Master Elements

Spencer

March 7, 2017

Given a group $G = \langle S \rangle$ and any element $g \in G$, it is often desirable to find a factorization of g in terms of the elements in S. If we were to generate all elements of G and store them in terms of their factorizations using S, then G becomes a search space for the factorization of any given element $g \in G$. For all but the smallest of groups, however, this is completely impractical.

If we have a subnormal series of G, namely

$$\{e\} = H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n = G,$$

then it may be practical to store the coset representatives of each factor group H_i/H_{i-1}. These become a search space at each tier in the subgroup chain. We let k be the smallest integer for which $g \in H_k$, then let $h_1 \in H_k$ be the stored coset representative such that $gH_{k-1} = h_1 H_{k-1}$. We then find that $h_1^{-1} g \in H_{k-1}$, and repeat this process until we find

$$h_r^{-1} \dots h_1^{-1} g \in H_1,$$

at which point we can conclude that

$$g = h_1 \dots h_r,$$

which can be rewritten in terms of the elements in S, provided brought them along at each level in the chain.

Note that the generators for H_i/H_{i-1} can be found in terms of the generators S_i for H_i as

$$H_i/H_{i-1} = \{s_1 \dots s_j H_{i-1} | s_k \in S_i\} = \{(s_1 H_{i-1}) \dots (s_j H_{i-1}) | s_k \in S_i\}.$$

Once the factor group H_i/H_{i-1} is generated in terms of a sequence of coset representatives, these can also be used as a transversal in Schreier's lemma to find generators S_{i-1} for H_{i-1}.

This approach to factorization has its own set of diffulties as well, however; not the least of which being the difficulty in producing the subnormal chain. Factorizations found this way grow exponentially as the chain is descended.

So we turn now to what might be a more practical method in circumstances where more about the group is known up front.

Definition 0.1. *For any group G, let an element $m \in G$ be a* ***master element*** *if for every $g \in G$, there exists a sequence $\{r_i\}_{i=1}^{k} \subset G$ such that*

$$g = \prod_{i=1}^{k} r_i m r_i^{-1}. \tag{1}$$

A master element is often known for groups of interest, and the set of all possible r_i becomes the search space. In the context of permutation groups, each r_i found may help us descend a stabilizer chain we needn't generate.

Calling a group **mastered** if it has a non-empty subset of master elements, we give our first lemma.

Lemma 0.1 (Gallian)**.** *The cyclic groups are the only mastered Abelian groups.*

Proof. Notice that equation (1) immediately reduces to

$$g = m^k.$$

Clearly every element of every cyclic group is of this form, and so every master element is a generator of the group. This is not the case, however, for any non-cyclic Abelian group. □

This factorization method, therefore, cannot generally help us with Abelian groups. This isn't too desparaging, however, since the factoring problem may be generally harder in the non-Abelian cases anyway.