Permutations and Rejewski's Theorem

Klaus Pommerening
Fachbereich Mathematik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-55099 Mainz

7 January 2008, english version 29 November 2011

The Symmetric Group

A **permutation** is a bijective map of a set M onto itself. The permutations of M form a group $\mathcal{S}(M)$.

This group is (at least in discrete mathematics, including cryptologic applications) of particular interest when the set M is finite. In most applications the nature of the elements doesn't matter. (A more formal statement is: "A bijection between two sets M und N induces an isomorphism of the groups $\mathcal{S}(M)$ und $\mathcal{S}(N)$".) Therefore we often simply take the set $\{1, \ldots, n\}$ of natural numbers as our set M and denote the group $\mathcal{S}(M)$ by $\mathcal{S}_n$. This group is called the **symmetric group** of order n.

Proposition 1 *The symmetric group of order n has $n!$ elements:*

$$\#\mathcal{S}_n = n!.$$

Proof. A permutation π is uniquely determined by its values at the arguments $1, \ldots, n$. For $\pi(1)$ we have n possibilities, for $\pi(2)$ then $n-1$, ..., for $\pi(n-1)$ two and for $\pi(n)$ only one. This makes a total of $n!$. $\diamond$

(Note that the dots "..." are a sloppy version of a proof by complete induction. In the remainder of this text we write πx instead of $\pi(x)$.)

Description of Permutations

Often a permutation π of the set $\{1, \ldots, n\}$ is represented by its value table, written in two rows:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi 1 & \pi 2 & \ldots & \pi n \end{pmatrix}.$$

Of course this representation my also be used with other sets M; for $M = \{\mathrm{A}, \ldots, \mathrm{Z}\}$, the alphabet of classic cryptology, a permutation is the same as a monoalphabetic substitution σ and denoted in the form

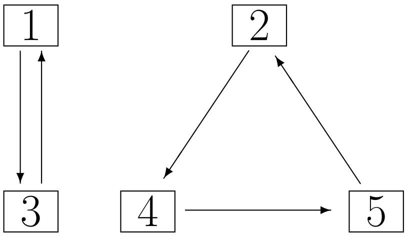
$$\begin{pmatrix} A & \ldots & Z \\ \sigma A & \ldots & \sigma Z \end{pmatrix}$$

(often without parantheses); below each letter we write its image under encryption.

Another description of a permutation π is the **cycle representation**. Let's illustrate this first with an example where $n = 5$: The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

has a natural graphical representation:



and this graph is completely characterized by the arrangement

$$(1\,3)(2\,4\,5)$$

of numbers. This means that each parenthesis defines a "cycle"—start with any element, write its image right of it, then the image thereof, and so on until you get back to the start. Then take any element that's not yet written down (if there is one) and do as before until all elements are met. Fixed points of the permutation yield cycles of length one. The general formula is

$$(a_1, \pi a_1, \ldots, \pi^{k_1-1} a_1) \cdots (a_i, \pi a_i, \ldots, \pi^{k_i-1} a_i) \cdots,$$

where k_i is the smallest natural number ≥ 1 with $\pi^{k_i} a_i = a_i$.

This consideration shows:

Proposition 2 *Each permutation of a finite set has a decomposition into disjoint cycles. This representation is unique except for the order of the cycles and cyclic permutations of the elements inside the cycles.*

Group Theoretic Interpretation

A cycle by itself represents a permutation: permute its elements in the written order in a cyclic way, and let all other elements of M fixed.

Example: The cycle $(2\,4\,5)$ in $\mathcal{S}_5$ corresponds to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \quad \text{or in cycle representation} \quad (1)(2\,4\,5)(3).$$

The cycle (i) in $\mathcal{S}_n$ defines the identity map, no matter which $i = 1, \ldots, n$ we choose. If we identify cycles with the permutations they describe, we immediately get:

Lemma 1 *Disjoint cycles commute as elements of the group $\mathcal{S}_n$.*

If we write the cycles of the cycle decomposition of a permutation next to each other, we just get the product of the corresponding permutations in $\mathcal{S}_n$. Therefore we may express Proposition 2 in the following way:

