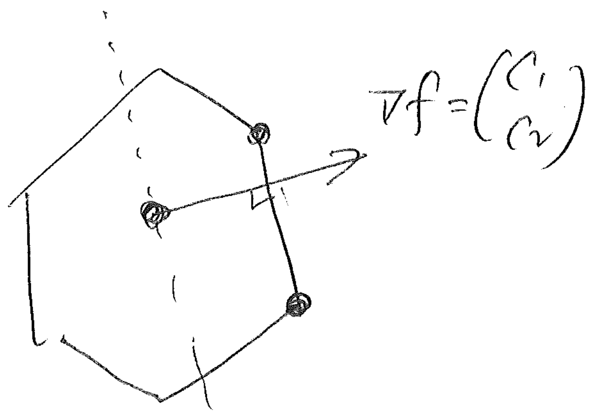
April 14

2D LP

$$\max \quad c_1x_1 + c_2x_2$$

s.t.

$\vdots$

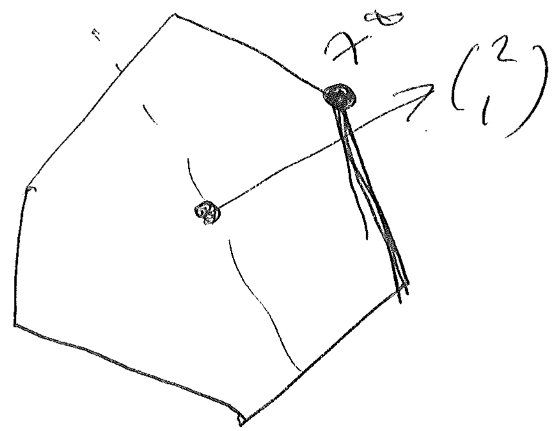


