Análise de Algoritmos

Parte destes slides são adaptações de slides

do Prof. Paulo Feofiloff e do Prof. José Coelho de Pina.

Tabelas de espalhamento

CLRS Cap 12

Conjuntos dinâmicos

Conjunto dinâmico, que sofre as seguintes operações:

- inserções,
- remoções,
- buscas.

Como armazenar tal conjunto?

Conjuntos dinâmicos

Conjunto dinâmico, que sofre as seguintes operações:

- inserções,
- remoções,
- buscas.

Como armazenar tal conjunto?

Tempo de pior caso:

	inserção	busca	remoção
LL	$\mathrm{O}(1)$	$\mathrm{O}(n)$	$\mathrm{O}(1)^*$
ABB	$\mathrm{O}(\lg n)$	$\mathrm{O}(\lg n)$	$\mathrm{O}(\lg n)$

* depois da busca

Conjuntos dinâmicos

Conjunto dinâmico, que sofre as seguintes operações:

- inserções,
- remoções,
- buscas.

Como armazenar tal conjunto?

Tempo de pior caso:

	inserção	busca	remoção
LL	$\mathrm{O}(1)$	$\mathrm{O}(n)$	$\mathrm{O}(1)^*$
ABB	$\mathrm{O}(\lg n)$	$\mathrm{O}(\lg n)$	$\mathrm{O}(\lg n)$

Tempo esperado:

hashing	$\mathrm{O}(1)$	$\mathrm{O}(1)$	$\mathrm{O}(1)$

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Colisão: duas chaves distintas x e y tq $h(x) = h(y)$.

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Colisão: duas chaves distintas x e y tq $h(x) = h(y)$.

Geralmente se escolhe m de modo que
o número de elementos na tabela seja $\Theta(m)$.

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Colisão: duas chaves distintas x e y tq $h(x) = h(y)$.

Geralmente se escolhe m de modo que
o número de elementos na tabela seja $\Theta(m)$.

Operações: inserções, remoções, e buscas.

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Colisão: duas chaves distintas x e y tq $h(x) = h(y)$.

Geralmente se escolhe m de modo que
o número de elementos na tabela seja $\Theta(m)$.

Operações: inserções, remoções, e buscas.

Resolução de colisões: usando listas ligadas, por exemplo.

Tabelas de espalhamento

U: universo de chaves possíveis

função de hashing: $h : U \to \{0, \ldots, m-1\}$

m: tamanho da tabela de hashing

Colisão: duas chaves distintas x e y tq $h(x) = h(y)$.

Geralmente se escolhe m de modo que
o número de elementos na tabela seja $\Theta(m)$.

Operações: inserções, remoções, e buscas.

Resolução de colisões: usando listas ligadas, por exemplo.

Aplicações: tabela de símbolos de um compilador.

Boas funções de hashing

- $h(k) = k \bmod m$,
  onde sugere-se usar como m
  um primo distante de potências de 2.

Boas funções de hashing

- $h(k) = k \bmod m$,
  onde sugere-se usar como m
  um primo distante de potências de 2.

- $h(k) = m(kA \bmod 1)$,
  onde A é uma constante em $(0, 1)$ e
  $kA \bmod 1$ é a parte fracionária de kA.
  A escolha de m aqui é livre neste caso.
  Knuth sugere que $A = (\sqrt{5} - 1)/2 = 0.6180339\ldots$
  é uma boa escolha em geral.

Boas funções de hashing

- $h(k) = k \bmod m$,
  onde sugere-se usar como m
  um primo distante de potências de 2.

- $h(k) = m(kA \bmod 1)$,
  onde A é uma constante em $(0, 1)$ e
  $kA \bmod 1$ é a parte fracionária de kA.
  A escolha de m aqui é livre neste caso.
  Knuth sugere que $A = (\sqrt{5} - 1)/2 = 0.6180339\ldots$
  é uma boa escolha em geral.

- hashing universal

Hashing universal

U: conjunto universo (contém todas as possíveis chaves).

n: um número muito menor que $|U|$.

$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Hashing universal

U: conjunto universo (contém todas as possíveis chaves).

n: um número muito menor que $|U|$.

$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Se, para cada par de chaves distintas k, ℓ em U, o número de funções h em $\mathcal{H}$ tais que $h(k) = h(\ell)$ é no máximo $|\mathcal{H}|/n$, então $\mathcal{H}$ é uma coleção universal de hashing (para U e n).

Hashing universal

U: conjunto universo (contém todas as possíveis chaves).

n: um número muito menor que $|U|$.

$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Se, para cada par de chaves distintas k, ℓ em U, o número de funções h em $\mathcal{H}$ tais que $h(k) = h(\ell)$ é no máximo $|\mathcal{H}|/n$, então $\mathcal{H}$ é uma coleção universal de hashing (para U e n).

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Hashing universal

U: conjunto universo $\qquad n \ll |U|$
$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Hashing universal

U: conjunto universo $\qquad n \ll |U|$
$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Hashing universal

U: conjunto universo $\qquad n \ll |U|$
$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Então $X = \sum_i X_i$ e $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i \Pr\{X_i = 1\}$.

