# Even and odd permutations

March 7, 2008

Let $S$ be a finite set. Recall that any permutation $\sigma \in Sym(S)$ can be written as a product of disjoint cycles:

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r.$$

Furthermore this expression is unique up to reordering. (Here we don't allow any $\gamma_i$ to be the identity permuation.) Recall also that if $\gamma$ is a cycle of length $\ell > 0$, then $\gamma$ can be written as a product of $\ell - 1$ transpositions.

**Definition 1** *Let $\sigma$ be a permuation of a finite set $S$, and write $\sigma$ as a product of disjoint cycles:*

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r.$$

*Then*

$$N(\sigma) := (\ell_1 - 1) + (\ell_2 - 1) + \cdots + (\ell_r - 1) = \ell_1 + \cdots + \ell_r - r,$$

*where $\ell_i$ is the length of $\gamma_i$.*

Thus if $\ell_i$ is the length of the cycle $\gamma_i$ above, then $\sigma$ can be written as a product of $N(\sigma)$ transpositions. However, such an expression is not unique, and in fact even the number of transpositions in such an expression is not unique. However, the following *is* true.

**Theorem 1** *Suppose that $\sigma$ is written as a product of $m$ transpositions*

$$\sigma = \tau_1 \tau_2 \cdots \tau_m.$$

*Then $m \equiv N(\sigma) \pmod 2$.*

Since congruence is an equivalence relation, it follows that if $\sigma$ is also written as a product of $m'$ transpositions: $\sigma = \tau'_1 \tau'_2 \cdots \tau'_{m'}$, then $m \equiv m' \pmod 2$.

Theorem 1 follows from the following more suggestive result.

**Theorem 2** *If $\alpha$ and $\beta$ are permuations of $S$, then*

$$N(\alpha\beta) \equiv N(\alpha) + N(\beta) \pmod 2.$$

Indeed, note that if $\tau$ is a transposition, then $N(\tau) = 1$. Hence it follows from Theorem 2 that

$$N(\sigma) = N(\tau_1 \tau_2 \cdots \tau_m) \equiv 1 + 1 + \cdots + 1 \equiv m \pmod 2.$$

Note that in fact we only needed to apply Theorem 2 when $\beta$ was a transposition, but in fact the general case of Theorem 2 follows by induction from this case anyway. (Hint: write $\beta$ as a product of transpositions and use the associative law.)

Let us prepare for the proof of Theorem 2 by means of some calculations.

**Lemma 1** *If $\gamma_1$ and $\gamma_2$ are two cycles with exactly one element in common, then $\gamma_1\gamma_2$ is a cycle of length $\ell_1 + \ell_2 - 1$, where $\ell_i$ is the length of $\gamma_i$.*

*Proof:* Actually I think it is convincing enough to compute a typical example:

$$(1\ 2\ 3\ 4)(4\ 5\ 6\ 7) = (1\ 2\ 3\ 4\ 5\ 6\ 7).$$

□

**Lemma 2** *If $\tau$ is a transposition $(a\ b)$ and $\gamma$ is a cycle containing both $a$ and $b$, then $\gamma\tau$ is a product of disjoint cycles $\gamma_1\gamma_2$, where $\ell_1 + \ell_2 = \ell$ (the length of $\gamma$).*

*Proof:* Again, an example should be convincing:

$$(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)(2\ 5) = (1\ 2\ 6\ 7\ 8)(3\ 4\ 5)$$

□

*Proof of Theorem 2:* It suffices to prove the theorem when $\beta$ is a transposition $\tau$. Since $N(\tau) = 1$, we have to prove that $N(\alpha\tau) \equiv N(\alpha) + 1 \pmod ()2$. Write $\alpha$ as a product of disjoint cycles $\alpha = \gamma_1\gamma_2 \cdots \gamma_r$, so by definition, $N(\alpha) = \ell_1 - 1 + \cdots \ell_r - 1$.

Case 1: $\tau$ is disjoint from all the $\gamma_i$.

Then $\alpha\tau = \gamma_1\gamma_2 \cdots \gamma_r\tau$ is a product of disjoint cycles, and so by definition:

$$N(\alpha\tau) = \ell_1 - 1 + \cdots \ell_r - 1 + (2 - 1) = N(\alpha) + 1.$$

Case 2: $\tau$ meets just one of the $\gamma_i$'s, in just one element.

We might as well assume that $\tau$ meets $\gamma_r$ and no other. Then by Lemma 1, $\gamma_r\tau$ is a cycle $\gamma'_r$ of length of $\ell_r + 1$. Then $\alpha\tau = \gamma_1\gamma_2 \cdots \gamma_{r-1}\gamma'_r$ as a product of disjoint cycles, so

$$\begin{aligned} N(\alpha\tau) &= \ell_1 - 1 + \ell_2 - 1 + \cdots \ell_{r-1} - 1 + \ell'_r - 1 \\ &= \ell_1 - 1 + \ell_2 - 1 + \cdots \ell_{r-1} - 1 + \ell_r + 1 - 1 \\ &= N(\alpha) + 1. \end{aligned}$$

Case 3: $\tau$ meets two of the $\gamma_i$'s. Again we may as well assume that it meets $\gamma_{r-1}$ and $\gamma_r$; necessarily it meets each in exactly one element. Then $\gamma_r' := \gamma_r\tau$ is a cycle of length $\ell_r' = \ell_r + 1$, which now contains $\tau$. Hence $\gamma_{r-1}' := \gamma_{r-1}\gamma_r'$ is a cycle of length $\ell_{r-1} + \ell_r' - 1 = \ell_{r-1} + \ell_r$. Hence $\alpha\tau = \gamma_1' \cdots \gamma_{r-1}'$ as a product of disjoint cycles, and

$$\begin{aligned} N(\alpha\tau) &= \ell_1' - 1 + \cdots + \ell_{r-1}' - 1 \\ &= \ell_1 - 1 \cdots + \ell_{r-1} + \ell_r - 1 \\ &= \ell_1 - 1 + \cdots + \ell_{r-1} - 1 + \ell_r = N(\alpha) + 1. \end{aligned}$$

Case 4: $\tau$ meets one of the $\gamma_i$'s in two elements. Thus, we assume that $\tau := (a\ b)$ where $a$ and $b$ both occur in $\gamma_i$, and we may as well assume that $i = r$. Then $\gamma_r\tau$ is a product of two disjoint cycles $\gamma_r'\gamma_{r+1}'$, and $\ell_r' + \ell_{r+1}' = \ell_r$. Hence

$$\begin{aligned} N(\alpha\tau) &= \ell_1 - 1 + \cdots + \ell_r' - 1 + \ell_{r+1}' - 1 \\ &= \ell_1 - 1 + \cdots + \ell_r - 2 = N(\alpha) - 1. \end{aligned}$$

Since $N(\alpha) - 1 \equiv N(\alpha) + 1 \pmod 2$, the result holds in this case too! $\square$