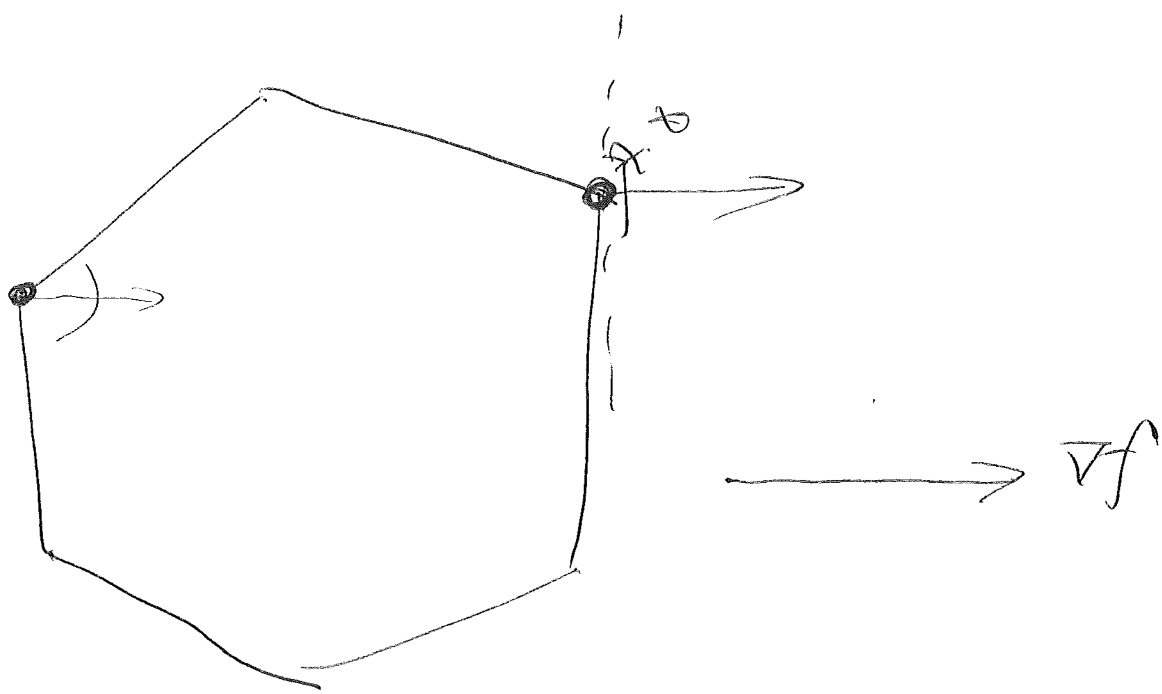
$$\max \quad 2x_1 + x_2$$

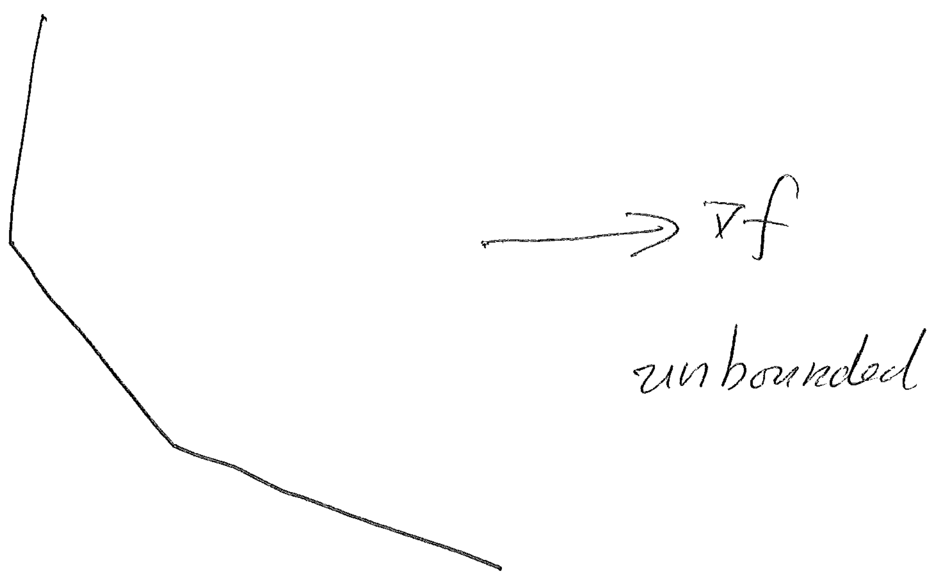
s.t. $2x_1 + 3x_2 \le 12$

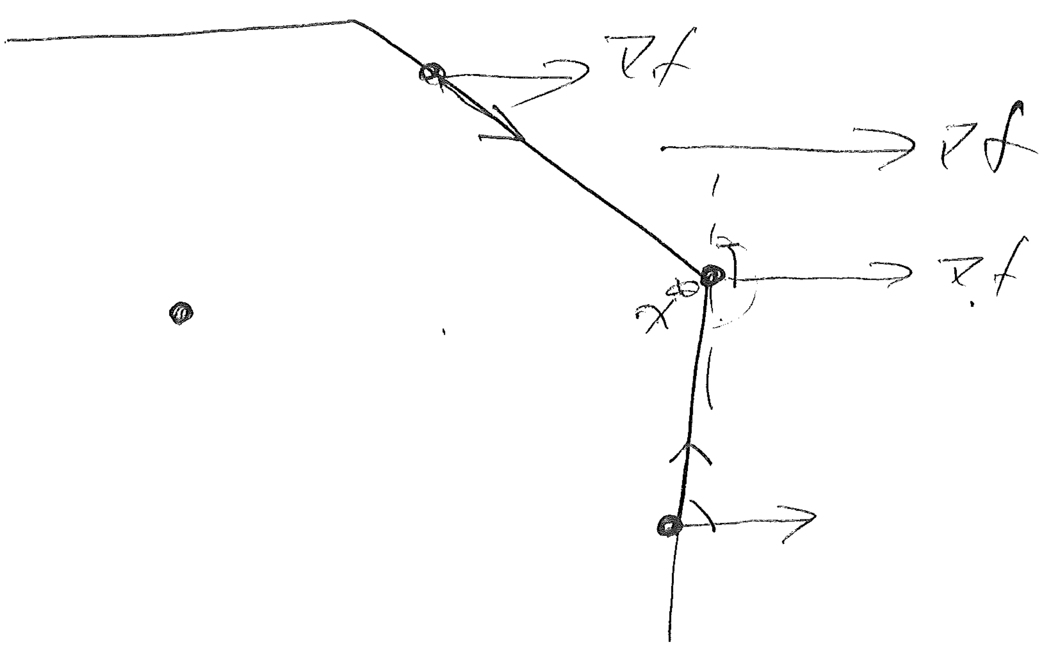
