Master Elements

Spencer

March 27, 2017

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*

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

Calling a group **mastered** if it has a non-empty subset of master elements, we give the following 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. □

We now describe a class of permutation groups that are all mastered. Our convention for composition is that, for permutations a and b, the composition ab maps domain elements through a first, then b. Similarly, products of cycles are evaluated from left to right. The notation $x^a = y$ is used instead of $a(x) = y$ to avoid the idea that $a(x)$ is a composition of the permutation a with the 1-cycle (x).

Lemma 0.2. *Let $p_i = (p_{i,1}, \ldots, p_{i,n})$ be one of m permutations, each an n-cycle of elements in a domain Ω, and let $G = \langle \{p_i\}_{i=1}^m \rangle$. If there exists $1 \leq j \leq m$ such that for any $1 \leq k \leq m$, we can find $r \in G$ in the form*

$$r = (p_{k,1}, p_{j,1}) \ldots (p_{k,n}, p_{j,n})q,$$

where q is a permutation that, for all $1 \leq i \leq m$, has $p_{j,i}^q = p_{j,i}$, then G is a mastered group.

Proof. Since every element of G is a product of the generators, it suffices to show that every generator factors as shown in equation (1). By hypothesis, it is easy to see that

$$p_k = r p_j r^{-1},$$

showing that p_j is a master element of G. □

Corollary 0.1. *The symmetric group on a domain Ω of size n is a mastered group.*

Proof. Note that $S_n = \{(1,2)(2,3)\ldots(n-1,n)\}$. Now choose, arbitrarily, $m = (1,2)$ to be our master element. Then, for any generator, we have $(x, x+1) = rmr^{-1}$, where

$$r = \prod_{j=1}^{x-2} (x-i, x-i-1)(x-i+1, x-i).$$

□

The distinction between an idealy master group and one that is merely mastered comes into play when we consider exploiting the mastered property of a group for the purpose of factoring its elements in terms of a set of generators for the group.

Definition 0.2. *Call a group G* ***ideally*** *mastered if for every $g \in G$, there exists $r \in G$ such that*

$$|A(grmr^{-1})| < |A(g)|,$$

where $A : G \to \Omega$ is a function defined as

$$A(g) = \{i \in \Omega | i^g \neq i\}.$$

Lemma 0.3. *The symmetric group on a domain Ω of size n is an ideally mastered group.*

Proof. Note that $S_n = \langle\{(x, y)|x, y \in \Omega \text{ and } x \neq y\}\rangle$. We now again choose, arbitrarily, $m = (1, 2)$ to be our master element. Then, for any generator, we have $(x, y) = rmr^{-1}$, where

$$r = \prod_{i=0}^{x-2}(x - i, x - i - 1) \prod_{j=0}^{y-3}(y - i, y - i - 1).$$

$\square$

For any $g \in S_n$, finding a factorization of g in terms of the generators found in lemma 0.3, or even those of corollary 0.1, is trivial. For other mastered groups, however, finding a factorization in terms of the generators may not be so easy. So we consider the following algorithm for factoring an element g in an ideally mastered group G.

Let $g_1 = g$, and then, while $g_k \neq e$, let $g_{k>1} = g_{k-1}r_kmr_k^{-1}$ where $|A(g_k)| < |A(g_{k-1})|$. The idea here is that if we can factor each r_k in terms of the generators, and we know the factorization of m in terms of the generators, then we've deduced a factorization of g. At each iteration, the crux is finding r_k.

Can we find a test for a mastered group being ideal? Can we find a test for a group being mastered for that matter? Can we prove something about finding r_k? Clearly we can go down the generator tree, but can we show an upper-bound on how far we'd have to go?