Corollary 1 *Each permutation is a product of disjoint cycles. This representation is unique except for the order of the factors.*

Partitions

If r_k is the number of cycles of length k of a permutation $\pi \in \mathcal{S}_n$, then we have

$$n \cdot r_n + \cdots + 1 \cdot r_1 = n.$$

Call a finite sequence $[s_1 s_2 \ldots s_m]$ of natural numbers with $s_1 \geq \ldots \geq s_m \geq 1$ a **partition** of n, if $n = s_1 + \cdots + s_m$. If we write down the cycle lengths of a permutation $\pi \in \mathcal{S}_n$ ordered by magnitude – each length with the multiplicity with which it occurs – then we get a partition of n. Call this the **(cycle) type** of π.

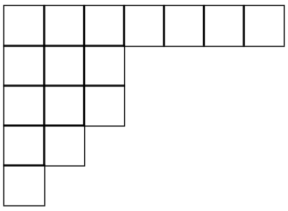
Example: The cycle type of

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\,3)(2\,4\,5)$$

is

$$[3\,2].$$

We often visualise partitions by Young **diagrams**. Given a partition $[s_1 s_2 \ldots s_m]$ of n we build the corresponding Young diagram in the following way: Take m rows and put s_i squares in row i, left aligned. The partition $[7\,3\,3\,2\,1]$ of 16 has the diagram



(The defining condition of a Young diagram is that none of the rows is longer than the row above it.)

Conjugate Permutations

Given $\pi, \rho \in \mathcal{S}_n$, how are the cycle representations of π and of the conjugate permutation $\rho\pi\rho^{-1}$ connected? First we consider the case of a single cycle π,

$$\pi = (a_1 \ \ldots \ a_k),$$

hence $\pi a_i = a_{1+(i \bmod k)}$ for $i = 1, \ldots, k$, all other elements being fixed by π. Then, for $b_i = \rho a_i$, we have

$$\rho\pi\rho^{-1} b_i = \rho\pi a_i = \rho a_{1+(i \bmod k)} = b_{1+(i \bmod k)},$$

hence

$$\rho\pi\rho^{-1} = (b_1 \ \ldots \ b_k).$$

Therefore also $\rho\pi\rho^{-1}$ is a cycle of length k.

Conjugating with ρ is an inner automorphism of the group $\mathcal{S}_n$, that means $\rho(\pi_1\pi_2)\rho^{-1} = (\rho\pi_1\rho^{-1})(\rho\pi_2\rho^{-1})$. Therefore in the general case we can conjugate the single cycles of π with ρ and get as a result the first part the following theorem:

Theorem 1 (i) *Let $\pi, \rho \in \mathcal{S}_n$ be two permutations. Then we get the cycle decomposition of the conjugate permutation $\rho\pi\rho^{-1}$ from that of π by replacing each cycle $(a_1 \ \ldots \ a_k)$ of π with the cycle $(\rho a_1 \ \ldots \ \rho a_k)$.*

(ii) *Two permutations of a finite set are conjugated if and only if they have the same cycle type.*

In other words: The conjugacy classes of the symmetric group $\mathcal{S}_n$ are in a natural correspondence with the partitions of n resp. with the Young diagrams with exactly n squares.

Proof. We only have to show the inverse direction of statement (ii). To this end let $\sigma, \tau \in \mathcal{S}_n$ be of the same cycle type. Write the cycle decompositions of σ and τ below each other in such a way that cycles of the same length align; from this read off a permutation ρ with $\rho\sigma\rho^{-1} = \tau$: Simply map each element to the one below it. ◇

This theorem, as simple as it is, is an essential ingredient to the cryptanalysis of the cipher machine Enigma, and therefore sometimes was called "the theorem that won world war II"; this is an obvious exaggeration, but with a certain confidence we may state that it *helped* in shortening the war in a significant way.

Exercise. Given $\sigma, \tau \in \mathcal{S}_n$, describe all solutions ρ of $\rho\sigma\rho^{-1} = \tau$. (For the case $\tau = \sigma$ see the next section.)

