# MC-202 — Unidade 19 Tabela de Espalhamento

Rafael C. S. Schouery rafael@ic.unicamp.br

Universidade Estadual de Campinas

2° semestre/2017

## Introdução

Queremos contar o número de ocorrências de cada palavra da biblioteca



## Introdução

Queremos contar o número de ocorrências de cada palavra da biblioteca



• no idioma, há cerca de milhares de palavras ( $\approx 435.000$ )

## Introdução

Queremos contar o número de ocorrências de cada palavra da biblioteca



- no idioma, há cerca de milhares de palavras ( $\approx 435.000$ )
- mas no total, há milhões de ocorrências!

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrências ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

ocorrencias["ilha"] = 8

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

ocorrencias["ilha"] = 8

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

#### Primeiras opções:

• Vetor - acesso/escrita/inserção em  $\mathrm{O}(n)$ 

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

```
ocorrencias["ilha"] = 8
```

- Vetor acesso/escrita/inserção em  $\mathrm{O}(n)$
- ullet Vetor ordenado acesso/escrita em  $O(\lg n)$

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

```
ocorrencias["ilha"] = 8
```

- Vetor acesso/escrita/inserção em  $\mathrm{O}(n)$
- Vetor ordenado acesso/escrita em  $O(\lg n)$ 
  - inserir um novo leva O(n)

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

```
ocorrencias["ilha"] = 8
```

- Vetor acesso/escrita/inserção em O(n)
- Vetor ordenado acesso/escrita em  $O(\lg n)$ 
  - inserir um novo leva O(n)
- ullet ABB balanceada acesso/escrita/inserção em  $O(\lg n)$

dia: 6 ocorrências escola: 13 ocorrências gratuito: 1 ocorrência ilha: 8 ocorrências jeito: 5 ocorrências lata: 2 ocorrências

Queremos acessar uma palavra como se fosse um vetor:

```
ocorrencias["ilha"] = 8
```

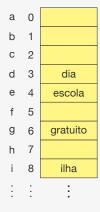
#### Primeiras opções:

- Vetor acesso/escrita/inserção em O(n)
- Vetor ordenado acesso/escrita em  $O(\lg n)$ 
  - inserir um novo leva O(n)
- ullet ABB balanceada acesso/escrita/inserção em  $O(\lg n)$

Conseguimos fazer em O(1)?

#### Caso fácil

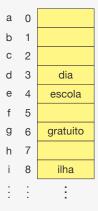
Se tivéssemos apenas uma palavra começando com cada letra era fácil



#### Caso fácil

Se tivéssemos apenas uma palavra começando com cada letra era fácil

• bastaria ter um vetor de 24 posições





Ideia:



#### Ideia:

• uma lista ligada para cada letra



#### Ideia:

- uma lista ligada para cada letra
- guardamos os ponteiros para as listas em um vetor





Inserindo "bala":



#### Inserindo "bala":

descobrimos a posição pela primeira letra



#### Inserindo "bala":

- descobrimos a posição pela primeira letra
- atualizamos o vetor para apontar para o nó de "bala"



#### Inserindo "bala":

- descobrimos a posição pela primeira letra
- atualizamos o vetor para apontar para o nó de "bala"





Inserindo "bela":



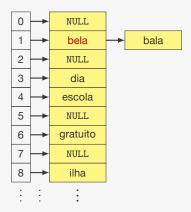
#### Inserindo "bela":

• descobrimos a posição pela primeira letra



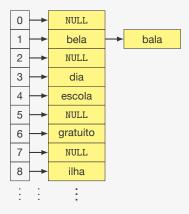
#### Inserindo "bela":

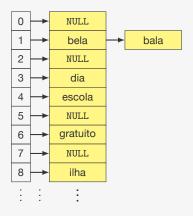
- descobrimos a posição pela primeira letra
- temos uma colisão com "bala"



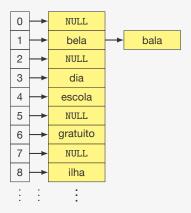
#### Inserindo "bela":

- descobrimos a posição pela primeira letra
- temos uma colisão com "bala"
- inserimos no começo da lista da letra b



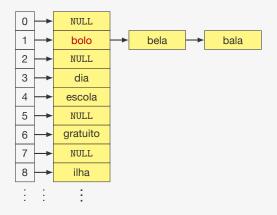


Após a inserção de várias palavras começando com b:



