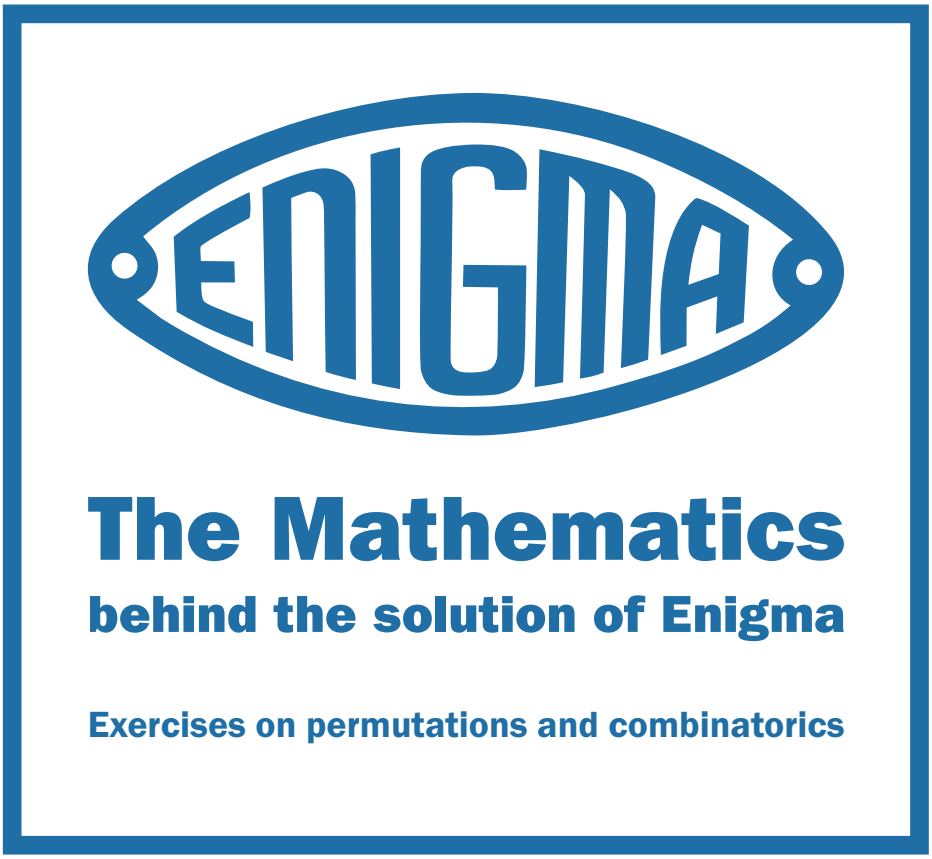


The Mathematics

behind the solution of Enigma

Exercises on permutations and combinatorics

Haderslev, 2008.

The mathematics which solved the Enigma machine

In this document we will be looking at the mathematics necessary to understand how the Polish mathematician *Marian Rejewski* in the late 1930's was able to break the codes of the german cryptomachine *Enigma*. Rather than writing everything out in detail, I have decided to make the necessary definitions from the theory of *permutations*, and then add a number of exercises in order for students from late high school or college to be able to write about this subject in a manuscript or major project, and in that way forcing the student to deliver a more personal contribution. This document is mainly meant as an instruction in reading the following article:

Chris Christensen. *Polish Mathematicians Finding Patterns in Enigma Messages*. Mathematics Magazine (Mathematical Association of America), Vol 80, No. 4, Oct. 2007.

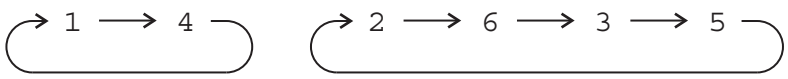
This article can be downloaded from my website. The whole idea behind the construction of Enigma was the desire to have an electro-mechanical device changing letters in a text in a systematic way, so that the result will be unreadable for the enemy. Therefore it is not a surprise that the mathematics involved is the theory of permutations. Some Combinatorics will be needed to calculate the number of combinations.

What is a permutation?