Centralizers of Permutations

Theorem 1 provides an easy approach to determining the centralizer of a permutation. First let us consider a single cycle $\pi = (a_1\, a_2\, \ldots\, a_k)$ of length $2 \leq k \leq n$. Then π acts transitively on the subset $A := \{a_1, a_2, \ldots, a_k\}$ and fixes all elements of the complement $\bar{A} = \{1, \ldots, n\} - A$. For $\rho \in \mathcal{S}_n$ the conjugate $\rho\pi\rho^{-1}$ is the cycle $(\rho a_1\, \ldots\, \rho a_k)$ by Theorem 1. By definition ρ centralizes π if and only if $\rho\pi\rho^{-1} = \pi$. Therefore for $\rho \in C_{\mathcal{S}_n}(\pi)$, the centralizer of π, we must have $\rho a_1 = a_i$ for some i, and then $\rho a_2 = a_{i+1}$ and so on, reducing the indices $\bmod n$ if necessary. That is, ρ acts on A as π^i, and on $\bar{A}$ as an arbitrary permutation. In the reverse direction each permutation with these properties centralizes π. Let $\mathcal{S}_n^A \leq \mathcal{S}_n$ be the subgroup of permutations that fix A elementwise. It is canonically isomorphic with $\mathcal{S}_{n-k}$. Using this notation we may formulate the result of our considerations as:

Proposition 3 *Let $\pi = (a_1\, a_2\, \ldots\, a_k) \in \mathcal{S}_n$ be a single cycle of length $2 \leq k \leq n$, and $A = \{a_1, a_2, \ldots, a_k\}$. Then the centralizer $C_{\mathcal{S}_n}(\pi)$ of π in $\mathcal{S}_n$ is the direct product of the subgroups $< \pi >$ and $\mathcal{S}_n^A$, and is isomorphic with the direct product $\mathcal{Z}_k \times \mathcal{S}_{n-k}$.*

Here $\mathcal{Z}_k$ is the cyclic group of order k.

We want to apply this result to arbitrary permutations. First we observe:

Proposition 4 *Let $\pi = \pi_1 \cdots \pi_s$ be a product of disjoint cycles π_i. For $k = 1, \ldots, n$ let*

$$A_k := \{a \mid 1 \leq k \leq n, a \text{ is in a cycle of } \pi \text{ of length } k\}.$$

Let $\rho \in \mathcal{S}_n$ centralize π. Then $\rho(A_k) = A_k$ for all k, and $\rho|A_k$ centralizes $\pi|A_k$.

Proof. Let $\pi_i = (a_{i1} \cdots a_{ik})$ be a cycle of length k. Then $\rho\pi_i\rho^{-1} = (\rho a_{i1} \cdots \rho a_{ik})$ is a cycle of length k, and $\rho\pi\rho^{-1} = \rho\pi_1\rho^{-1} \cdots \rho\pi_l\rho^{-1}$ is the unique decomposition into disjoint cycles. If ρ centralizes π, then $(\rho a_{i1} \cdots \rho a_{ik})$ is one of cycles of π of length k. Therefore $\rho(A_k) = A_k$. The second assertion follows because the actions of π and ρ on $\{1, \ldots, n\}$ directly decompose into the actions on the subsets A_k. $\diamond$

Proposition 4 reduces the task of determining the centralizer to the case where all the cycles π_i have the same length k. Let $\pi_i = (b_{i1} \ldots b_{ik})$, and $B_i := \{b_{i1}, \ldots, b_{ik}\}$. Then $\{1, \ldots, n\} = B_1 \dot{\cup} \cdots \dot{\cup} B_s$ (and $n = ks$).

