1 Secret Sharing

1.1 秘密共享

Secret Sharing：将秘密分成若干份，分发给不同的用户。用户特定子集共同提供各自的份额，才能重构初始秘密。

Treshold Scheme(t, n) : 在 n 人之间共享秘密，其中任意 $t \leq n$ 个人可求出秘密，任意 $t-1$ 个人无法求出秘密。

1.2 Combinatorial Mathematics

问题：Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

采用组合数学的方法："少数"与"多数"：

1. 设相关人共有 $2n+1$ 个，任意 n 人组成的"少数"团体不能打开安全门，任意 $n+1$ 人组成的"多数"团体可以打开安全门
2. 两个不同的"少数"团体联合必包含某个多数团体
3. 任一"少数"团体和不属该团体的任一人联合可成为多数团体

用数学上集合的语言来表述：给锁编号 $1, 2, \cdots, l$，打开所有门的钥匙的全集即为 $K = 1, 2, \cdots, l$，任意第 i 人拥有的钥匙集合为 S_i，则满足：

(1) $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_n} \subset K/k_i$

(2) $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_n} \cup S_{i_{n+1}} = K$

则有：

1. 那么对于不同的 n 的并，所对应的 k_i 不同，任意一个 k_i 必有一族 $\{i_1\ i_2, \cdots i_n\}$ 与之对应则 $k_i \in K$ 共有 C_{2n+1}^{n} 个
2. $k_i \in S_{i_{n+1}}$，这样的 k_i 有 C_{2n+1}^{n+1} 个