$5x_1 + 6x_2 \le 5$

$\vdots$

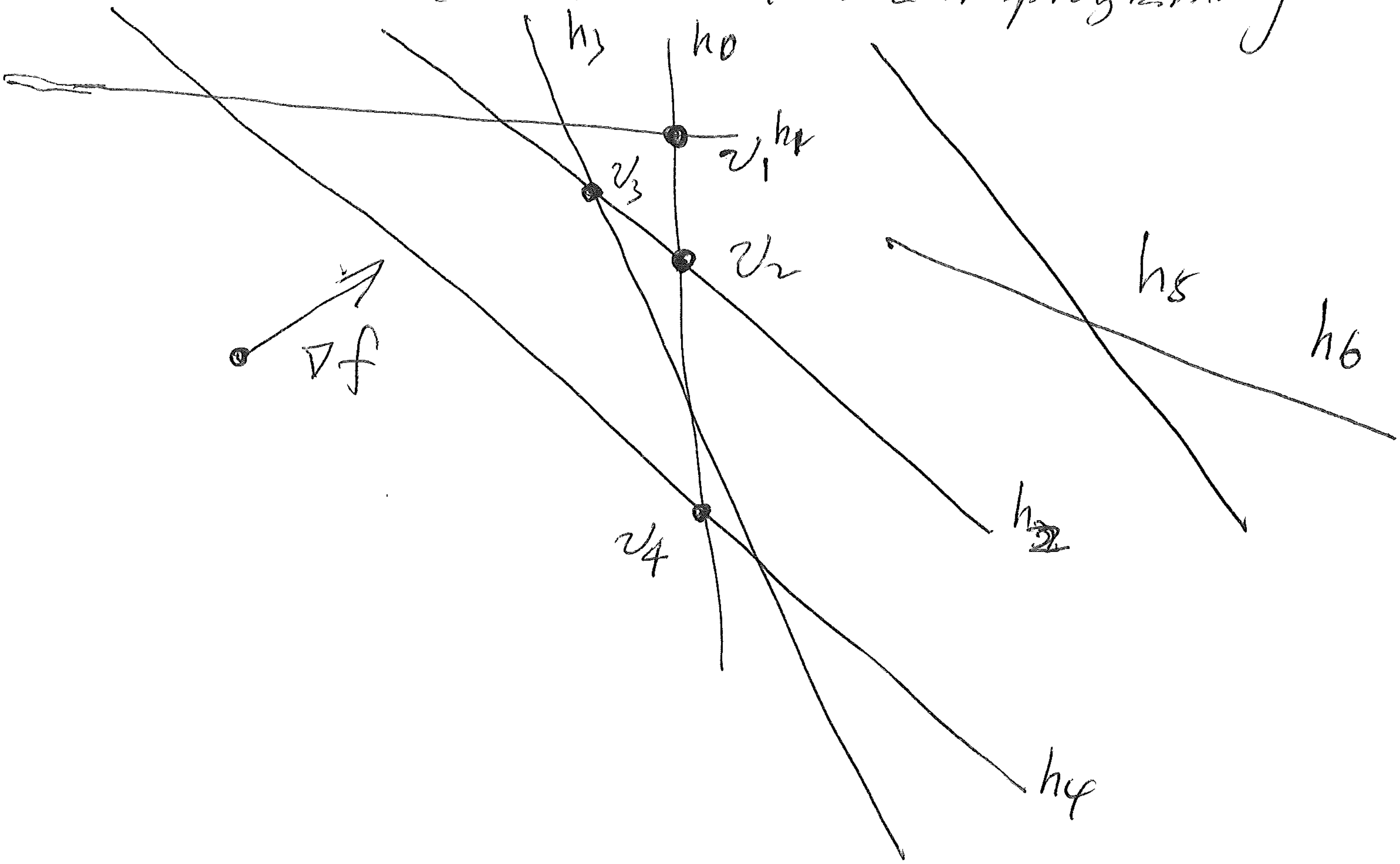


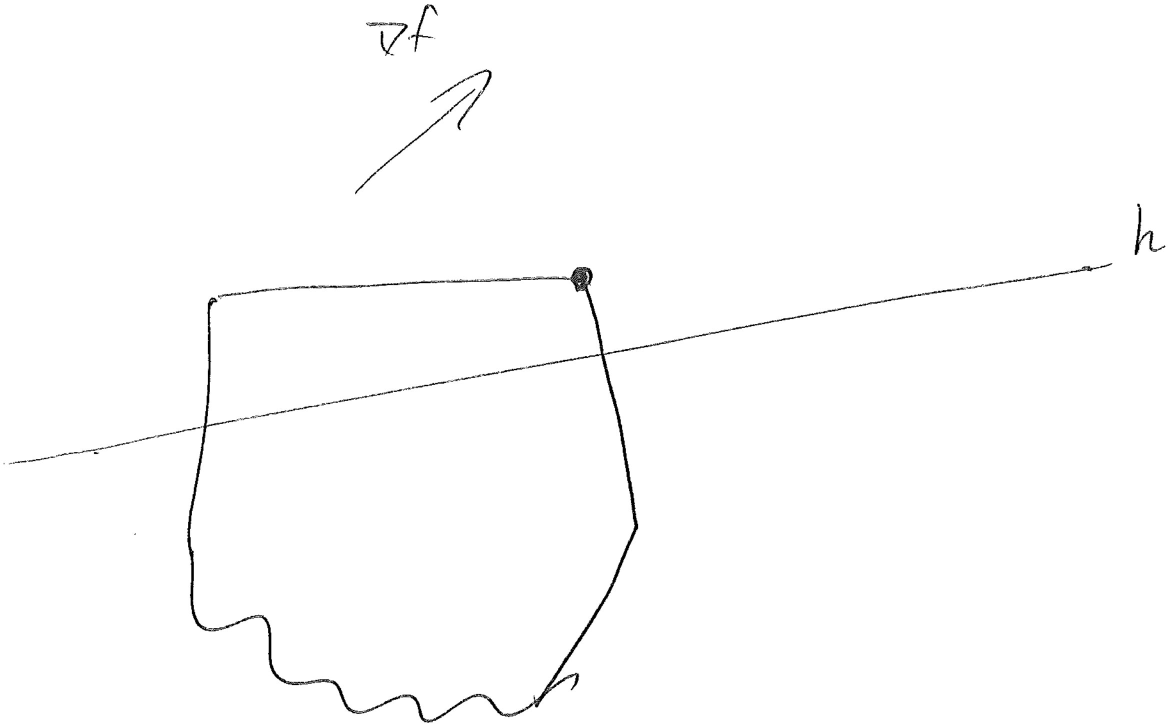

x^*
∇f

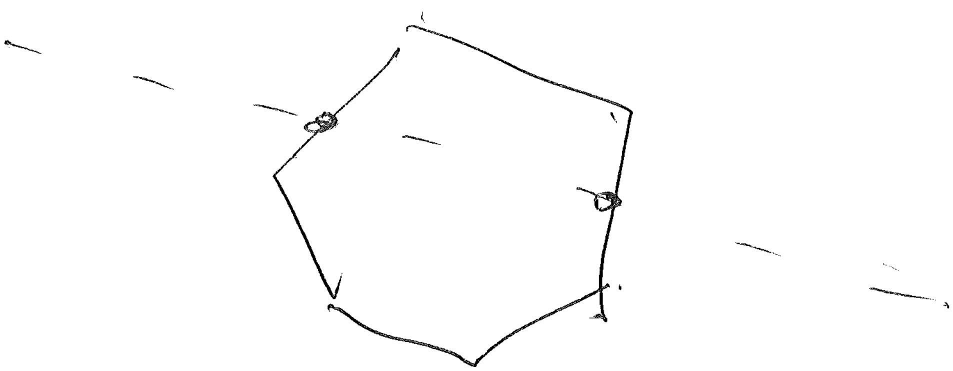

∇f
unbounded


∇f
∇f
x^*
∇f

Assume that we have m constraints
we will feed the constraint one by one to
the objective function
this is called incremental linear programming







