计算机科学的伟大思想 笔记

The Busy Beaver Problem

如果在图灵机上有 n 个状态，且必须能够停机，问这个图灵机最多可以制造多少个 1 ？

Q : $BB（n）=?$

考虑 $n=1$, $BB(1)=1$;

考虑 $n=2$, $BB(2)=6$;

考虑 $n=3$, $BB(3)=14$;

n 更大的时候 , $BB(n)$ 将会爆炸式增长。

课后查阅资料：
如果暴力求解 $BB(n)$ 的值，则其复杂度为 $(4n+4)^{2n}$
$BB(47)$ 可能对证明哥德巴赫猜想有帮助。

密码机

单表系统

定义：单表代换密码是一种通过代换表将明文中的每个字符替换为密文中的对应字符来实现加密的方法。

设26个字母构成的集合为A，现在建立$f:A\to A$ 的双射

(凯撒密码： 可能性 $m=26$)

f 理论上有 $26!$ 种可能

一个映射就是一个置换群，它可以视为多个 Cycle Group 的乘积

频率分析法： 根据文章在不同领域的高频词汇进行猜测。

多表系统

多表替换密码是古典密码中的一种加密方法，通过使用一系列（两个以上）代换表依次对明文消

息的字母进行替换。

ENIGMA机

历史：一战时期由德国人 Auther Scherbius 发明. 在 1920 年后投入商业化使用。

在键盘上按下一个键，另一个键盘对应位置的灯将会亮起,从而完成加密。