Now consider the centralizer $C := C_{\mathcal{S}_n}(\pi)$, and take a $\rho \in C$. Then ρ doesn't necessarily respect the subsets B_i, but it permutes them: There is a unique $j = \bar{\sigma} i$—depending on ρ—such that $\rho(B_i) = B_j$. This defines a permutation $\bar{\sigma} \in \mathcal{S}_s$ of the indices $1, \ldots, s$. This way we get a group homomorphism

$$\Phi \colon C \longrightarrow \mathcal{S}_s, \quad \rho \mapsto \bar{\sigma}.$$

Lift $\bar{\sigma} i$ to a permutation $\sigma \in \Phi^{-1}(\bar{\sigma}) \subseteq \mathcal{S}_n$ by setting $\sigma b_{ih} := b_{\bar{\sigma} i, h}$. Then also $\sigma \in C$, and $\sigma^{-1}\rho$ is in the subgroup

$$C^\circ := \ker \Phi = \{\tau \in C \mid \tau(B_i) = B_i \text{ for } i = 1, \ldots, s\}$$

of permutations that centralize π and respect the B_i. The following characterization of this subgroup is immediate, because for $\tau \in C^\circ$ the restriction $\tau|B_i$ centralizes $\pi_i|B_i$ and therefore is a power of $\pi_i|B_i$.

Lemma 2 *The subgroup C° is the set of permutations with cycle decomposition of the type $\pi_1^{a_1} \cdots \pi_s^{a_s}$, and is isomorphic with the direct product $\mathcal{Z}_k^s$ of s cyclic groups $\mathcal{Z}_k$. This isomorphism defines an embedding $e \colon \mathcal{Z}_k^s \longrightarrow C$. The sequence*

$$\mathbf{1} \longrightarrow \mathcal{Z}_k^s \xrightarrow{e} C_{\mathcal{S}_n}(\pi) \xrightarrow{\Phi} \mathcal{S}_s \longrightarrow \mathbf{1}$$

is exact. The centralizer $C_{\mathcal{S}_n}(\pi)$ has $k^s \cdot s!$ elements.

This result easily generalizes to the general case. Let $\pi = \pi_1 \cdots \pi_s$ be a product of disjoint cycles π_i, let k_i be the length of π_i, and let r_k be the number of cycles of length $k_i = k$, for $k = 1, \ldots, n$. Note that $r_1 + \cdots + nr_n = n$, and many of the r_k are 0. Then we have a natural epimorphism

$$\Phi \colon C \longrightarrow \prod_{k=1}^{n} \mathcal{S}_{r_k},$$

with kernel

$$C^\circ := \ker \Phi = < \pi_1 > \cdots < \pi_s > \cong \prod_{i=1}^{s} \mathcal{Z}_{k_i}$$

We sum this up to a Theorem.

Theorem 2 *For each permutation $\pi \in \mathcal{S}_n$ we have a natural exact sequence*

$$\mathbf{1} \longrightarrow \prod_{i=1}^{s} \mathcal{Z}_{k_i} \xrightarrow{e} C_{\mathcal{S}_n}(\pi) \xrightarrow{\Phi} \prod_{k=1}^{n} \mathcal{S}_{r_k} \longrightarrow \mathbf{1}$$

where the k_i are the lengths of the cycles of π and the r_k are the numbers of cycles of π of length k.

The centralizer $C_{\mathcal{S}_n}(\pi)$ of π has

$$\#C_{\mathcal{S}_n}(\pi) = \prod_{i=1}^{s} k_i \cdot \prod_{k=1}^{n} r_k!$$

elements.

Example. In $\mathcal{S}_n$ both permutations (13)(245) and (245) = (245)(1)(3) have a 6 element centralizer isomorphic with $\mathcal{Z}_3 \times \mathcal{Z}_2$. Its elements (in both cases) are the three different powers of (245) times the two different powers of (13).

Transpositions

A **transposition** is a cycle of length 2, that is a permutation that interchanges two elements and fixes all the other ones. The formula

$$(a_1\, a_2\, \ldots\, a_k) = (a_1\, a_k) \cdots (a_1\, a_3)(a_1\, a_2)$$

shows:

Lemma 3 *Each cycle of length k can be written as a product of $k-1$ transpositions.*

From this and Proposition 2 we conclude:

Corollary 2 *Each permutation π can be written as a product of $n-r$ transpositions where r is the number of cycles with more than one element in the cycle decomposition of π.*

Note that these transpositions need not be disjoint, therefore generally they don't commute, and the decomposition into transpositions is not unique. Even the number of transpositions is not unique; but at least we have:

