图灵机

- 为什么在图灵机中不方便用二进制表示一个数?

以 $4 = (100)_2$ 为例：后面还会有多的 0，因此无法确定是 4 还是 8 还是.....

如果要用二进制表示，那么需要再引入一个字符（`*`）来表示数字的结束。

相反如果使用 unary 表示，用 1 的个数来记录答案，用 0 来分割数字与数字，就不会遇到上述的问题。

这种表示方式在表示很大的数的时候效率会很低。但是实现功能还是没问题的。

- $BB(5)$，$BB(n)$ 函数代表什么?

考虑所有 n 个状态，单条纸袋，字符集为 2 并且会停机的图灵机，在停机前运行次数最大的那个图灵机的运行次数被称为 $BB(n)$

目前人类只确定了 $BB(5)$ 的数值，$BB(n)$ 目前还是不可计算数。

密码机

加密方法:

加密的本质：构造一个映射：$DA \to DB$

单表代替密码：最简单的是凯撒密码，但是只有 26 种可能的情况，太容易被破解。若是简单的将每个字母对应一个新的字母，那么刚好有 $26!$ 种排列，看起来很难破译。

然而可以通过频率分析法，通过高频词来反推：如 `and` 和 `the` 很可能出现多次，那么他们对应的加密也会出现多次，那么就可以猜测那些出现多次的单词是某些单词，这样就能够反推映射，然后暴力判断是否正确。

多表代替密码:

单表代替密码的弱点在于原文中自然语言的特征在密文中也会被保留。

因此使用多表代替：使用一个表格，每行对应一个映射，然后不同的位置用不同的表。比如：第 i 位用第 $i \mod p$ 张表来映射，p 是行数。

因此，频率法就失效了，这也被称为"不可破译的密码"。

用密码机加密与破译密码

用机械的手段加密，大大提高了效率，在二战时期（由于无线电大家都听得到）被广泛运用。

Enigma 密码机：运用前面所说的多表代替密码，通过转子来实现多表的操作。

此外还有一个反射器，连接键盘和显示器中的相同字母，用来方便解码过程。反射器的副作用是让一个字母不会被加密成自己。

Enigma 在二战时期被德国运用，一度被认为是不可破译的。然而后来，盟军发现原文的密钥就在电报的开头并且为了避免误操作会被重复两次。（当然，原文的密钥也是会事先被另外一个每天不同的约定好的密钥来加密过，因此重复两次的密钥结果是不同的）。这意味着，在收集了足够多的电报之后，能够得到若干信息：两个密文对应的原文是相同的。

最后能够通过这个方法来破译。