linear time

Worse case analysis:

$$O(m^2) = \sum_{j=1}^{m} j$$

Best case analysis

$$O(m).$$

Strategy: randomly perturb the constraints

Let X_j be the r.v. of the running ~~time~~ of the jth iteration.

Two scenarios

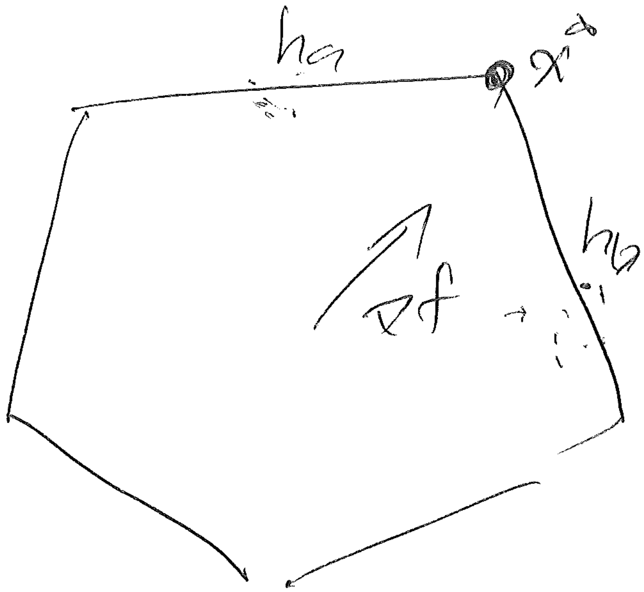
(1) No updates needed $X_j = 1$ $Pr(X_j = 1) = \frac{j-2}{j}$