A permutation can be regarded as a map interchanging the elements of a given set. If this set is $\{1,2,3,4,5,6\}$, then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 2 & 3 \end{pmatrix}$$

is the permutation mapping $1 \to 4, 2 \to 6, 3 \to 5, 4 \to 1, 5 \to 2$ og $6 \to 3$. Another way of viewing the same permutation is to focus on images of images. Since the set is finite, it is always true, that after a while one will always end up with the starting element. A sequence generated in this way is called a *cycle*. In this case we get a 2-cycle and a 4-cycle, with the number referring to the number of elements in the actual cycle.



This explains why we sometimes write the same permutation in *cycle-form*:

$$(14)(2635)$$

It is often more convenient to work with the cycle-form: The image-element is just the next element in the cycle, unless we are at the end of the cycle, in which case the image is the first element in that cycle. The trivial permutation called the *identity* and denoted by *I* actually does nothing:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \quad \text{or} \quad (1)(2)(3)(4)(5)(6)$$

Given two permutations A og B:

$$A = (124)(365)$$
$$B = (16)(235)(4)$$

The *composite* of A and B is a new permutation defined in the following way: A maps 1 to 2 and B maps 2 to 3, hence AB maps 1 to 3. Continuing the same way yields

$$AB = (13)(246)(5)$$

It is important to point out that I have decided to follow Chris Christensen and Marian Rejewski in their choice to let compositions take place from left to right, that is, when writing AB then A is understood to be applied *before* B. There doesn't seem to be any convention in mathematics in favour of one way or the other. Some people prefer to let compositions take place from right to left, as is the case with functions and matrices.

We state without proof, that the *associative law* is valid for permutations, i.e. parentheses can be placed as desired: $(AB)C = A(BC)$.

Exercise 1

The *commutative law* is satisfied if the order of *any* two permutations in a composition doesn't matter: $AB = BA$. Prove by finding a counter example that the commutative law *doesn't hold* for permutations.

The *inverse* of a permutation A is defined as the unique permutation A^{-1} satisfying the following conditions:

(1) $$A^{-1}A = I \quad \text{og} \quad AA^{-1} = I$$

Exercise 2

Determine the inverse elements of the following permutations:

a) $A = (162)(3)(4,5)$

b) $B = (1)(2465)(3)$

c) $C = (123456)$

Exercise 3

a) What can be said about the lengths of the cycles of the inverse permutation in comparison with the original permutation?

b) Show that the inverse element of AB is $B^{-1}A^{-1}$, i.e. show that $(AB)^{-1} = B^{-1}A^{-1}$ by using definition (1) on the inverse permutation.

Given two permutations A and T. Then $T^{-1}AT$ is called the *conjugate element* of A by T. In the following we will be looking at an important property, which Marian Rejewski used heavily in his attack on Enigma, namely the fact that the cycle-structure, i.e. the lengths of the cycles, is preserved under conjugation.

Exercise 4

Assume that A contains the cycle $(a_1 a_2 \cdots a_r)$:

(2) $$A = (\ldots)\ldots(a_1 a_2 \cdots a_r)\ldots(\ldots)$$

Let T be another, arbitrary permutation. Show that $\big(T(a_1)T(a_2)\cdots T(a_r)\big)$ will then be a cycle contained in the conjugate permutation $T^{-1}AT$, i.e.

(3) $$T^{-1}AT = (\ldots)\ldots\big(T(a_1)T(a_2)\cdots T(a_r)\big)\ldots(\ldots)$$

Hint: What is the image of the permutation of $T^{-1}AT$ when applied to $T(a_1)$? The same question for $T(a_2)$, etc? Make use of the fact that $A(a_1) = a_2$, $A(a_2) = a_3$, etc.

Explain why the property in exercise 4 means that the cycle-lengths of A and $T^{-1}AT$ are equal in pairs – the permutations are said to have the same cycle-structure.

Later in this document we will be considering a *mini-Enigma* machine, which has 12 different letters: `a,b,c,d,e,f,g,h,i,j,k,l`, so the following exercises will be dealing with permutations of those 12 letters.

Exercise 5

Given the two permutations

$$A = \texttt{(akcj)(b)(dlf)(ehgi)}$$
$$T = \texttt{(ahib)(cd)(egjfkl)}$$

Calculate the conjugate element $T^{-1}AT$ of A. Can you confirm the statement in Exercise 4, that the cycle-structure is preserved under conjugation?

