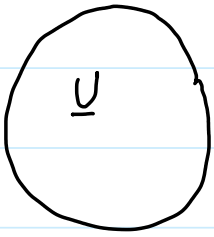
جلسه هفدهم

13:21 Tuesday, November 23, 2021

موضوع : درهم سازی - درهم سازی دوگانه - توابع هش Universal

هش کامل

خیلی بزرگ $|U|$



تعداد کلید : n

آرایه A : N

تابع درهم سازی : h $\quad h: U \longrightarrow 0 \dots N-1$

$x \longrightarrow h(x) \longrightarrow A[h(x)]$

تصادم : $x, y \longrightarrow x \neq y \;\; و \;\; h(x) = h(y)$

Oped Addressing :

واررسی خطی : $h(x) \;-\; h(x)+1 \;-\; h(x)+2 \;-\; \dots$

واررسی مربعی : $h(x) \;-\; h(x)+1 \;-\; h(x)+4 \;-\; h(x)+9 \dots$

N اول باشه - واررسی مربعی $\frac{N}{2}$ خانه‌ها را چک می‌کند

اگر کمتر از $\frac{1}{2}$ باشد، حتماً خانه خالی پیدا می‌شود. $\boxed{\alpha = \frac{n}{N}}$

قضیه [بدون اثبات] متوسط عملیات در یک جستجوی ناموفق $\frac{1}{1-\alpha}$

$\quad$ موفق $\quad$ " $\quad$ " $\quad$ " $\quad \frac{1}{\alpha} \log \frac{1}{1-\alpha}$

۳- هش دوگانه یا Double Hashing

۲ تابع هش داریم : h_1 و h_2

$h_1(x) - h_1(x) + h_2(x) \rightarrow h_1(x) + 2h_2(x) - \dots$

نسبت به جمله اول

$h_1(x) = x \times 13$ — $h_2(x) = \frac{2x \times 5}{x \times 4}$

$x \times 8$

$x = 24$

$0 - 2 - 4 - 6 - 8 - \dots$

* $h_2(x)$ هیچ‌گاه صفر نشود
* هم جدول (یا بخش قابل توجهی از جدول را دور بزند
* $N \leftarrow$ عدد اول.

* $n \nmid N \leftarrow$ ضریب ۲ ، ۳

تصادم غیر ۱ $\rightarrow$ $N \ll |U|$

مشکل تمام روش های درهم سازی این است که اگر یک نفر از تابع هش اطلاع داشته باشد، می تواند وروری بد بدهد.

Adversary

۹۰۲۱۰۵۲۶

۹۰۲۱۰۵۲۶

۸۵۱۱۰۵۲۶

⋮

برای حل این مشکل ؟ استفاده از رندم.

ایده اصلی: تعداد زیادی تابع درهم سازی داشته باشیم و در هنگام اجرا، یکی از

ایده اصلی: تعداد زیادی تابع درهم سازی داشته باشیم و در هنگام اجرا، یکی از آن‌ها را به صورت تصادفی انتخاب کنیم.

خانواده خانواده

تعریف: فرض کنید H یک مجموعه از توابع درهم سازی باشد. در این صورت H یک مجموعه جهانی یا universal است اگر

$$\forall_{x,y\in U},\ \Pr_{h\in H}[h(x)=h(y)] \leq \frac{1}{N}$$

* در H تعداد توابعی از H که در آن‌ها $h(x)=h(y)$ کمتر از $\frac{|H|}{N}$ است

$|H|$ $\frac{1}{|H|} \times \frac{|H|}{N} = \frac{1}{N}$

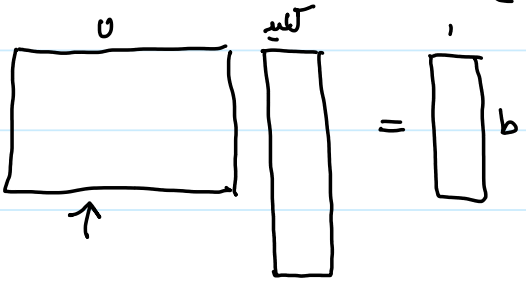
قضیه: فرض کنید H یک خانواده جهانی است و h یک تابع تصادفی از H است. در این صورت به ازای n درج، متوسط تعداد تصادم‌ها $\frac{n}{N}$ برای یک کلید است.

اثبات: کلید x را در نظر بگیرید. به ازای هر کلید $y\neq x$ احتمال تصادم $\frac{1}{N}$ است.
لذا متوسط تصادم‌ها $=\frac{n}{N}$ برای یک کلید است.