(2) update needed $X_j = j$ $Pr(X_j = j) = \frac{2}{j}$

$$E[X_j] = \frac{2}{\cancel{j}} \cancel{j} + \frac{j-2}{j} 1$$

$$\leq 3$$

$$\sum_{j=1}^{m} E[X_j] = 3m$$



j th iter

either ha or hb is hj then we have to update in the jth iteration $\dfrac{2}{j}$

Hashing

Let $U = \{0, 1, 2, \cdots, M-1\}$ be a universe of keys

Let m be the size of a table, $m \ll M$

a hash function h is a function

from $\{0, 1, 2, \cdots, M-1\} \rightarrow \{0, 1, \cdots, m-1\}$

E.g. $h(x) = x \bmod m$

For $x \neq y$, $x, y \in U$, if $h(x) = h(y)$, then we say a collision happens

---

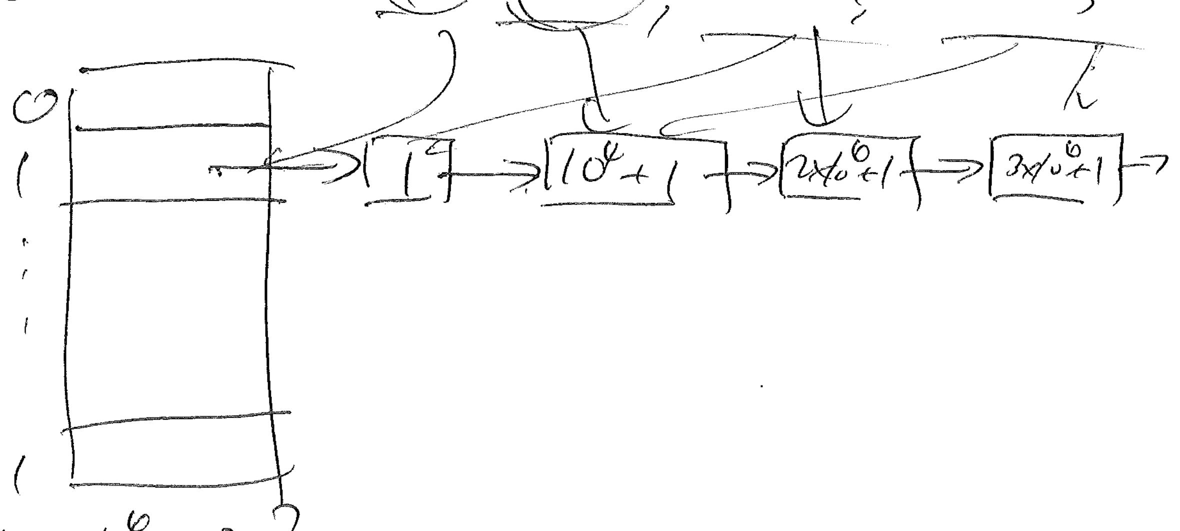
Let $M = 10^9$ $m = 10^4$

$h(x) = x \bmod 10^4$

$a = qb + r$ $(0 \leq r < b)$

$a \bmod b = r$

imagine hashing the input 1, 10^4+1, $2\times10^4+1$, $3\times10^4+1$, ...



search $(100\times10^4+1)$?

The performance of the hash table depends on how bad the collisions.

Strategy to defeat the adversary.

We will have a HUGE collection of hash functions, randomly pick one to use

---

Example. Let m be the size of the hash table
M be the size of the universe
Let p be a prime such that $p > M$
The family of hash functions

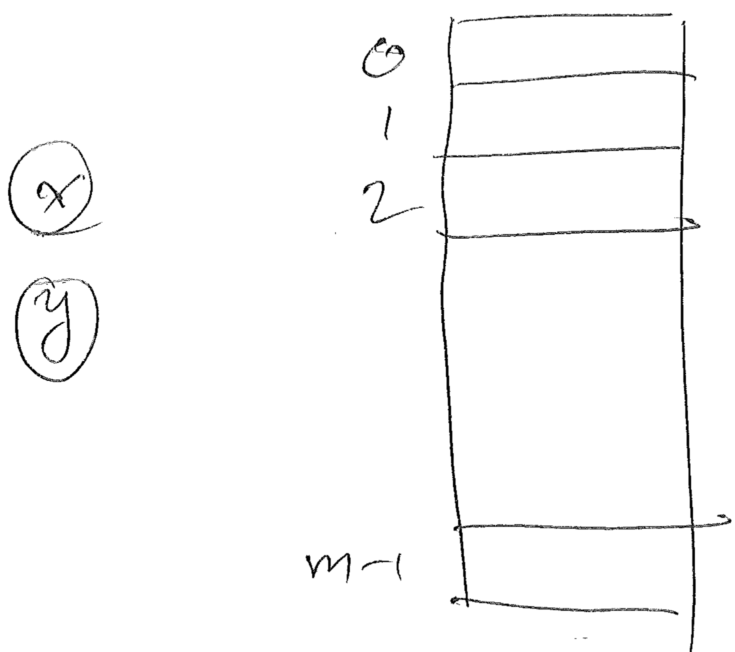
$$H = \{ h_{a,b} \mid a \in \{1, 2, \cdots, p-1\}, b \in \{0, 1, \cdots, p-1\},$$

$$h_{a,b}(x) = ((ax+b) \bmod p) \bmod m \}$$

$$|H| = p(p-1) \sim \Theta(p^2) \sim \Omega(M^2)$$

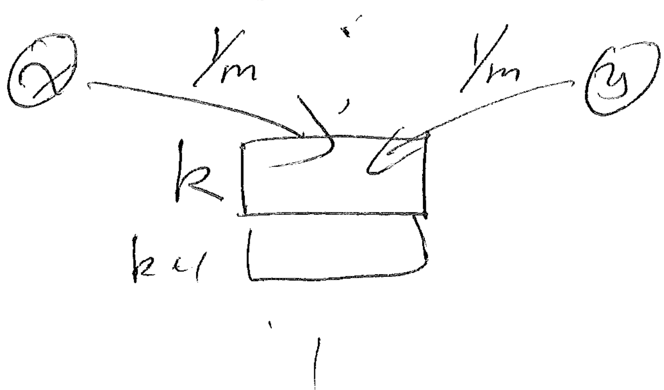
What kind of family of hash functions are good?

