Homework 11

孙锴

June 6, 2012

练习(7.6). 对于任意互不相等的$x_1, x_2 \in \{1, 2, \ldots, m\}$，任意的$z_1, z_2 \in \{0, 1, 2, \ldots, M\}$，都有
$Prob(h(x_1) = z_1 \wedge h(x_2) = z_2) = \frac{1}{(M+1)^2}$
所以$Prob(h(0) = 0) = \sum_{i=0}^{M} Prob(h(0) = 0 \wedge h(1) = i) = (M+1)\frac{1}{(M+1)^2} = \frac{1}{M+1}$。
同理，对于任意$x \in \{1, 2, \ldots, m\}, z \in \{0, 1, 2, \ldots, M\}$，都有$Prob(h(x) = z) = \frac{1}{M+1}$。

练习(7.7). *(a)*不是。因为若有$h(x) = u, h(y) = v\ (x \neq y)$，则由此可得

$$\begin{pmatrix} x & 1 \\ y & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}\ (mod\ M)$$

所以a, b可以唯一确定，因此在此基础上$h(z)\ (z \neq x, y)$的值是确定的。
所以，取$x = x_0, y = y_0, z = z_0, u = u_0, v = v_0$（$x_0, y_0, z_0$为$\{0, 1, \ldots, p-1\}$中任意互不相等的定值，$u_0, v_0$为$\{0, 1, \ldots, p-1\}$中任意定值），设由$x_0, y_0, u_0, v_0$确定的$a = a_0, b = b_0$，取$w = w_0$，其中$w_0 = a_0 z_0 + b_0\ mod\ p$。则
$Prob(h(x_0) = u_0 \wedge h(y_0) = v_0 \wedge h(z_0) = w_0) = Prob(h(x_0) = u_0 \wedge h(y_0) = v_0) = \frac{1}{p^2} \neq \frac{1}{p^3}$，从而$h_{ab}$构成的集合不是$3-universal$。
(b)$\{h_{abc} = ax^2 + bx + c\ mod\ p | 0 \leq a, b, c < p\}$，其中$p$为质数。
下面做简要证明：
对于任意互不相等的$x, y, z \in \{0, 1, \ldots, p-1\}$，任意$u, v, w \in \{0, 1, \ldots, p-1\}$，满足$h(x) = u, h(y) = v, h(z) = w$当且仅当

$$\begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} u \\ v \\ w \end{pmatrix}\ (mod\ M)$$

易见等式中的矩阵是对范德蒙矩阵进行若干列交换所得，因此其可逆。从而有且只有一组a, b, c满足上述等式。
因此当a, b, c为随机值时，$Prob(h(x) = u, h(y) = v, h(z) = w) = \frac{1}{p^3}$。

练习(7.8). （以下讨论均设定义域为$\{0, 1, 2, \ldots, m-1\}$ $(m \geq 2)$）
实际上只需取集合$\{h_a(x) = a | 0 \leq a < m\}$。但是考虑到这个例子中的哈希函数过于糟糕，因此下面给出另一个例子：
$\{h_{ab}(x) = ax + b \, mod \, 2p | 0 \leq a, b < 2p\}$，这里$p$是一个质数。
接下来说明这个例子不是*2-universal*的。
对于任意互不相等的x, y，设$A = \{(a, b) | ax + b = 0 \wedge ay + b = 0 \, (mod \, 2p)\}$，则$P(h(x) = 0 \wedge h(y) = 0) = \frac{|A|}{4p^2}$。下面计算$|A|$，显然满足$ax + b = 0$的$(a, b)$的集合为$\{(0, 0), (1, -x), (2, -2x), \ldots, (2p-1, -(2p-1)x)\} \, (mod \, 2p)$，满足$ay+b = 0$的集合为$\{(0, 0), (1, -y), (2, -2y), \ldots, (2p-1, -(2p-1)y)\} \, (mod \, 2p)$，从而$|A|$等于满足在模$2p$意义下$-kx = -ky$ $(0 \leq k \leq 2p-1)$的k的个数，不难得出$(x - y)$为偶数时，满足条件的k有*2*种，$(x - y)$为奇数时，满足条件的k有*1*种，从而可取$x = 0, y = 2$，则得到$P(h(0) = 0 \wedge h(2) = 0) = \frac{1}{2p^2} \neq \frac{1}{4p^2}$，从而证明了这个例子不是*2-universal*的。

练习(7.10). 设期望的翻转次数为E，则
$E = p + 2(1-p)p + 3(1-p)^2 p + \ldots$
$(1-p)E = (1-p)p + 2(1-p)^2 p + \ldots$
两式相减，得$pE = p + (1-p)p + (1-p)^2 p + \ldots = 1$，从而$E = \frac{1}{p}$。

练习(7.12). 考虑序列$0, 0, 0, 0, 1, 2, 3, 4, 5$，则用给出的算法所得的答案是*5*，而真正的众数是*0*。