Rejewski's Theorem and the Theory of Permutations

Aaditya Rushabh Shah
Arjun Maneesh Agarwal

July 9, 2026

Theorem 1 (Rejewski's Theorem)**.** *The product of two proper involutions on the same elements can be expressed as a product of pairs of cycles of the same length.*

Theorem 2. *A permutation can be expressed as the product of two involutions without fixed points iff every cycle length occurs an even number of times.*

Lemma 1. *Given involutions X and Y such that they don't contain identical transpositions, we can decompose*

$$X = X_1X_2 \dots X_k, \qquad Y = Y_1Y_2 \dots Y_k$$

such that

$$X_i = (a_{i,1}a_{i,2})(a_{i,3}a_{i,4}) \dots (a_{i,2m_i-1}a_{i,2m_i})$$

and

$$Y_i = (a_{i,2}a_{i,3})(a_{i,4}a_{i,5}) \dots (a_{i,2m_i}a_{i,1}).$$

Proof. We provide the following algorithm to find this decomposition.

- Choose an arbitrary transposition in X and name it (a_1, a_2).
- Find the transposition in Y with a_2 and name it (a_2, a_3). Notice, $a_3 \neq a_1$ as the products don't contain identical transpositions.
- Find the transposition in X with a_3 and name it (a_3, a_4). And so on.
- After m_1 iterations, if we find (a_{2m_1}, a_1) in Y, we name

  $$X_1 = (a_1a_2)(a_3a_4) \dots (a_{2m_1-1}a_{2m_1})$$

  and

  $$Y_1 = (a_2a_3)(a_4a_5) \dots (a_{2m_1}a_1).$$

- Repeat the process with $X \backslash X_1$ and $Y \backslash Y_1$.

Notice, that $X \backslash X_1$ and $Y \backslash Y_1$ are still involutions on the same set of elements as we only got rid of the same $a_1, \dots, a_{2m_1}$ elements from both of them.

The algorithm terminates as every iteration of the loop reduces the number of elements in the involutions.

Correctness is obvious and follows immediately. □

Lemma 2. *For two given involutions X and Y defined on a set S, such that $|S| = 2n$,*

$$X = (a_1a_2)(a_3a_4)\dots(a_{2n-1}a_{2n})$$

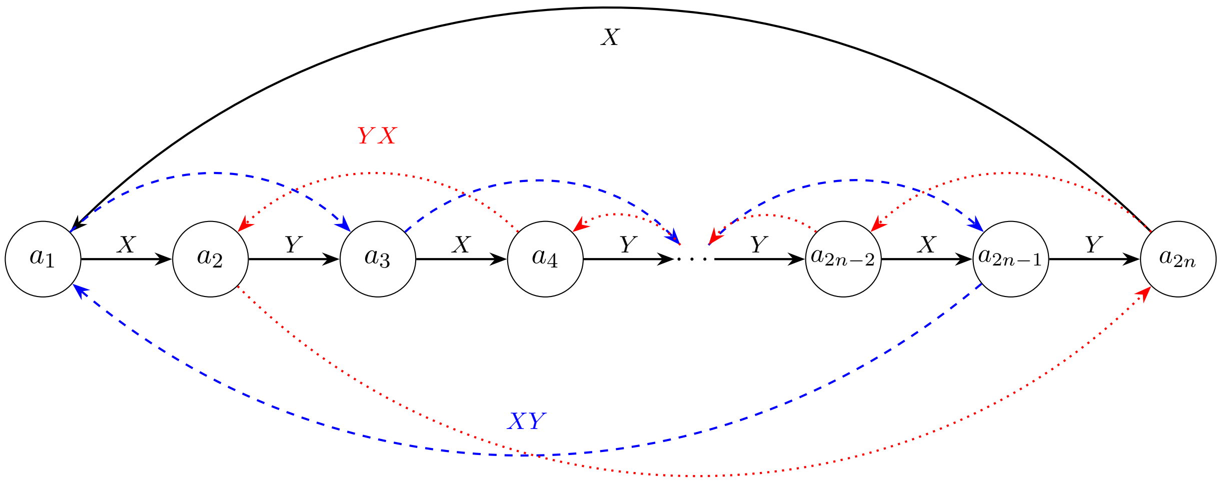
and

$$Y = (a_2a_3)(a_4a_5)\dots(a_{2n}a_1),$$

the product of X and Y will consist of two disjoint cycles of equal length n, that is given by

$$XY = (a_1a_3\dots a_{2n-1})(a_{2n}\dots a_4a_2).$$

Proof.



It can be seen from the above figure that product of X and Y will form two disjoint cycles of length n, such that

$$XY = (a_1a_3\dots a_{2n-1})(a_{2n}\dots a_4a_2).$$

□

Proof of Rejewski's Theorem. Let X and Y be two proper involutions defined on the set S, that is,

$$X : S \to S$$

is a permutation such that $X(X(a)) = a$ for all $a \in S$, and

$$Y : S \to S$$

is a permutation such that $Y(Y(b)) = b$ for all $b \in S$, both not having any fixed points and $|S| = 2n$.

Let us ignore the identical transpositions between X and Y to form X' and Y'.

Using Lemma 1, we can decompose X' and Y' into X_i''s and Y_i''s such that

$$X_i' = (a_1a_2)(a_3a_4)\dots(a_{2k-1}a_{2k})$$

and

$$Y_i' = (a_2a_3)(a_4a_5)\dots(a_{2k}a_1),$$

where $a_i \in S$ for all $i \in \{1, 2, \dots, 2k\}$ and $k \le n$.

Using Lemma 2, $X_i'Y_i'$ can be written as product of two cycles of length k, say C_iC_i' where

$$|C_i| = |C_i'|.$$

Thus,

$$\begin{aligned} X'Y' &= (X_1'X_2'\dots X_m')(Y_1'Y_2'\dots Y_m') \\ &= (X_1'Y_1')(X_2'Y_2')\dots(X_m'Y_m') \\ &= C_1C_1'C_2C_2'\dots C_mC_m'. \end{aligned}$$

Finally, notice that

$$(xy)(yx) = (x)(y).$$

Thus, product of identical transposition produces 2 singleton cycles of the elements of the transposition.

Thus, product of two proper involutions on the same elements can be expressed as a product of pairs of cycles of the same length. □

Proof of the generalized theorem. ($\Longrightarrow$) Same as Rejewski's Theorem.

($\Longleftarrow$) Given

$$P = C_1C_1'C_2C_2'\dots C_mC_m'$$

such that

$$|C_i| = |C_i'|.$$

We can find involutions X, Y that product up to P as follows:

- If

  $$C_1 = (a_1a_2\dots a_k)$$

  and

  $$C_1' = (b_1b_2\dots b_k),$$

  add to X the transpositions (a_ib_i) and to Y the transpositions (b_ia_{i+1}) along with (b_ka_1).

- Repeat.

This terminates as m is finite.

The correctness is implied by Lemma 2. □

References

[1] Rejewski, M. (1980). *An Application of the Theory of Permutations in Breaking the Enigma Cipher.*