A good family should be as good as a <u>random function</u>



Whats a minimum probability of collision?

imagine that a hash function h that hash x to any entry with equal probability



$$\left(\frac{1}{m}\right)^2$$

$$m \cdot \left(\frac{1}{m}\right)^2 = \frac{1}{m}$$

A family of hash funcions is universal if for every pair of distinct keys x, y,

when we randomly choose a hash function $h \in H$ the odds of collision is $\frac{1}{m}$.

Consider partition H into H_1, H_2

Let H_1 contain all the hash function causing x, y to collide

H_2 contain all the hash functions causing x, y not to collide

When randomly pick a hash function, the odds of collision is $\frac{|H_1|}{|H_1|+|H_2|}$

if the family is universal, then $\frac{|H_1|}{|H_1|+|H_2|} = \frac{1}{m}$.

Let the universe be $M=6$ $U=\{0,1,2,3,4,5\}$

Let the table size $m=3$

$p=7$

$$H=\left\{ h_{a,b} \;\middle|\; \begin{array}{l} a\in\{\cancel{0},1,2,3,4,5,6\} \\ b\in\{0,1,2,3,4,5,6\} \end{array} \right\} \qquad |H|=42$$

$x=2,\ y=3.$

H_1

H_2

$h_{1,0}\ ,\ h_{1,1}\ ,\ h_{1,2}$

$\cdots$

Lemma 1 if $b \equiv c \mod m$, then $m \mid (b-c)$

b is congruent to c mod m

$b \bmod m = c \bmod m$

Example $7 \equiv 13 \mod 3$

$7 \bmod 3 = 1 \qquad 13 \bmod 3 = 1$

Pf: Assume $b = q_1 m + r \quad (0 \le r < m)$

$c = q_2 m + r \quad (0 \le r < m)$

$b - c = q_1 m - q_2 m = (q_1 - q_2) m$

$m \mid (b-c)$

Lemma 2 if $m \mid (b-c)$, then $b \equiv c \bmod m$

Pf: assume $b = q_1 m + r_1 \quad (0 \leq r_1 < m)$ $b \bmod m = r_1$

$c = q_2 m + r_2 \quad (0 \leq r_2 < m)$ $c \bmod m = r_2$

Need to show $r_1 = r_2$

Since $m \mid (b-c)$, $m \mid (q_1 m + r_1) - (q_2 m + r_2)$

which is $m \mid (q_1 - q_2) m + (r_1 - r_2)$

thus $m \mid (r_1 - r_2)$

On the other hand

$$-(m-1) \leq r_1 - r_2 \leq m-1$$

Hence $r_1 - r_2 = 0$

Given integes a, b, p

if $\gcd(a,p)=1$ and $\gcd(b,p)=1$

then $\gcd(ab,p)=1$

Recall: $k, a, b \in \mathbb{Z}^+$

if $k \mid a$ and $k \mid b$, then k is a common divisor

Ex. $a=12$ $b=16$, $k=2$

2 is a common divisor of 12 and 16.

the gcd of a, b is their largest common divisor

the $\gcd(12,16) = 4$

Recall: $a, b \in \mathbb{Z}^+$, $a > b$

Let $a = qb + r$

$r = a \bmod b$

$q = a/b$

$0 \leq r < b$

~~then~~ if $r = 0$, $\gcd(a,b) = b$

if $r \neq 0$ $\gcd(a,b) = \gcd(b,r)$

GCD(a, b)

input a, b $a \geq b$

$q = a/b$ $r = a \bmod b$

if $r = 0$, return b

else return GCD(b, r)

Observe $r < \frac{a}{2}$

Pf. if $b < \frac{a}{2}$, then $r < b < \frac{a}{2}$

else $b > \frac{a}{2}$

$a = qb + r = b + r$

$r < a - b \leq a - \frac{a}{2} = \frac{a}{2}$