5 The Control Logic of a Rotor Machine

We treat several approaches to rotor stepping. The first three are streamlined versions of real control mechanisms that in practice are implemented in a more complex way: the odometer, the gear drive with gaps, the gear drive with different number of cogs. We also treat the ultimate mechanism: the pseudorandom stepping, and a historical one: the HEBERN mechanism. For the stepping of the Enigma we refer to Chapter 6.

The insight that an irregular movement is the essential ingredient for a secure rotor machine is apparently due to FRIEDMAN after he broke he HEBERN machine. He himself, together with his collaborator ROWLETT, then in several steps developed the top-level rotor machine, the SIGABA.

Example 1: The Odometer Logic

The rotors step like in a mechanical counter or electricity meter. Assume the rotors are mounted as in Figure 4. The rightmost rotor moves by one position for each input letter. Each rotor, after completing one revolution, by some kind of protrusion makes its left neighbor move by one position.

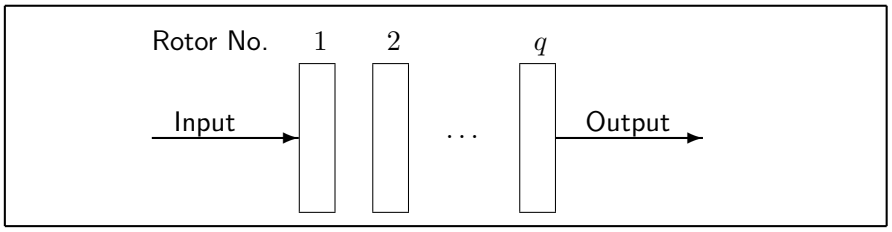

Figure 4: *Odometer logic*

Using the identification of the states with the integers mod n^q the sequence of states simply corresponds to the natural sequence of numbers beginning with the initial state.

Remarks

1. In this example the rightmost rotor, rotor number q, is a "fast" rotor, it moves with every step.
2. The leftmost rotor, number 1, is a "slow" rotor. It moves only after n^{q-1} steps, that is almost never, or only for very long messages. For this reason it makes little sense to use more then three rotors with odometer stepping. The effect of all additional rotors together only amounts to a fixed substitution. In the best case they could move once during encryption, effecting two different fixed substitutions.

3. Of course we could also implement the converse stepping where rotor 1 is fast and rotor q is slow.
4. The sequence of states has period n^q.

Example 2: Gaps

Figure 5 shows the principle of this control logic. For an implementation we have several mechanical options, for example a pin wheel.

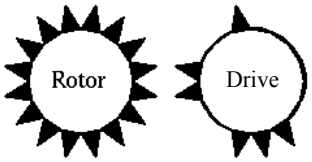

Figure 5: *Gear drive with tooth gaps*

A single wheel is characterized by a binary vector

$$u_{(j)} = (u_{j0}, \ldots, u_{j,t-1}) \in \mathbb{F}_2^t \quad \text{for } j = 0, \ldots, t-1$$

where t is the circumference of the wheel, not necessarily $t = n$. A 1 denotes a cog, a 0, a gap. We may describe all the wheels together by a binary matrix

$$u = \begin{pmatrix} u_{10} & \ldots & u_{1,t-1} \\ \vdots & \ddots & \vdots \\ u_{q0} & \ldots & u_{q,t-1} \end{pmatrix} \in M_{qt}(\mathbb{F}_2)$$

The column vectors

$$u^{(i)} = (u_{1i}, \ldots, u_{qi}) \in \mathbb{F}_2^q \quad \text{for } i = 0, \ldots, q-1$$

apply one after the other from left to right, cyclically repeated. This gives a sequence of period t for the states of the gear drive. The states of the rotors generally have a much larger period.

In the simplest case this logic steps the rotor j

- by one position, if $u_{ji} = 1$,
- not at all, if $u_{ji} = 0$,

for the i-th plaintext letter. This gives the formula

$$z^{(i+1)} = z^{(i)} + u^{(i)}$$

where addition is vector addition in $(\mathbb{Z}/n\mathbb{Z})^q$.

Another way to use gap wheels is turning them around a full turn in each step. Then the each of the rotors moves a number of steps given by the corresponding row sum in the matrix. This logic is equivalent with Example 3 below.

Example 3: Different Gear Wheels

Each rotor is driven by its own gear wheel. These share a common axis and make a full turn in each step. If wheel i has n_i cogs, then rotor i moves by n_i positions. The states occur with a period of $\operatorname{lcm}(n_1, \ldots, n_q)$.

The first models of Enigma (A and B) had a control like this.

Example 4: Pseudorandom Stepping

The rotor stepping is controlled by a (pseudo-) random generator, that is a mechanism or an algorithm that generates numbers indinguishable from pure random such as generated with the help of dice. This is easy for a computer simulation. For an (electro-) mechanical rotor machine one can use a key generating mechanism such as in one of the (later) HAGELIN machines.

FRIEDMAN was the first to detect the weaknesses of a regular rotor stepping when he analyzed the then current rotor machines in the 1920's. He came up with the idea of an irregular stepping by a pseudorandom mechanism. First he tried a punched paper tape, but this proved not robust enough. Then ROWLETT had the idea of realizing the stepping control by another set of rotors. Thus the American super rotor machine SIGABA was invented.

For details see the book

> Stephen J. Kelly: *Big Machines.* Aegean Park Press, Walnut Creek 2001, ISBN 0-89412-290-8.

Example 5: The HEBERN Machine

The HEBERN machine has $q = 5$ rotors and uses the standard alphabet with $n = 26$. The stepping follows an odometer logic, but with a complex mechanism that doesn't affect the neighboring rotor but another one, in more detail:

- Rotors 2 and 4 don't rotate at all. They are "stators".
- Rotor 5 moves by 1 position with every step, it is a fast rotor.
- Rotor 1 moves by 1 position with each complete turn of rotor 5. It is a "semi-fast" rotor.
- Rotor 3 moves by 1 position with each complete turn of rotor 1. It is a slow rotor.

Moreover the rotors move in the other direction compared with the description in Section 2.

The equation for the state change—not yet the correct one!—is

$$g(z_1, z_2, z_3, z_4, z_5) = (z_1 + \lambda(z_5), z_2, z_3 + \lambda(z_1)\lambda(z_5), z_4, z_5 + 1)$$

where $\lambda(x) = \delta_{x,25}$ is the KRONECKER symbol. The states occur with period $26^3 = 17576$.

Characteristic features:

- That the rotors 2 and 4 are static doesn't harm the security of the machine. By the odometer logic they would move only after 26^3 or 26^4 steps, that is only for extremely long messages.
- The stepping of rotor 1 (resp. 3) is induced by rotor 5 (resp. 1) moving from position "N" to position "O". The correct equation for the state change is left as an **exercise** to the reader.
- The wiring between the keyboard and rotor 1 as well as from rotor 5 to the light bulbs is irregular but static. It therefore is assumed as known to the enemy. We may interpret this wiring as two additional stators, one at each end of the rotor pack.
- For decryption there is a switch "direct/reverse" that interchanges input contacts and output contacts.
- The HEBERN rotors are symmetric: they may be mounted with their sides interchanged. This makes the number of possible primary keys larger by a factor of 2^5.