

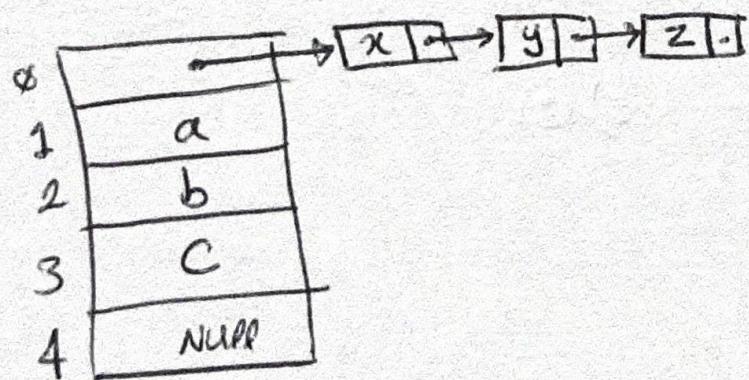
دروهم سازی سراسری (Universal Hashing)

در تبلیغات در بودجه بجز از جمله در دو هم ساز باشد حافظه کردن آنها من می‌تواند مخفی مقادیر هم می‌تواند آنلاین را هم بر انتخاب کند و در داره ساختار ذهنی نماید که حزینه بازیابی آن از مرتبه $O(n)$ باشد.

مثال مبارزه دلیل ایجادی هستور را تابع در هم ساز در بودجه بجز از جدول داره ساز HT همواره ثابت است.

دیگر فنور در برش از کاربردهای عملی مدل کامپیوترها که از صیغه ای داره ساز برای ذهنی و بازیابی مستقیم هاست برمی‌کنم که بحث نمایند، همچو در اینست رسب افرادی هستور در کارسی می‌شود.

مثال: مرض کنند بزم مسائل سُلْستیفسِر و بطری ۲۰۰۷ است و جدول داره ساز HT مسائل ۵ خانه است و مستقیمها هستند تابع داره ساز از این جدول HT به صورت زیر نگارش شده است.



مفرغ کنید بزایم راه هم به بخوب است که اگر آن فتح است از متغیرها برای α و β استفاده نمی کنیم.
با این اوصاف واضح است که در حین تنظیمی همراه استرس به متغیرها α و β در
هزینه کمتر می بازد اما در حین تنظیمی برای هر برآوردی می باشد.

اگر بزر مر باشد α و β را در صفاتی مورث نماید، می تواند فواید برای
هزینه کمتر کاریابی داشت از بزایم و متغیرها آن باشد.

جمع دیدی: با توجه به صفاتی باید در این سفری کنیم به کم عذرخواهی خانواده
متناهی از تراکم (ردهم ساز) هست کنیم که هیچ اساحت جدول در همین عذر AT
بطوری اتفاقی نیست از تراکم داخل آن را استخراج برای هم ساز را بر اساس
آن انجام دهیم. لازم به ذراست که به معنی انتخاب تابع ردهم
ساز، آن تابع مابه می باشد باقی می ماند و درین مابل از اجرای
مسئل مخفی نیست.

نکته: در هم ساز سراسری که برگزاریه بالا را در دل خود جای را دارد است برای هر
Application این بزایم کاربرد مناسب نیست و مابه درآمد انتخاب آن دست گردید
مثال دیگر بزایم کاربرد کاربری پایه ای دارند مابه مبنی برگردان سه هفتم اساتید
می کنند که نتیجه علیه بزرگتر برگزار در هم ساز سراسری است در آن می باشند این است
بر این نتایج در مفهومی در درستی بزایم کاربردی گسترده است این نتایج
ایجاد

نتایج ایکندر در هم سازی سراسری:

$$[n] = \{0, 1, \dots, m-1\}$$

$$U = \text{دسته ملندها}$$

تابع $H = \{h_1, \dots, h_m\}$ ، where $h_i : U \rightarrow [m]$
در هم ساز خانوار معادل از تابع

$$m \ll n \leq |U|$$

حالیکنہ π بیانگر تعداد عنصر مجموعی یوں (باقیداً عنصر فقر جمل در هم ساز H)

سوال: مجموعی تابع در هم ساز H بیانگر راستاری باشد؟

عکسیقہ π : مجموعی H دار و بیانگر Universal است اگر

برای هر دو $U, k, l \in U$ تعداد تابع در هم ساز H که $h \in H$ است،

$$h(\ell) = h(k)$$

است، حداقل $\frac{|H|}{m}$ باشد، برعبارت دیگر بالتعاب دیگر

تابع در هم ساز تصادفی از H ، احتمال بر این $h(\ell) = h(k)$ بیش از $\frac{1}{m}$ باشد.