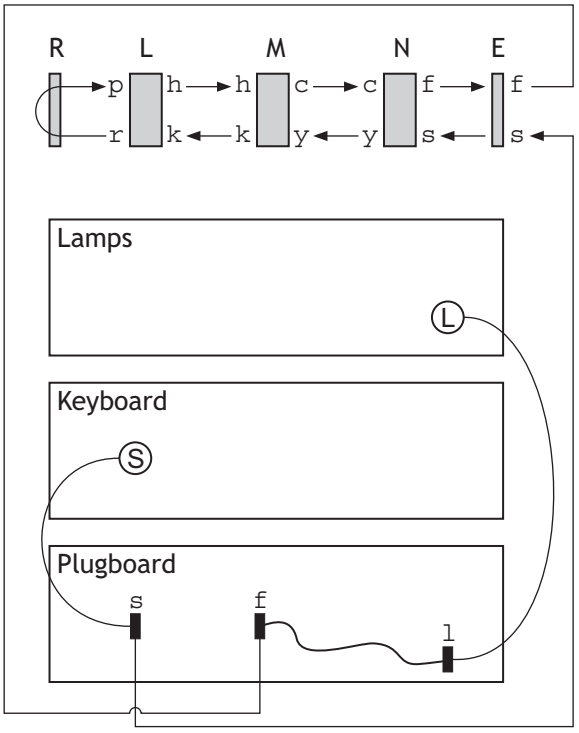
Making composites with the permutation itself a certain number of times yields the identity permutation I. The smallest positive integer n satisfying $A^n = I$ is denoted the *order* of the permutation A.

Exercise 6

Try to find a mathematical rule on how to calculate the order of a permutation given it's cycle-structure. Apply the rule on A = `(achbf)(di)(eklgj)`. What is the order of the permutation A?

In case you don't already know the function of Enigma, you can study it on the figure below. The key for letter `s` on the keyboard is pressed down, allowing for a signal to go to `s` in the plugboard. At the same time the right rotor *N* moves forward by one step. Since there is no plug in the letter `s`, the signal goes directly to the *Entry Wheel E*. Nothing happens in that wheel. However in each rotor *N*, *M* and *L*, the letters are permuted in accordance with the complicated interior wirings inside those wheels. The same happens in the *Reflector*, before the signal is returning back via a different path through the rotors and back to the plugboard in the letter `f`. Because a plug is connected to `f`, the signal is transferred to the letter `l` in the plugboard before finally the lamp `l` on the lampboard lights up.

Figur 1



In the following you are supposed to solve some of the combinatorial problems in order to find the overall number of different settings for the Enigma machine. In the article it is described on page 253-255.

Exercise 7

a) (*Plugboard settings*). Show that the number of possible plugboard settings when using *n* plugs, i.e. *n* connections in the plugboard, is given by the expression below. Binomial coefficients are being used. See also on page 253 in the article.

$$\frac{\binom{26}{2}\cdot\binom{24}{2}\cdot\binom{22}{2}\cdot\ \cdots\ \cdot\binom{26-2(n-1)}{2}}{n!}$$

b) Calculate the number of different plugboard settings for the different values of n between 1 and 13 (remember there are 26 letters, so up to 13 pairs are possible!). Which number of plugs yields the highest number of combinations?

c) (*Rotor arrangements*). Shortly before the beginning of the War only three different rotors were in use. They could be placed in every order desired. How many orders are possible? Later in the war the Germans used 5 different rotors, from which three had to be chosen. How many rotor arrangement orders do that give rise to, including the order of the rotors chosen?

d) (*Ring settings*). Each rotor has a ring containing 26 letters. This ring can be moved relative to the internal wiring of the rotor and one out of 26 possible settings is chosen by fastening the movable ring using a needle. On level with a specific letter on the ring is placed a fixed *notch*. When a pawl reaches that notch, the next wheel is advanced by one step. Only the notches on the first two rotors do add to the security of Enigma. How many ring settings can be said to exist? (See the article on page 254).

e) (*Rotor settings/ground settings*). Each of the three rotors has 26 possible starting positions, according to which of the 26 letters is on top. How many different rotor settings do that account for?

f) (*Total key number*). A *key* contains information about which rotors are being used and in what order, the ring settings, the ground settings of the wheels and the plugboard settings. How many keys are there in total, when we assume it was early in the war, when only three different rotors were in use and where only 6 plugs were used for the plugboard?