Proposition 5 *If we write a permutation $\pi \in \mathcal{S}_n$ as a product of transpositions in different ways, then the number of transpositions either is always even or always odd.*

Proof. Let $\pi = \tau_1 \cdots \tau_s$ where the τ_i are transpositions. On the other hand let $\pi = \zeta_1 \cdots \zeta_r$ be the decomposition into disjoint cycles (complete, that means including all cycles of length 1). If we multiply π from the left with a transposition $\tau = (a\, b)$, we can distinguish two cases:

Case 1. a und b are in the same cycle. Because the cycles commute we may assume that this is the first one $\zeta_1 = (a_1 \ldots a_k)$, and $a = a_1$, $b = a_i$. Then $\tau\pi$ has the effect that

$$\begin{array}{rcccl}
a_1 & \overset{\pi}{\mapsto} & a_2 & \overset{\tau}{\mapsto} & a_2 \\
 & & \vdots & & \\
a_{i-1} & \mapsto & a_i & \mapsto & a_1 \\
a_i & \mapsto & a_{i+1} & \mapsto & a_{i+1} \\
 & & \vdots & & \\
a_k & \mapsto & a_1 & \mapsto & a_i
\end{array}$$

Therefore $\tau\pi = (a_1 \ldots a_{i-1})(a_i \ldots a_k)\zeta_2 \cdots$ (all other cycles unchanged).

Case 2. a and b are in different cycles. Assume that these are the first two $\zeta_1 = (a_1 \ldots a_k)$ and $\zeta_2 = (b_1 \ldots b_l)$, and $a = a_1$, $b = b_1$. Then $\tau\pi = (a_1 \ldots a_k\, b_1 \ldots b_l)\zeta_3 \cdots$.

In any case the number of cycles grows by 1 or decreases by 1, hence is $r \pm 1$. If we multiply with another transposition from the left, the total number of cycles becomes $r + 2$, r or $r - 2$. After multiplication with q transpositions we have $r + t_q$ cycles, where $t_q \equiv q \pmod 2$. Therefore the product $\tau_s \cdots \tau_1\pi$ has $r + t_s$ cycles where $t_s \equiv s \pmod 2$. But this is the identy map $\pi^{-1}\pi$ and therefore $r + t_s = n$. Hence $s \equiv n - r \pmod 2$, no matter what was the starting decomposition into transpositions. $\diamond$

The Alternating Group

If we assign to each permutation in $\mathcal{S}_n$ the parity of the number of transpositions in an arbitrary decomposition, then, by the last section, we get a well-defined function

$$\operatorname{sgn} : \mathcal{S}_n \longrightarrow \mathbb{F}_2,$$

that obviously is a group homomorphism into the additive group. We call the kernel the **alternating group** of order n and denote it by $\mathcal{A}_n$. The elements of $\mathcal{A}_n$, that is the permutations that decompose into an even number of transpositions, are called **even** permutations, the other ones **odd**. $\mathcal{A}_n$ is a normal subgroup of index 2 in $\mathcal{S}_n$ and therefore has $n!/2$ elements.

Involutions

Call a permutation an **involution**, if it has order 2 as a group element in $\mathcal{S}_n$, or alternativly, if its cycle decomposition consists of transpositions (and fixed points) only. An involution ist **proper**, if it has no fixed points. Of course this is possible only, if n is even. Then a proper involution is a product of $n/2$ disjoint 2-cycles (i. e. cycles of length 2).

A task that occurs in computing the total number of keys of Enigma, is determining the number of involutions in the symmetric group $\mathcal{S}_n$ that have exactly k 2-cycles where $0 \leq 2k \leq n$. It equals the number $d(n,k)$ of possibilities of choosing k pairs from n elements (where the order of the pairs does not matter).