لست. بجز این ساده ترینی ℓ و k در U از مختلف جدا

در خانه های مختلف از زیر چی سووند.

مثال - مجموع توابع درهم ساز H :

مربع کنید P عدد اول بزرگتر از هم انداد داخل را فن بلند (عنین ۷) باشند

$$\mathbb{Z}_P^+ = \{1, \dots, P-1\}$$

$$Z_P = \{0, \dots, P-1\}$$

تابع درهم ساز $h_{a,b}$ را به صورت زیر تعریف کنیم:

$$h_{a,b}(k) = ((ak+b) \bmod P) \bmod m$$

محاسبه $b \in Z_P$, $a \in \mathbb{Z}_P^+$ بایسند

حال مجموع توابع درهم ساز H را به صورت زیر تعریف کنیم:

$$H_{P,m} = \{ h_{a,b} : a \in \mathbb{Z}_P^+, b \in Z_P \}$$

برآورده به صورت کاندید بر a و b برداشته است که:

$$|H_{P,m}| = P(P-1)$$

> فعل لـ «کتاب در قصیبی» ۱۱.۵ صفحه ۲۶۷، حصیبی Universal بین

بلر خانواده خود نیان داده دستور کر ~~باید بجهات خوبی~~ علاوه بر این باره علاوه بر این تراشیده آن خوبیه ندارد.

کفته: اگر مجموع دو هزار Universal باشد آنگاه به صورت
میانگین متریکه $\frac{1}{2}(1-\alpha)$ حذف / مستجو از مرتبه $(1+\alpha)$ می باشد

نکته: در روکیر در هم ساز سراسری، ابتدا تغییمات مرتبه ب جدول در هم ساز
انجام می شود و سپس در هر بار اجرای آن یک تابع h از مجموع در هم ساز
 H به صورت انتخاب می شود.

نکته: قبل از دیدن کسر لارگه یک جدول در هم ساز بر انتقالیات کرده اکن $m \ll n$
است، مقوازن بولن تابع در هم ساز بیانگری تابع خوب مرحله در هم ساز
بهماری آهد. با اینحال یک فصل که نه تنها بیانگری تابع در هم ساز
خوب مرحله کاربردی باشد. برای این منظور، به مثال زیر دقت
کنید.

مثال: یک جدول در هم ساز با تغییمات زیر را در نظر بگیرید:

$$[m] = \{10, \dots, 99\}^2 = \text{ادواره ماعمل}$$

$$U = [1^8]$$

$$h(k) = k \bmod 1000 = \text{تابع در هم ساز}$$

$$m \ll n$$

میرن لئیند جدول در حجم ساز عوّق می خواهد در راسته ای اعنهان سه کاره فتح سوار و
کار داشتوبین هاراین راسته به گلخان است که بر مدد ۱۰۰۰ نفر است.

بنابران، با همین درجه ممتاز موفق به حفظ دانش بریان به خانه ۱۰ نگاهستی می‌رسند و ۹۹۹۹ خانه حافظه خالی می‌مانند.

جمع و بندی و محدوده این در فرم مسازی محاسبه می شود و نتایج آن
از یک فرستاده کلی بهره گرفته.

ملحق در رابطه با المدارزه حافظه (m) :

اما نظرگره پیشتر نیز تاکنون کرایم، هدف ما داشتن بیت تابع در «همه ساز متوزن» (ذرب) است. در این راستا، تعیین معنادار مناسب حافظه های ترازنی تا سیر فدار باشد. به مثال زیر دقت کنید

مثال: آگر تابع در هم ساز زیر را انتخاب کرده باشیم، باید به این معور دقت کنیم که m رکه کمالی لیستم سایر دلایل ۲ باشد ($m \neq 2^{\alpha}$).

$$h(k) = k \bmod m$$

مُرْفَقْ لِسْنَهْ دَلِيلْ ك دَالِهِ لِسْنَهْ l-bit بَالِهِ لِسْنَهْ

$$K = \begin{pmatrix} a & a & \dots & a & a & a & \dots & a & a & a \\ & a_{l-1} & a_{l-2} & \dots & a_{d+1} & a_{d+1} & a & \dots & a_2 & a_1 & a_0 \end{pmatrix}_b$$

$$= \alpha_0 \times 2^0 + \alpha_1 \times 2^1 + \alpha_2 \times 2^2 + \dots + \alpha_d \times 2^d + \alpha_{d+1} \times 2^{d+1}$$

$$\underbrace{a_{d+2}x^2^{d+2} + \cdots + a_{l+1}x^{l+1}}_{جواب صفری} \rightarrow 0 \pmod{2^d}$$

از راهنمایی که در میانه $m=2^\alpha$ می‌سبه می‌شود، بیر دانع است که آنها

α بیست کم از زدن در خروجی تابع در هم ساز h تا نیز کنار است.