Exercise 8

Remember the Enigma machine is an electro-mechanical realization of a *poly- alphabetical substitution cipher*, like the *Vigenère cipher*. How many letters do one need to press before the Enigma machine repeats a permutation (or alphabet)? See the article page 251.

Each time pressing a letter on the keyboard, the first rotor N advances by one step. That way it is ensured that a new alphabet is being used when decrypting the next letter. In the following we need to represent the action that wheel N advances one step by using a permutation: P: `(abcdefghijklmnopqrstuvwxyz)`.

In the following let's assume we are dealing with a *mini-Enigma* machine containing 12 letters only. The permutation, representing the action that wheel N moves forward by one step is then given by: $P =$`(abcdefghijkl)`.

Exercise 9

Assume that the internal wiring of the first rotor N gives rise to the permutation:

N = (akcj)(b)(dlf)(ehgi)

Show that if you include the action of the wheel advancing one step, represented by the permutation P mentioned above, the combined action of the stepping forward and the effect of the wheel is represented by the permutation PNP^{-1}. Calculate the value of this composition in the actual situation. *Hint*: Use the result of exercise 4, observing that PNP^{-1} is a conjugation of N by $T = P^{-1}$ (Remember $(P^{-1})^{-1} = P$).

Exercise 10

Let's still work with the mini-Enigma machine with 12 letters. In the following it is assumed that wheel 2 and 3, i.e. M and L, don't move during the encryption, only the first wheel N moves! We also assume that 4 pairs of letters are connected with plugs in the plugboard, represented by the following permutation:

S: (ai)(bc)(d)(e)(fh)(gj)(k)(l)

The permutation moving the first wheel one step forward is represented by:

P: (abcdefghijkl)

The wirings inside the wheels can be represented by arbitrary permutations, say:

N: (alehbfcikj)(gd)
M: (a)(bikfd)(eghl)(cj)
L: (adgihljk)(bcef)

Remember that the reflector is acting as a permutation, consisting of six 2-cycles, say:

R: (ac)(bl)(de)(fk)(gi)(hj)

a) Calculate the composition $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$ representing the permutation associated with the first key-press. What is the image of a? *Hint*: For clarity, write out the permutations in the correct order below each other and apply the permutations in succession.

b) Show that $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1} = \left(SPNP^{-1}ML\right)R\left(SPNP^{-1}ML\right)^{-1}$. *Hint*: Use the result of exercise 3b).

c) The permutation representing the reflector R consists entirely of *transpositions*, i.e. 2-cycles. Use b) and the statement in exercise 4 to conclude, that also the permutation representing the first key-press consists entirely of 2-cycles. The same property applies of course to all the following key-presses!

d) Use c) to conclude that the Enigma machine is *self-reciprocal*, i.e. when typing the encrypted text on Enigma – using the same settings as when the text was decrypted – one get the plain text!

e) Explain why the property in d) was important for the Germans?

f) Why is it impossible for a letter to be encrypted into the same letter? This property was a severe weakness of Enigma and used by the people at Bletchley Park to break the daily code. *Hint*: Assume by contrast that one letter was encrypted into itself. Explain why that would imply the presence of a 1-cycle in the following permutation $SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$ associated with the first key press?

On page 257 in the article is mentioned the concept referred to as *depth*: When encrypting messages a whole day using the same key, the opponent receives a lot of statistics, because the first letter in the messages always are encrypted using the same alphabet that day. The same is true for the second letter of each message and so on. That's the reason why the Germans decided to apply *double* encryption. Besides applying the *daily key* delivered in German *codebooks*, every message was also encrypted using a *message key*. The message key consisted of three letters indicating the ground-settings of the rotors *N*, *M* and *L*. The plain text was first encrypted using the message key, the message key was then written twice and put in front of the decrypted message and finally the whole thing was encrypted using the daily key. When a German operator decrypted using the daily key from his codebook, he could read the message key as the first three letters in the document, say `nku`. He then adjusted the rotors, so the rotor *N* was in startposition `n`, rotor *M* in startposition `k` and rotor *L* in startposition `u`. Finally the plain text was achieved by decrypting the rest of the document using those settings! The Germans made just one fatal mistake: Because the reception of signals sometimes caused problems, they wrote the message key *twice*. This habit was one Rejewski immediately recogniced and used: Although he didn't know the message key `nkunku` he was sure that this whole day the 1st and 4th letter in the crypto text originated from the same letter! Same conclusion holds regarding 2nd and 5th letter and 3rd and 6th letter.

