

Hashing: Universal & Perfect

Recuerdos

①	ϵ -NP	Monte Carlo	$P[\text{correct}] > p$	Tiempo Actual
	G	Las Vegas	$P[\text{correct}] = 1$	No testado

② Hashing

e.g.

$$f: [1..w] \rightarrow [1..N] \quad w \leq N$$

$$f_1(x) = \log_N x = \frac{\log_2 x}{\log_2 N} \mod N$$

$$f_2(x) = ax + b \mod N$$

Hashing Universal

cf video por Leiserson en cursos

Idea: Una familia de funciones de hash
— misma firma $[1..w] \rightarrow [1..N]$ ($N < w$)
— cobra todas las instancias.

$$\forall S \subset [1..w] \quad \exists f \in \mathcal{F} \quad |f(S)| = |S|$$

(ningunas colisiones)

Example

$$f: [1..N] \rightarrow [1..N]$$

$$f(x) = (ax + b) \bmod N$$

$$\begin{matrix} \hookrightarrow [0..N-1] \\ \hookrightarrow [1..N] \end{matrix}$$

$$\mathcal{F}_N = \left\{ f_{a,b} \mid \forall a \in [1..N-1], \forall b \in [0..N-1] \right\}$$

$$f_{a,b}(x) = ax + b \bmod N$$

Th $\mathcal{F}_N$ es una familia universal de hash.

Proof (direct)

Dados , a, b eleborizados

$$\mathbb{P}_N [f_{a,b}(x) = f_{a,b}(y)] = \frac{1}{N}$$

(---)

$$\mathbb{P}_N [\forall x, y \in S \quad f_{a,b}(x) \neq f_{a,b}(y)] > 0 \\ \Rightarrow \exists f \text{ no collisiones} \quad \square$$

II Perfect Hashing

Pb Se puede calcular f sin collision
[en tiempo razonable?]

① Tiempos para verificar si f es sin collision
sobre $O(N)$

② Cuantos funciones? $|X|$, e.g. $O(N^2)$

$\Rightarrow O(N^3)$ determinística

③ si R_n [perfecto por S] $\Rightarrow C \xrightarrow{N_c} \text{Monte Carlo}$
④ $\Rightarrow$ Las Vegas en promedio $\frac{N_c}{2}$