کله، تجربه دستان می‌نگردد هر قابل فرق انتساب h در این هر از m طرفه با به مثال

می‌شود و از نظر نفعی مناسب باشد. به مثال صدر فرق شده در میان هار علی در خروجی
بهم تابع در هم ساز بوده و این نیز است. اینجا m میانه می‌شود و A میانه
که h سه عدد برابر توصیه این انتساب می‌شوند این باشد که سبیل شود
ترزیع را اینه میانه خانه هار چانه به صورت مناسب انجام شود.

هر از m تابع در هم ساز را صفری می‌سینم و برخلاف مثال قبل، لذاره چانه
بر این مناسب است. نوع m میانه و نظریت انتساب اینها اینه را در

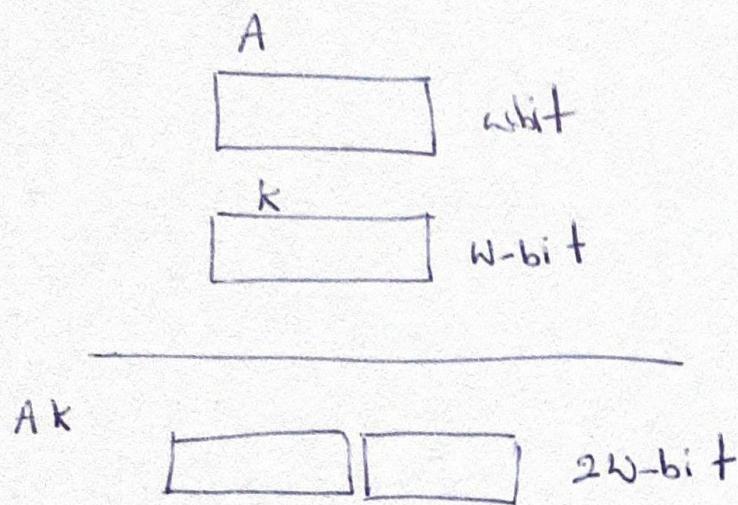
$$h(k) = \left\lceil m \left(kA \bmod 1 \right) \right\rceil$$

مثال:

جایی که $A < 1$ و توصیه شده $m=2^\alpha$ و $A = \frac{\sqrt{5}-1}{2}$ میانه ایند
 تمام سی هزار از دری سبه تابع h (عنی می‌کند) با اینکه طرفه مناسب هر از خود
هستند

$$m = 2^{\alpha}$$

می‌دانیم که $(AK \bmod 1)$ در واقع میت اعداد حاصل‌تفتر AK را فراود خواهد. مزون لینکر A, K هر یکم N -bit است.



طبق تابع $t = \alpha^{m=2^{\alpha}}$ در AK فنرستیم، آنگاه میت از AK که بیانفر کسر است بهشت راست سیف زاده شده و به عنوان فرودج تابع t در نظر گرفته شود. باقی اسکرین \varnothing بیت بر ارزش حاصل‌تفتر AK ، تمام میت هار A و K را برای نسبت اند.

$$\begin{array}{cccccc} a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 \end{array}$$

$a_3 b_1$	$a_3 b_2$	$a_3 b_3$	$a_2 b_0$	$a_2 b_1$	$a_2 b_2$	$a_2 b_3$	$a_1 b_0$	$a_1 b_1$	$a_1 b_2$	$a_1 b_3$	$a_0 b_0$	$a_0 b_1$	$a_0 b_2$	$a_0 b_3$
$a_3 b_1$	$a_3 b_2$	$a_3 b_3$	$a_2 b_0$	$a_2 b_1$	$a_2 b_2$	$a_2 b_3$	$a_1 b_0$	$a_1 b_1$	$a_1 b_2$	$a_1 b_3$	$a_0 b_0$	$a_0 b_1$	$a_0 b_2$	$a_0 b_3$
$a_3 b_1$	$a_3 b_2$	$a_3 b_3$	$a_2 b_0$	$a_2 b_1$	$a_2 b_2$	$a_2 b_3$	$a_1 b_0$	$a_1 b_1$	$a_1 b_2$	$a_1 b_3$	$a_0 b_0$	$a_0 b_1$	$a_0 b_2$	$a_0 b_3$
$a_3 b_1$	$a_3 b_2$	$a_3 b_3$	$a_2 b_0$	$a_2 b_1$	$a_2 b_2$	$a_2 b_3$	$a_1 b_0$	$a_1 b_1$	$a_1 b_2$	$a_1 b_3$	$a_0 b_0$	$a_0 b_1$	$a_0 b_2$	$a_0 b_3$