Choose	**possibilities**	**choose**	**possibilities**
1st element: 1st partner:	n $n-1$	 1st pair:	 $n(n-1)/2$
2nd element: 2nd partner:	$n-2$ $n-3$	 2nd pair:	 $(n-2)(n-3)/2$
...	...	...	...
k-th element: k-th partner:	$n-2(k-1)$ $n-2(k-1)-1$	 k-th pair:	 $(n-2k+2)(n-2k+1)/2$

Adding all together and respecting the order we get

$$\frac{n(n-1)\cdots(n-2k+2)(n-2k+1)}{2^k} = \frac{n!}{(n-2k)!\cdot 2^k}$$

possibilities. If we now disregard the order we have always $k!$ identical choices. Hence we have shown:

Proposition 6 *The number of involutions in the symmetric group $\mathcal{S}_n$ that have exactly k 2-cycles is*

$$d(n,k) = \frac{n!}{2^k k!(n-2k)!} \quad \textit{for } 0 \leq 2k \leq n.$$

Example: In the case of the Wehrmacht Enigma we have $n = 26$ and $k = 10$, and the number of possible involutions is

$$\frac{26!}{2^{10}\cdot 10!\cdot 6!} = 150738274937250.$$

Products of Proper Involutions

The cryptanalysis of the Enigma by Rejewski involves products of two proper involutions σ and τ. Let $(a\,b)$ be a cycle of τ. If $(a\,b)$ is also a cycle of σ, then $\sigma\tau$ fixes the two elements a and b, hence has the two cycles (a) and (b) of length 1.

In the general case starting with an arbitrary element a_1 one finds a chain $a_1, a_2, a_3, \ldots, a_{2k}$ such that

$$\begin{aligned} \tau = &\quad (a_1\,a_2)(a_3\,a_4)\cdots(a_{2k-1}\,a_{2k}) \quad \times \text{ other 2-cycles},\\ \sigma = &\quad (a_2\,a_3)(a_4\,a_5)\cdots(a_{2k}\,a_1) \quad \times \text{ other 2-cycles}. \end{aligned}$$

In the product $\sigma\tau$ these become the two cycles

$$(a_1\, a_3\, \ldots\, a_{2k-1})(a_{2k}\, \ldots\, a_4\, a_2)$$

of length k. In particular all cycle lengths occur in an even number, the cycle type is **matched**.

Theorem 3 [Rejewski] *A permutation is the product of two proper involutions, if and only if its cycle type is matched.*

Proof. In order to prove the inverse direction we take a permutation π of matched type and give solutions σ, τ of the equation $\sigma\tau = \pi$.

In the simplest case, where π only consists of two cycles of the same length:

$$\pi = (p_1\, p_2\, \ldots\, p_k)(q_1\, q_2\, \ldots\, q_k),$$

an obvious solution is

$$\begin{aligned} \tau &= (p_1\, q_k)(p_2\, q_{k-1}) \cdots (p_k\, q_1), \\ \sigma &= (p_2\, q_k)(p_3\, q_{k-1}) \cdots (p_1\, q_1). \end{aligned}$$

In the general case we analogously construct the solution for each matching pair of cycles of the same length. ◇

Therefore the following procedure gives a decomposition of a partition of matched type into two proper involutions: Write cycles of the same length below each other, the lower one in reverse direction. Then read off the 2-cycles of τ by pairing the elements in the same column, and the 2-cycles of σ by pairing each element with the one diagonally to the left below it.

Example: Let $\pi =$ `(D)(K)(AXT)(CGY)(BLFQVEOUM)(HJPSWIZRN)`. Then we write down the scheme

```
(D)(AXT)(BLFQVEOUM)
(K)(YGC)(NRZIWSPJH)
```

and read off a solution of $\sigma\tau = \pi$:

τ = `(DK)(AY)(XG)(TC)(BN)(LR)(FZ)(QI)(VW)(ES)(OP)(UJ)(MH)`,

σ = `(DK)(XY)(TG)(AC)(LN)(FR)(QZ)(VI)(EW)(OS)(UP)(MJ)(BH)`.

It's also easy to find all solutions: Cyclically shift the lower cycles. If there are more then two cycles of the same length also consider all possible pairings. The solution is uniquely determined as soon as a 2-cycle of σ or τ is fixed for each cycle pair.

Exercise. Work out the formula for the number of solutions.