HWK7

11.2-3 成功查找：相同 $\Theta(1+\alpha)$

不成功查找：更快 但仍然为 $\Theta(1+\alpha)$

插入：更慢 仍 $\Theta(1+\alpha)$

删除：相同 $\Theta(1)$

11-4 a. 如果H为全域

则对于2个不同关键字 (x_1, x_2)，$(h(x_1), h(x_2))$ 为 m^2 个长度为2的序列中的任意一个的可能性相同.

则 $h(x_1)=h(x_2)$ 的概率为 $\frac{1}{m}$

∴ H为全域的.

b. 要证H全域，即证对于两个不同的n元组 x, y

$h(x)=h(y)$ 的概率不大于 $\frac{1}{p}$

$$h(x)=h(y) \Leftrightarrow \left(\sum_{i=0}^{p-1} a_i x_i\right) \bmod p = \left(\sum_{i=0}^{p-1} a_i y_i\right) \bmod p.$$

$$\Rightarrow \underbrace{\sum_{i=0}^{p-1} a_i (x_i - y_i) \bmod p = 0}_{\text{设为 } A}.$$

x 不等于 y 则 $\exists k \in \{0, \dots, p-1\}$, $x_k \neq y_k$.

设 $C=(a_k(x_k-y_k) \bmod p)$

设随机变量 $X=(A-C \bmod p)$

$Y = A \bmod p$.

$$\therefore Pr\{Y=i\} = \sum_{j=0}^{p-1} Pr\{X=[(i-j) \bmod p]\} \cdot Pr\{C=j\}$$

易知 $Pr\{C=j\} = \frac{1}{p}$

$$\therefore Pr\{Y=i\} = \frac{1}{p} \sum_{j=0}^{p-1} Pr\{X=[(i-j) \bmod p]\}$$

由于涵盖了 X 的所有的取值

$\therefore P_r\{Y=j\} = \frac{1}{p}\cdot 1 = \frac{1}{p}$

$\therefore P_r\{Y=0\} = \frac{1}{p}$

$\therefore$ H 是全域的.

而对 $x=(0,0,\dots,0)$. $\forall a\in U$ $h_a(x)=0$

$\therefore$ H 不是2全域的.

C. H 共有 p^{n+1} 个函数.

令 $x,y\in U$, $x\neq y$, 对 $\forall d_x, d_y\in Z_p$:

$$\begin{cases} \sum_{i=0}^{n-1} a_i x_i + b = d_x \pmod p \\ \sum_{i=0}^{n-1} a_i y_i + b = d_y \pmod p \end{cases}$$

在 Z_p 中解这个方程组, 由于 $x\neq y$, 则方程组增广矩阵的秩为2,

所以自由变量有 $n-1$ 个. 所以有 p^{n-1} 组解

所以 H 中有 p^{n-1} 个函数使得 $h'_{ab}(x)=d_x$ $h'_{ab}(y)=d_y$

$P(h'_{ab}(x)=d_x, h'_{ab}(y)=d_y) = \frac{1}{p^2}$

$\therefore$ H 为2全域.

d. 由于 H 为2全域的

对于 $\forall h\in H$. (m,m'), $P\{h(m)=t\cdot h(m')=t'\} = \frac{1}{p^2}$

此时已知 $h(m)=t$

则 $P\{h(m')=t'\} = \frac{1}{p}$

$\therefore$ 成功欺骗的概率至多为 $\frac{1}{p}$.