Hashing universal

U: conjunto universo $\qquad n \ll |U|$
$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Então $X = \sum_i X_i$ e $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i \Pr\{X_i = 1\}$.

Por definição, para cada ℓ em U, com $\ell \neq u$, o número de funções h em $\mathcal{H}$ tais que $h(\ell) = h(u)$ é no máximo $|\mathcal{H}|/n$.

Hashing universal

U: conjunto universo $\qquad n \ll |U|$
$\mathcal{H}$: conjunto de funções de U em $\{0, \ldots, n-1\}$.

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Então $X = \sum_i X_i$ e $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i \Pr\{X_i = 1\}$.

Por definição, para cada ℓ em U, com $\ell \neq u$, o número de funções h em $\mathcal{H}$ tais que $h(\ell) = h(u)$ é no máximo $|\mathcal{H}|/n$.

Em particular, para cada i, se h é escolhida aleatoriamente de $\mathcal{H}$, então $\Pr\{X_i = 1\} = \Pr\{h(s_i) = h(u)\} \leq \frac{|\mathcal{H}|/n}{|\mathcal{H}|} = 1/n$.

Hashing universal

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Então $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i \Pr\{X_i = 1\}$.

Para cada ℓ em $U \setminus \{u\}$, o número de funções h em $\mathcal{H}$ tais que $h(\ell) = h(u)$ é no máximo $|\mathcal{H}|/n$.

Para cada i, se h é escolhida aleatoriamente de $\mathcal{H}$, então $\Pr\{X_i = 1\} \leq 1/n$.

Hashing universal

Teorema: Seja $u \in U$, $S \subseteq U$ tal que $|S| \leq n$ e $\mathcal{H}$ uma coleção universal de hashing para U e n. Se h é escolhida aleatoriamente de $\mathcal{H}$ e X é o número de elementos s em $S \setminus \{u\}$ tais que $h(s) = h(u)$, então $\mathrm{E}[X] \leq 1$.

Prova: Seja s_i o i-ésimo elemento de $S \setminus \{u\}$.

X_i: variável aleatória binária que vale 1 sse $h(s_i) = h(u)$.

Então $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i \Pr\{X_i = 1\}$.

Para cada ℓ em $U \setminus \{u\}$, o número de funções h em $\mathcal{H}$ tais que $h(\ell) = h(u)$ é no máximo $|\mathcal{H}|/n$.

Para cada i, se h é escolhida aleatoriamente de $\mathcal{H}$, então $\Pr\{X_i = 1\} \leq 1/n$.

Logo $\mathrm{E}[X] \leq |S|/n \leq 1$. ■

Uma coleção universal de hashing

Seja p um primo tal que $U \subseteq \{0, \ldots, p-1\}$.

$\mathbb{Z}_p$: conjunto $\{0, \ldots, p-1\}$.
$\mathbb{Z}_p^*$: conjunto $\{1, \ldots, p-1\}$.

Uma coleção universal de hashing

Seja p um primo tal que $U \subseteq \{0, \ldots, p-1\}$.

$\mathbb{Z}_p$: conjunto $\{0, \ldots, p-1\}$.
$\mathbb{Z}_p^*$: conjunto $\{1, \ldots, p-1\}$.

Para todo a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$, seja

$$h_{a,b}(k) \;=\; ((ak + b) \bmod p) \bmod n,$$

para todo k em U.

Uma coleção universal de hashing

Seja p um primo tal que $U \subseteq \{0, \ldots, p-1\}$.

$\mathbb{Z}_p$: conjunto $\{0, \ldots, p-1\}$.
$\mathbb{Z}_p^*$: conjunto $\{1, \ldots, p-1\}$.

Para todo a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$, seja

$$h_{a,b}(k) \;=\; ((ak + b) \bmod p) \bmod n,$$

para todo k em U.

Teorema: $\mathcal{H} \;=\; \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $\; b \in \mathbb{Z}_p\}$ é universal.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^* \text{ e } b \in \mathbb{Z}_p\}$ é universal.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Mostraremos que, para k e ℓ em U, com $k \neq \ell$,
o número de funções h em $\mathcal{H}$ tq $h(k) = h(\ell)$ é $\leq |\mathcal{H}|/n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Mostraremos que, para k e ℓ em U, com $k \neq \ell$,
o número de funções h em $\mathcal{H}$ tq $h(k) = h(\ell)$ é $\leq |\mathcal{H}|/n$.

Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Note que $r - s = a(k - \ell) \bmod p$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Mostraremos que, para k e ℓ em U, com $k \neq \ell$,
o número de funções h em $\mathcal{H}$ tq $h(k) = h(\ell)$ é $\leq |\mathcal{H}|/n$.

Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Note que $r - s = a(k - \ell) \bmod p$.

Como p é primo, $a \neq 0$ e $k - \ell \neq 0$, temos que
$a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

(Colisões podem ocorrer apenas devido ao $\bmod n$.)

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Mostraremos que, para k e ℓ em U, o número de funções h em $\mathcal{H}$ tais que $h(k) = h(\ell)$ é no máximo $|\mathcal{H}|/n$.

Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^* \text{ e } b \in \mathbb{Z}_p\}$ é universal.

Prova: Mostraremos que, para k e ℓ em U, o número de funções h em $\mathcal{H}$ tais que $h(k) = h(\ell)$ é no máximo $|\mathcal{H}|/n$.

Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada par (a, b) com $a \neq 0$ resulta num par (r, s) distinto pois determinamos (a, b) unicamente a partir de (r, s):

$$\begin{aligned} a &= ((r - s)((k - \ell)^{-1} \bmod p) \bmod p \\ b &= (r - ak) \bmod p \end{aligned}$$

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^* \text{ e } b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada par (a, b) com $a \neq 0$ resulta num par (r, s) distinto pois
$a = ((r - s)((k - \ell)^{-1} \bmod p) \bmod p$ e $b = (r - ak) \bmod p$

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada par (a, b) com $a \neq 0$ resulta num par (r, s) distinto pois
$a = ((r - s)((k - \ell)^{-1} \bmod p) \bmod p$ e $b = (r - ak) \bmod p$
é a única solução em $\mathbb{Z}_p$ do sistema

$$\begin{aligned} r &= ak + b \bmod p \\ s &= a\ell + b \bmod p \end{aligned}$$

nas variáveis a e b.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada um dos $p(p-1)$ pares (a, b) com $a \neq 0$
resulta num par (r, s) distinto com $r \neq s$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada um dos $p(p-1)$ pares (a, b) com $a \neq 0$
resulta num par (r, s) distinto com $r \neq s$.

Existem $p(p-1)$ pares possíveis de (r, s) com $r \neq s$.
Logo há uma bijeção entre os (a, b) e os (r, s).

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.
Note que $r - s = a(k - \ell) \neq 0 \bmod p$. Ou seja, $r \neq s$.

Cada um dos $p(p-1)$ pares (a, b) com $a \neq 0$
resulta num par (r, s) distinto com $r \neq s$.

Existem $p(p-1)$ pares possíveis de (r, s) com $r \neq s$.
Logo há uma bijeção entre os (a, b) e os (r, s).

Resta então determinar quantos pares (r, s) com $r \neq s$
são tais que $r = s \bmod n$, ou seja, $r - s = 0 \bmod n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Há uma bijeção entre os (a, b) e os (r, s) com $r \neq s$.

Resta determinar quantos pares (r, s) com $r \neq s$
são tais que $r = s \bmod n$, ou seja, $r - s = 0 \bmod n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Há uma bijeção entre os (a, b) e os (r, s) com $r \neq s$.

Resta determinar quantos pares (r, s) com $r \neq s$
são tais que $r = s \bmod n$, ou seja, $r - s = 0 \bmod n$.

Para cada $r \in \mathbb{Z}_p$,
há $\lfloor (p-1)/n \rfloor$ valores de $s \neq r$ tais que $s = r \bmod n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Há uma bijeção entre os (a, b) e os (r, s) com $r \neq s$.

Resta determinar quantos pares (r, s) com $r \neq s$
são tais que $r = s \bmod n$, ou seja, $r - s = 0 \bmod n$.

Para cada $r \in \mathbb{Z}_p$,
há $\lfloor (p-1)/n \rfloor$ valores de $s \neq r$ tais que $s = r \bmod n$.

Logo há $p\lfloor (p-1)/n \rfloor \leq p(p-1)/n = |\mathcal{H}|/n$ pares (r, s)
com $r \neq s$ tais que $s = r \bmod n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Há uma bijeção entre os (a, b) e os (r, s) com $r \neq s$.

Para cada $r \in \mathbb{Z}_p$,
há $\lfloor (p-1)/n \rfloor$ valores de $s \neq r$ tais que $s = r \bmod n$.

Logo há $p\lfloor (p-1)/n \rfloor \leq p(p-1)/n = |\mathcal{H}|/n$ pares (r, s)
com $r \neq s$ tais que $s = r \bmod n$.

Uma coleção universal de hashing

p: primo tal que $U \subseteq \mathbb{Z}_p$.

Para a em $\mathbb{Z}_p^*$ e b em $\mathbb{Z}_p$,
seja $h_{a,b}(k) = ((ak + b) \bmod p) \bmod n$ para todo k em U.

Teorema: $\mathcal{H} = \{h_{a,b} : a \in \mathbb{Z}_p^*$ e $b \in \mathbb{Z}_p\}$ é universal.

Prova: Sejam $r = (ak + b) \bmod p$ e $s = (a\ell + b) \bmod p$.

Há uma bijeção entre os (a, b) e os (r, s) com $r \neq s$.

Para cada $r \in \mathbb{Z}_p$,
há $\lfloor (p-1)/n \rfloor$ valores de $s \neq r$ tais que $s = r \bmod n$.

Logo há $p\lfloor (p-1)/n \rfloor \leq p(p-1)/n = |\mathcal{H}|/n$ pares (r, s)
com $r \neq s$ tais que $s = r \bmod n$.

Portanto há $\leq |\mathcal{H}|/n$ funções h em $\mathcal{H}$ tais que $h(k) = h(\ell)$. ■