1}sr_{u,v} \mid v \in O_u,\, s \in S_u\}$$

とすればよい．この生成系は閉路の生成系と考えられる．

計算量を解析する．

各 $S_u$ に対して Sims filter を適用して $|S_u| \leq \binom{n-u}{2}$ を仮定してよい．入力の $S$ に対する Sims filter は $O(|S|n^2)$ 時間・$O(n^3)$ 空間．

各 $0 \leq u \leq n-1$ について，DFS または BFS は $|O_u||S_u| = O(n^3)$ 時間，木 DP で $r_{u,v}$ たちを求めるのに $O(n^2)$ 時間，記録に $O(n^2)$ 空間．Schreier の補題によって構成した生成系のサイズは $|O_u||S_u| = O(n^3)$ なので，それに対する Sims filter の適用は $O(n^5)$ 時間・$O(n^3)$ 空間．

以上より，合計 $O(|S|n^2 + n^6)$ 時間・$O(n^3)$ 空間．

任意の $g \in G$ は $g = r_0 r_1 \cdots r_{n-1}$ $(r_u \in R_u)$ の形に一意に書ける．特に，$|G| = |R_0||R_1| \cdots |R_{n-1}|$．

$g \in \mathfrak{S}_n$ が与えられたとき $g \in G$ か否かの判定は $O(n^2)$ 時間でできる：

- $g(0) \in O_0$ のとき，$r_{0,g(0)}^{-1} g \in \mathfrak{S}_{[1,n)}$ が $G_1$ に含まれるかの判定に帰着．
- $g(0) \notin O_0$ のとき，$g \notin G$．

## 4 incremental

前節のアルゴリズムを追うと，$S$ の元が incremental に与えられたとき，$R_u, S_u$ もすべて incremental に管理できることがわかる [2]．

$g \in \mathfrak{S}_{[u,n)}$ に対する以下の関数を設計する：

- `contains`$(u, g)$：$g \in G_u$ かどうか判定する．
  - $u = n$ のとき true を返す．
  - $g(u) \in O_u$ のとき，`contains`$(u+1, r_{u,g(u)}^{-1} g)$ を返す．
  - $g(u) \notin O_u$ のとき，false を返す．
- `add`$(u, g)$：$G_u$ に $g$ を追加する．
  1. `contains`$(u, g)$ を呼び，$g \in G_u$ なら何もせず返す．
  2. $S_u$ に $g$ を追加する．
  3. 各 $v \in O_u$ に対し，`dfs`$(u, gr_{u,v})$ を呼ぶ (各頂点から新しい辺を辿る)．
- `dfs`$(u, g)$：$O_u$ において頂点 $v := g(u)$ を訪れる．
  - $v \in O_u$ のとき，`add`$(u+1, r_{u,v}^{-1} g)$ を呼ぶ (閉路)．
  - $v \notin O_u$ のとき，
    1. $O_u$ に $v$ を追加し，$r_{u,v} = g$ とする．
    2. 各 $s \in S_u$ に対し，`dfs`$(u, sg)$ を呼ぶ (新しい頂点から各辺を辿る)．

Sims filter の代わりの生成系として，追加しようとしている元が実際に群を広げるときのみ生成系に足すことにしている．$G_u$ が真に広がるのは $\left\lfloor \frac{3(n-u)-1}{2} \right\rfloor - \mathrm{popcnt}(n-u)$ 回しか起こらないことが知られてお

り [4]，$|S_u| = O(n)$ と抑えられる．

各 $u$ に対し，`dfs`$(u, *)$ は $|O_u||S_u| = O(n^2)$ 辺を過不足なく見る．各辺の置換計算が $O(n)$ 時間なので $O(n^3)$ 時間．

`add` の呼び出しは，外から $u = 0$ で呼ぶのが $O(|S|)$ 回，`dfs` から呼ぶのが各 $u$ から $O(|O_u||S_u|) = O(n^2)$ 回．これらにそれぞれに対し `contains` が呼ばれ，$O(n^2)$ 時間．

以上より，合計 $O(|S|n^2 + n^5)$ 時間・$O(n^3)$ 空間．

# 5 参考文献


[1] adamant, Permutation group basis construction (Schreier–Sims algorithm), `https://codeforces.com/blog/entry/111290`

[2] Benq, `https://codeforces.com/gym/421334/submission/210708091`

[3] `https://planetmath.org/schreierslemma`

[4] Peter J Cameron, Ron Solomon, Alexandre Turull, Chains of subgroups in symmetric groups, `https://doi.org/10.1016/0021-8693(89)90256-1`