مثال - فرض کنید مجموعه U شامل تمام اعداد b بیتی است. فرض کنید N برابر با 2^b است

$b \ll U$ $|U|=2^u$ $u=7$ h: عدد باینری ← عدد بیتی

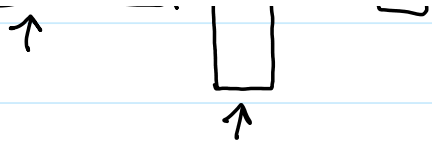
مجموعه H: تمام ماتریس‌های با اندازه $b\times U$ با مقدارهای 0 و 1



$b=3 \rightarrow N=8$

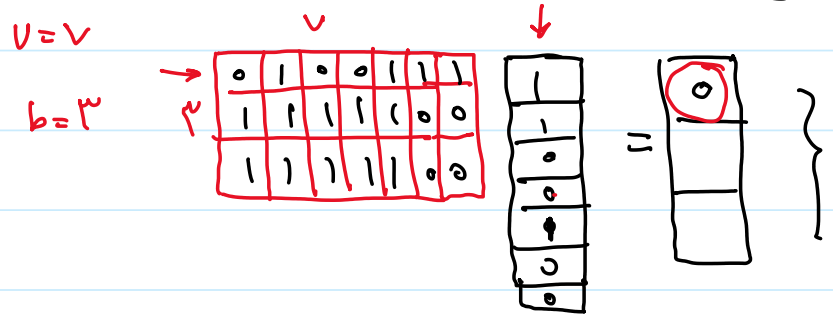
000
001
010

000
001
010
011
⋮



$|H| = 2^{b \times v}$

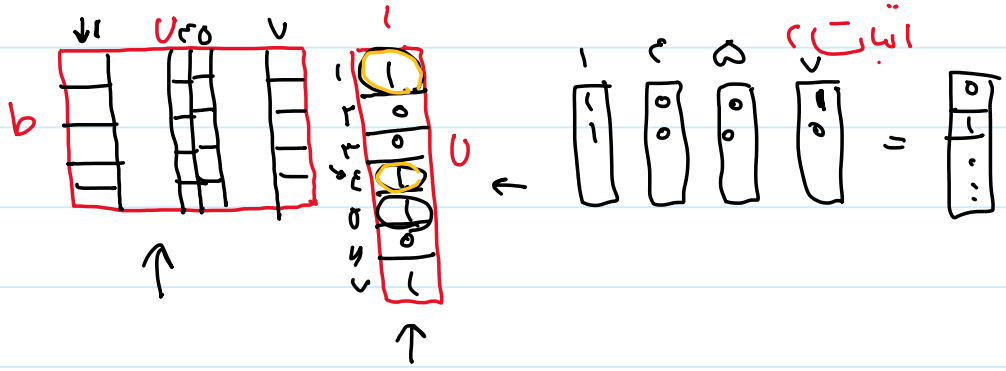
یکی از توابع $|H|$ به صورت تصادفی انتخاب می‌شود

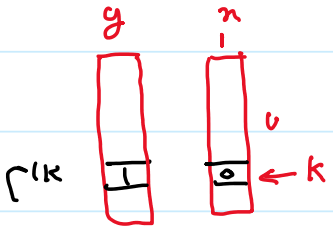


۰ + ۱ + ۰ + ۰ + ۱ + ۰ + ۰ = ۰

قضیه: فرض کنید h به صورت تصادفی از H انتخاب شده در این صورت:

$$\forall x \neq y \quad Pr[h(x) = h(y)] = \frac{1}{2^b} = \frac{1}{N}$$



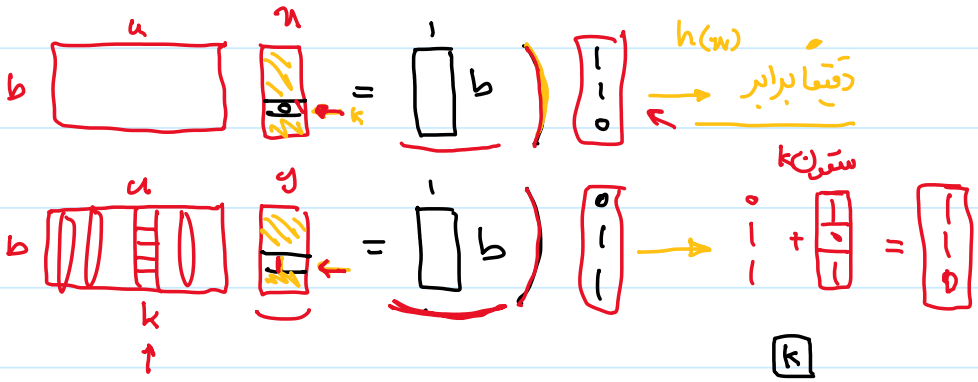


* حال ۲ کلید $x \neq y$ را در نظر بگیرید:

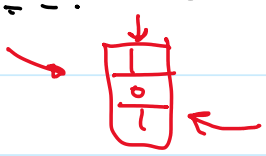
چون $x \neq y$، حداقل یک سطر در x و y متفاوت است.

این سطر را کناری گذارم و مقدار هش را بدون در نظر گرفتن این سطر محاسبه کنیم

این سطر را کاری کنارم و معادلش را بدون درج کردن این سطر کاسبه کنیه



ستون k در h با چه باشد که $h(x)=h(y)$ باشد؟



احتمال این که ستون k به گونه‌ای باشد که $h(x)=h(y)$ $= \frac{1}{2^b}$

مثال:

$$h_{ab}(x) = ((ax+b) \bmod P) \bmod N$$

P عدد اول و a و b

$$H = h_{ab} \quad 0 \le a, b \le P-1 \quad , \quad a \neq 0$$

تابع درهم سازی کامل : مجموعه S از کلید ها داده شده است. تابع هشی که بدون تصادم این کلیدها را در A ذخیره کند یک تابع هش کامل است.

تصادم $O(1)$