计算机伟大思想第八周笔记

图灵机

图灵机表示数的两种方式

1. 一进制存储，数字是几就存几个 1 。 如 $4=(1111)$.
2. 二进制存储，使用二进制来存储数。如 $4=(100)$.

两者优缺点:

一进制更清晰易懂，更易操作，但是存储空间大。

二进制使用空间小，但是停止边界存在问题，如 $4=(100)$, 最后位置是 0 ,我们不知道停止位置在何处。

二进制解决方式： 为了防止边界条件的问题，我们在结束位置加上 * ，这样就知道在哪里停了。

忙碌的海狸

在计算机科学中，**忙碌的海狸**（Busy Beaver）是一个在给定参数后，寻找可能产生的最大输出的可终止程序。忙碌的海狸游戏包括设计一个可终止的，只输出0或1的图灵机，让其在一条纸带上尽可能多的输出1。

包含两个状态的忙碌的海狸游戏有下面两条规则：

1. 该图灵机包括除终止态以外的两个状态
2. 纸带初始值都是0

玩家需要设计出可能输出最多1的状态转换表格，同时也要确保图灵机是会终止的。

能赢得n个状态的忙碌的海狸游戏的图灵机，称为第n个忙碌的海狸，或者用BB-n表示(BB是英文忙碌的海狸的缩写)。BB-n，是在所有n个状态的图灵机里面，可以输出最多的1的。比如BB-2，可能通过6次状态转换输出4个1。

忙碌的海狸函数

忙碌的海狸函数，又称为BB函数，或者Radó Sigma函数，记做$\Sigma(n)$或者BB(n),是n个状态的忙碌的海狸图灵机的最大输出。这一个增长特别快的函数，是一个非常著名的不可计算函数。Radó证明了这个函数最终会超过全部的可计算函数。

$\Sigma(n)$还可以定义为集合$T=\{n_1,n_2,\cdots,n_k\}$中最大的数，这个集合包括了n个状态的2色图灵机全部的输出。集合T的大小不超过$(4n+4)^{2n}$（这是n个状态的全部图灵机数量)。

更普遍的 $\Sigma(n,m)$表示n个状态，m个颜色的忙碌的海狸图灵机。

2022年最新成果，算出来 $BB(5)$。

密码机

单表系统 Mono-alpha

典例：凯撒密码。

单表系统的万能破解方法：frequency_analysis 频率分析法，通过频率分析，高概率出现的单词容易出现，然后对应自身单词出现次数较高的单元，进行猜测排除破解，如英文中 e 出现频率高。

多表系统

在一个多表替换密码中，会使用多个字母作为密码。为了加快加密或解密速度，所有的字母通常写在一张表格上，密码学上称作**tableau**。这种表格通常是26×26，因为这样才能放下全部26个英文字母。填充表格及选择下次使用的字母的方法，就是不同多字母替换密码之间的定义。多字母替换密码比单字母更难打破，因为其替换可能性多，密文要较长才可。

其中最著名的一种为吉奥万·巴蒂斯塔·贝拉索于1585年推出的维吉尼亚密码。它于1863年之前一直未被破解。法国人称它作“不能破译的密码”