On page 257 in the article it is explained how Rejewski introduced six more permutations *A*, *B*, *C*, *D*, *E* and *F*. When pressing a key on the keyboard another letter lights up on the lamp board, depending on what key was pressed. This action can be described mathematically by a permutation: *A* is the permutation representing the first key press, *B* is representing the second key press, etc. Let *S* be the permutation associated with the action of the plugboard, and let *N*, *M* and *L* represent the action of the three rotors. Finally let *R* represent the permutation associated with the reflector. This means that *A* can be written in the following way, as indicated in exercise 10a):

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1} \tag{4}$$

Remark, that there are some errors in the article in the expressions for *A* and *D* on page 259. The author Chris Christensen has pointed this out to me. The expressions of the same quantities are however stated correctly later on page 265.

Exercise 11

Explain why *A* in (4) is the permutation representing the result of the first key press. *Hint*: Remember exercise 9.

In the same way the permutation representing the 4th key press can be expressed as:

$$D = SP^4NP^{-4}MLRL^{-1}M^{-1}N^{-1}P^4S^{-1}P^{-4} \tag{5}$$

Here P^4NP^{-4} is representing the action of the rotor after it has moved forward by 4 steps. Remember that the correctness of (4) and (5) only holds true under the assumption that only the first rotor moves during the key presses. If the notch on the first wheel activates the advancement of the second wheel, the above analysis is false. Fortunately this doesn't occur too often, since the alphabet contains 26 letters!

Exercise 12

a) Show using the technique from page 259 that:

$$AD = SP_1P_4S^{-1} \quad \text{where} \quad \begin{cases} P_1 = PNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1} \\ P_4 = P^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4} \end{cases} \tag{6}$$

Remember correcting the errors in the expressions for A and D on page 259 mentioned earlier. Explain each step in the computations on page 259.

b) Why are P_1 and P_4 independent of the plugboard setting?

c) Use (6) including the conclusion of exercise 4 to explain why the cycle-structure in the permutation AD is independent of the plugboard settings.

We still need to explain why the permutation AD from exercise 12 is important. It turns out that we can say something about this permutation, because the Germans wrote the message key twice! We need to go back to page 258: First however it needs to be emphasized that the Enigma machine is *self-reciprocal*, meaning that if the user types in the decrypted message using the exact same settings, he will get the plain text! This property was investigated in exercise 10d). This is of course a very simple decryption procedure and makes it especially convenient in the middle of the battlefield!

Exercise 13

Like on page 258, we assume the plain text `nkunku` for the message key is being encrypted as `JHNQBG`, using the daily key.

a) Explain why the permutation AD is mapping the first letter `J` into the 4th letter `Q`? *Hint*: Remember that Enigma is self-reciprocal, according to exercise 10d).

b) Explain how it is possible to reconstruct the entire permutation AD, if sufficiently many encrypted messages was intercepted during one single day?

When AD is completely known, the length of the cycles can be computed. Exercise 12c) proves that the cycle-structure is independent of the plugboard settings. Any changes in the plugboard connections will of course imply changes in the permutation, but the length of the cycles will be the same. This observation was a major victory for

Rejewski, since in reality it meant that he could "separate the plugboard from the rest of the machine". The plugboard had in fact been introduced by the Germans to tremendously increase the number of combinations in order to make a *brute force* attack on the machine practically impossible within a decent timeframe! Using mathematics the Pole had succeeded in finding a quantity (the cycle-lengths), which was *invariant* under any changes in the plugboard settings!

Exercise 14

Explain how Rejewski was able to use the cycle-lengths to find the daily key? (See page 259-261 in the article).

The mathematics described in this document is an important part of the tools used to break Enigma shortly *before* World War II. However Rejewski was also able to determine the inner wiring in each rotor, using mathematical arguments. That way he was able to construct a true copy of Enigma, without ever having laid hands on a real Enigma machine! You can read more about this on page 263-268. The reader is welcome to investigate this on his own.