伟大思想上课笔记

图灵机存储数字的两种方式

二进制vs一进制

一进制存储数字

一进制（Unary system）是一种极为简单的数值表示方法，在这种表示方式中，每个数字都通过重复的符号来表示。例如，数字 5 用 5 个符号（如 `1`）表示，数字 10 用 10 个符号表示。

优点：

1. **简单直观：** 由于一进制就是直接通过重复符号表示数字，因此它的表示方法非常简单，理解起来没有难度。

缺点：

1. **存储效率低：** 一进制的主要缺点是存储非常低效。对于较大的数字，需要使用大量的符号。比如，表示数字 100，需要在带上写下 100 个符号（例如 `1`），这会浪费大量带上的空间。
2. **计算效率低：** 在图灵机中进行数字的加法、乘法等运算时，一进制的处理速度会非常慢。例如，进行加法时，如果需要将两个数字相加，就必须重复地将符号数目增加，操作量大。

二进制存储数字

二进制（Binary system）是计算机中最常用的数值表示方法，每个数字通过 `0` 和 `1` 的组合来表示。图灵机也常用二进制来表示数字。

优点

1. **存储效率高：** 二进制可以用极少的符号来表示数字。例如，数字 5 用 `101` 来表示，只需要 3 个符号，而数字 100 用 `1100100` 来表示，只需要 7 个符号。相比于一进制，二进制的存储效率显著提高。
2. **运算效率高：** 图灵机在进行加法、减法等运算时，二进制数的加法和进位机制较为简单，适合自动化处理。计算机体系中广泛采用二进制运算，因为加法和乘法可以通过位移和简单的逻辑运算来实现。

缺点：

边界问题例如4 = （100）最后位置是0，我们不知道停止在何处。
二进制的解决办法，在结束位置加上就知道在哪里停止了

忙碌的海狸

在计算机科学中，“忙碌的海狸”（**Busy Beaver**）是一个与计算理论相关的概念，具体指的是图灵机的一个极端例子。它描述了一种特殊的图灵机，它能够在其输入带上尽可能多地写下符号并停机，同时其运行时间和写入符号的数量不超过任何其他图灵机。忙碌的海狸是一个与**图灵机停机问题**相关的重要话题，通常用来研究**计算复杂性**和**不可计算性**。

特点：

- **极端性质**：忙碌的海狸函数在 n 增加时增长得非常快，比任何标准的计算函数都要增长得快。
- **不可计算性**：忙碌的海狸函数的值对于任意的 n 是不可计算的。这是因为对于图灵机来说，停机问题本身就是不可解的，因此无法提前知道一个图灵机是否会停机或它在停机之前会写入多少符号。
  换句话说，给定一个有 **n** 个状态的图灵机，忙碌的海狸函数给出了这个图灵机所能写入的最大符号数，前提是该图灵机最终会停机。

忙碌的海狸函数

忙碌的海狸函数（**Busy Beaver function**）是计算机科学中的一个极限函数，主要用于图灵机理论中，尤其是计算图灵机在给定状态数下能够执行的最“繁忙”行为。它定义为，对于一个有 **n** 个状态的图灵机，在其带上从空带开始运行时，能够写下的最大符号数，同时要求该图灵机最终停机。
例如**BB(1)**: 对于一个只有 1 个状态的图灵机，最多能写入 1 个符号。
随着状态数 **n** 的增大，**BB(n)** 的值增长极其迅速，甚至超出大多数计算函数的增长速度。事实上，**忙碌的海狸函数**是一个**超指数增长**的函数。
由于其不可计算性，我们无法通过传统的算法来计算出任意 **n** 对应的 **BB(n)** 的确切值。通常，计算 **BB(n)** 需要通过实验和枚举所有可能的图灵机程序并验证其输出。

密码机

单表系统
单表系统是一种使用单一的字母替换表的加密方式，在该系统中，每个明文字符总是被替换为一个固定的密文字符。换句话说，在单表系统中，每个字母都用一个固定的密文字母代替，且替换关系对整个加密过程都是一致的。
一个常见的单表密码是**凯撒密码**。例如，在凯撒密码中，每个字母都被替换为字母表中向后偏移固定位置的字母。假设偏移量为 3，那么：

- 明文字母 `A` 被替换为密文字母 `D`。

- 明文字母 `B` 被替换为密文字母 `E`，依此类推。
  缺点：
- 容易受到**频率分析攻击**。因为每个明文字母总是对应同一个密文字母，攻击者可以通过分析密文中各个字母的出现频率，推断出一些常见字母（如英语中的 `E` 或 `T`），从而破解密文。
  多表系统
  多表系统（也叫做多字母替换密码）在加密时使用多个不同的替换表，而不仅仅是一个。这意味着同一个明文字符在不同的位置可能会被替换为不同的密文字符，从而增加了密码的复杂度。

典型案例：维吉尼亚密码（Vigenère Cipher）

维吉尼亚密码使用多个凯撒密码表，每个字母的替换位置由密钥决定。假设密钥是“KEY”，那么明文中的每个字母都与密钥的字母一一对应，使用不同的替换规则：

- 明文 `HELLO`，密钥 `KEYKEY`。
- 根据维吉尼亚表，将每个字母根据密钥字母的偏移量进行替换。例如：
  - `H` 用 `K` 对应的偏移进行替换，变成 `R`。
  - `E` 用 `E` 对应的偏移进行替换，变成 `I`，以此类推。