Unique configurations over the length of a crib

10th February 2020

Abstract

Brief summary of the paper.

1 Introduction

Definition 1.1 ($U_E(n)$)**.** For a given enigma E, and crib of length n, the amount of unique configurations when encrypting a string of length n is defined as $U_E(n)$.

2 Bounds on $U_E(n)$

Using l letters, the absolute worst upper bound we can get is from assuming that a rotor can have any orientation, and in the next step also have any other configuration. At any point in encryption, there are l^r possible positions for the rotors, looking at this over encrypting n letters we get

Theorem 2.1 (worst upper bound on $U_E(n)$)**.** *If E has r rotors, l wires per rotor, the worst upper bound for $U_E(n)$ is*

$$U_E(n) < n^{l^r}$$

Really, a terrible bound. A typical crib has 10 letters, and with a normal 3-rotor enigma we get $U_E(10) < 10^{26^3}$

If we use a longer crib, we will naturally get more configurations. But if the crib was large enough from before, we might get the same amount when increasing the size.

Theorem 2.2 (Bound on $U_E(n)$ relative to $U_E(n-1)$)**.** *If E has r rotors, l wires per rotor, the worst upper bound for $U_E(n)$ is*

$$U_E(n-1) \leq U_E(n)$$

If we look at cribs with length 1, we have that the amount of configurations over the crib is equal to the amount of possible rotor configurations of the enigma

Theorem 2.3 (lower bound on $U_E(n)$)**.** *If E has r rotors, l wires per rotor, the worst upper bound for $U_E(n)$ is*

$$U_E(n) \geq U_E(1) = l^r$$

We tighten the bound by realising that from any configuration, the next configuration moves its fast rotor, but only occasionally any of the other rotors, and if any other than the fast rotors move there are at most two other rotors moving. So in general stepping from one configuration to the next, there are only r possible next configurations(rotor 1, rotor 2, rotor 2 and 3, rotor 3 and 4, rotor 4 and 5, ..., rotor r and rotor r-1)(note that that there is only a single rotor step for rotor 1 and 2, this is due to the double stepping procedure)

Theorem 2.4 (upper bound on $U_E(n)$)**.** *If E has r rotors, l wires per rotor, the worst upper bound for $U_E(n)$ is*

$$U_E(n) < (r^n)l^r$$

With 4 rotors and 26 letters we get $U_E(10) < 4^{10}26^3 = 18429771776$ still, very much a lot.

We can tighten the bound further. When a rotor steps the other rotors steps according to where the notches are. If we look at the configuration as the rotor steps, as soon as any of the other rotors also stepped we have locked down where the notch is, from here on out there is only a much narrower stepping pattern available for that rotor. The problem however, is finding out how this pattern affects the amount of unique configurations.

2.1 template stuff

Full proofs, numerical implementations.

Theorem 2.5 (Pythagoras)**.** *In a right triangle, the square of the hypotenuse is equal to the sum of the squares of the other two sides. That is,*

$$a^2 + b^2 = c^2, \tag{1}$$

where c is the length of the hypotenuse and a and b are the lengths of the two other sides.

Proof. Draw a figure. ■

3 Conclusions

Optional. Results, consequences, future work.

Table 1 lists some integers satisfying Equation (1) of Theorem 2.5.

a	*b*	*c*
3	4	5
65	72	97

Table 1: Some interesting numbers