The Orbit-Shuffler Theorem

Spencer T. Parkin

March 21, 2017

We work here to prove a generalization of the Orbit-Stabilizer Theorem. Let G be a finite permutation group with each $g \in G$ defined over the set Ω. We say that G is a subgroup of the symmetric group of Ω. Given a non-trivial subset P of Ω, we define, for any $g \in G$,

$$P^g = \{p^g | p \in P\}.$$

We also define

$$G^P = \{g \in G | P^g = P\},$$

and call this the shuffler of P in G. Of course, when P is a singleton set, this is the stabilizer of the sole member of P in G.

Lemma 0.1. *G^P is a subgroup of G.*

Proof. Closure being trivial, we need only show that for any $a \in G^P$, we also have $a^{-1} \in G^P$. To do this, we must convince ourselves that since a is a bijection, we must have $P^a = P$ if and only if $P = P^{a^{-1}}$. □

Lemma 0.2. *For any pair of elements $a, b \in G$, we have*

$$P^a = P^b \implies P^{ab^{-1}} = P.$$

Proof. If $p \in P$, then $p^b \in P^b = P^a$ means there exists $q \in P$ such that $p^b = q^a$. Then $q^{ab^{-1}} = p \implies p \in P^{ab^{-1}}$. On the other hand, let $p \in P^{ab^{-1}}$. So there exists $q \in P$ such that $q^{ab^{-1}} = p$. Now $q^a \in P^a = P^b \implies p^b \in P^b$. So there is $r \in P$ such that $p^b = r^b \implies p = r \in P$. □

We now define

$$P^G = \{P^g | g \in G\},$$

and say that P^G is the orbit of P in G. We can now prove the following theorem.

Theorem 0.1 (Orbit-Shuffler Theorem)**.** *A relationship between $|G|$, $|G^P|$ and $|P^G|$ is given by*

$$|G| = |G^P||P^G|.$$

Proof. Letting T be a right-transversal of G^P in G, we simply find a bijection between T and P^G. Map $t \in T$ to P^t. Let $a, b \in T$ such that $P^a = P^b$. It follows that $P^{ab^{-1}} = P$, and therefore, $ab^{-1} \in G^P$. In turn, we have $G^P a = G^P b \implies a = b$, since a and b are taken from T. □

Defining

$$G^{[P]} = \{g \in G | p^g = p \text{ for all } p \in P\},$$

it is worth noting where the proof of our theorem would fail if we replaced G^P with $G^{[P]}$. Where we run in to trouble is the implication

$$P^{ab^{-1}} = P \;\not\Longrightarrow\; ab^{-1} \in G^{[P]}.$$