Algorithms for permutation groups I

Adéla Skoková

In this talk we present some fundamental definitions, Sifting procedure and Schreier's lemma.
Sifting procedure is a factorization procedure and may be concidered as a permutation group version of Gaussian eliination. Sifting can also be used for testing membership in some permutation group.

Permutation group $\mathbf{G}$ is a group whose elements are permutations of the given set $\mathbf{M}$. Group operations are composition of permuttions in $\mathbf{G}$.

Group of all permutations is symetric group $\mathrm{Sym}(\Omega)$ and the group of permutations is its subgroup.

Definition 1 (Small-base group)**.** We call an (infinite) family Δ of permutation groups small-base groups if each $\mathbf{G} \in \Delta$ of degree n satisfies $\log |\mathbf{G}| < \log^c n$ for some fixed constant c.

Definition 2 (Base for permutation group)**.** A sequence of elements $\mathbf{B} = (\beta_1, \ldots, \beta_m)$ from Ω is called a base for $\mathbf{G}$ if the only element of $\mathbf{G}$ to fix $\mathbf{B}$ pointwise is the identity.

The sequence $\mathbf{B}$ defines a subgroup chain

$$\mathbf{G} = \mathbf{G}^{[1]} \leq \mathbf{G}^{[2]} \leq \ldots \leq \mathbf{G}^{[m]} \leq \mathbf{G}^{[m+1]} = 1,$$

where $\mathbf{G}^{[i]} := \mathbf{G}_{(\beta_1,\ldots,\beta_{i-1})}$ is the pointwise stabilizer of $\{\beta_1, \ldots, \beta_{i-1}\}$.

Definition 3 (Nonredundant base)**.** The base is called nonredundant if $\mathbf{G}^{[i+1]}$ is a proper subgroup of $\mathbf{G}^{[i]}$ for all $i \in [1, m]$.

The cosets of $\mathbf{G}^{[i]}$ mod $\mathbf{G}^{[i+1]}$ correspond to the elements of the orbit $\beta_i^{\mathbf{G}^{[i]}}$.

$$|\mathbf{G}^{[i]} : \mathbf{G}^{[i+1]}| = |\beta_i^{\mathbf{G}^{[i]}}| \leq n \text{ for all } i \in [1, m]$$

If $\mathbf{B}$ is nonredundant then $|\mathbf{G}^{[i]} : \mathbf{G}^{[i+1]}| \geq 2$.

$$2^{|\mathbf{B}|} \leq |\mathbf{G}| \leq n^{|\mathbf{B}|}$$

$$\frac{\log |\mathbf{G}|}{\log n} \leq |B| \leq \log |\mathbf{G}|$$

Definition 4 (Strong generating set (SGS))**.** A strong generating set (SGS) for $\mathbf{G}$ relative to $\mathbf{B}$ is a generating set $\mathbf{S}$ for $\mathbf{G}$ with the property that

$$\left\langle \mathbf{S} \cap \mathbf{G}^{[i]} \right\rangle = \mathbf{G}^{[i]}, \text{ for } 1 \leq i \leq m + 1.$$

Definition 5 (Fundamental orbits of SGS)**.** Orbits $\beta_i^{\mathbf{G}^{[i]}}$ of an SGS are called fundamental orbits of $\mathbf{G}$. By $|\mathbf{G}| = \prod i = 1, m|\mathbf{G}^{[i]} : \mathbf{G}^{[i+1]}|$ from orbit sizes we get $|\mathbf{G}|$.

Every $g \in \mathbf{G}$ can be written uniquely in the form $g = r_m r_{m-1} \cdots r_1$ with $r_i \in R_i$.

The sifting procedure:

(1) Given $g \in \mathbf{G}$, find the coset representative $r_1 \in R_1$ such that $\beta_1^g = \beta_1^{r_1}$.
(2) Then compute $g_2 := g r_1^1 \in \mathbf{G}[2]$; find $r_2 \in R_2$ such that $\beta_2^{g_2} = \beta_2^{r_2}$;
(3) compute $g_3 := g_2 r_2^1 \in \mathbf{G}[3]$;
(4) etc...

Definition 6 (Siftee)**.** The ratio h_i with the largest index i ($i \leq m+1$) computed by the sifting procedure is called the siftee of h.

Definition 7 (Schreier tree)**.** A Schreier tree data structure for $\mathbf{G}$ is a sequence of pairs (S_i, T_i) called Schreier trees, one for each base point β_i, $1 \leq i \leq m$.

T_i is a directed labeled tree, with all edges directed toward the root β_i and edge labels from a set $S_i \subseteq \mathbf{G}^{[i]}$.

Vertices of T_i are points of the fundamental orbit $\beta_i^{\mathbf{G}^{[i]}}$.

Labels satisfy the condition that for each directed edge from γ to δ with label h, $\gamma^h = \delta$.

If γ is a vertex of T_i then the sequence of the edge labels along the unique path from γ to β_i in T_i is a word in the elements of S_i such that the product of these permutations moves γ to β_i .

Each Schreier tree (S_i, T_i) defines inverses of a set of coset representatives for $G^{[i+1]}$ in $G^{[i]}$.

Memory requirement for storage:

- $\mathbf{S}_i$ is $O(|\mathbf{S}_i|n)$
- $\mathbf{T}_i$ is $O(n)$.

T_i can be stored in an array V_i of lenght n.

- γ-th entry of V_i is deffined iff $\gamma \in \beta_i^{\mathbf{G}^{[i]}}$
- $V_i[\gamma]$ is a pointer to the element of S_i
- that is the label of the unique edge of T_i starting at γ.

Lemma 8 (Schreier's Lemma)**.** *Let $\mathbf{H} \leq \mathbf{G} = \langle \mathbf{S} \rangle$ and let $\mathbf{R}$ be a right transversal for $\mathbf{G}$ mod $\mathbf{H}$, with $1 \in \mathbf{R}$.Then the set*

$$\mathbf{T} = rs(\overline{rs})^1 | r \in \mathbf{R}, s \in \mathbf{S}$$

generates $\mathbf{H}$.
The elements of T are called Schreier generators for $\mathbf{H}$.