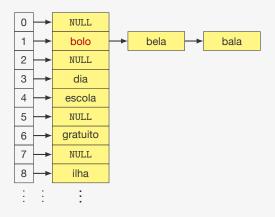
Após a inserção de várias palavras começando com b:

inserimos "bolo",



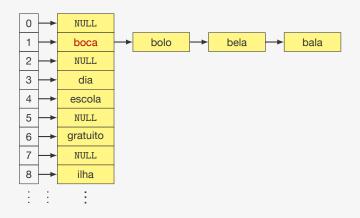
Após a inserção de várias palavras começando com b:

• inserimos "bolo",



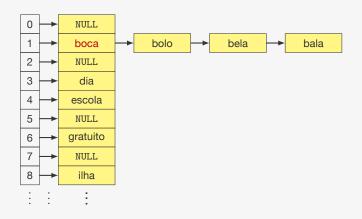
Após a inserção de várias palavras começando com b:

• inserimos "bolo", "boca",



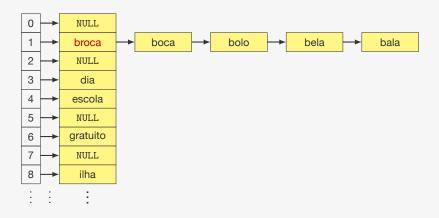
Após a inserção de várias palavras começando com b:

inserimos "bolo", "boca",



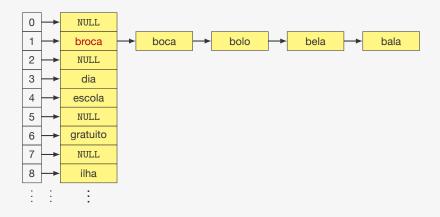
Após a inserção de várias palavras começando com b:

• inserimos "bolo", "boca", "broca"



Após a inserção de várias palavras começando com b:

• inserimos "bolo", "boca", "broca"



Após a inserção de várias palavras começando com b:

- inserimos "bolo", "boca", "broca"
- a tabela ficou degenerada em lista



boca

bolo

bela

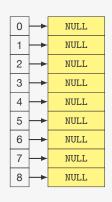
bala

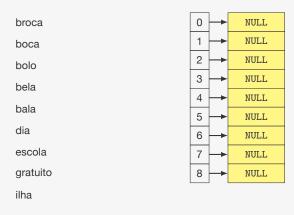
dia

escola

gratuito

ilha

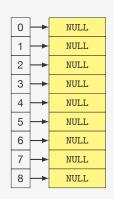




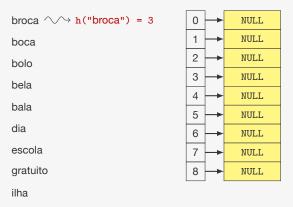
### Corrigindo:

• vamos tentar espalhar melhor

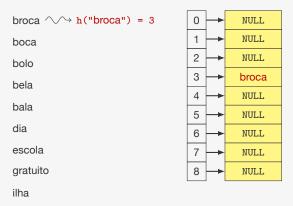




- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)

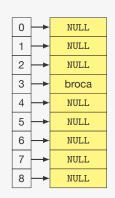


- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



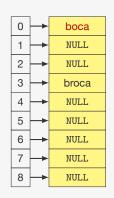
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
holo
bela
bala
dia
escola
gratuito
ilha
```



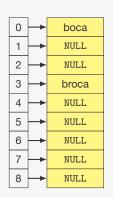
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
holo
bela
bala
dia
escola
gratuito
ilha
```



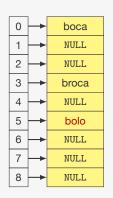
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
bolo \land \land \Rightarrow h("bolo") = 5
bela
bala
dia
escola
gratuito
ilha
```



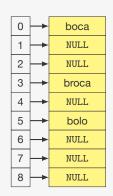
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
bolo \land \land \Rightarrow h("bolo") = 5
bela
bala
dia
escola
gratuito
ilha
```



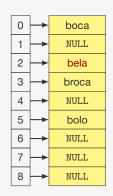
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \rightsquigarrow h("bela") = 2
bala
dia
escola
gratuito
ilha
```



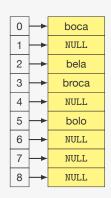
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala
dia
escola
gratuito
ilha
```



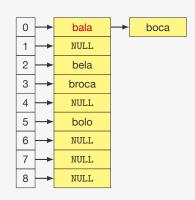
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

```
broca \rightsquigarrow h("broca") = 3
boca \wedge \rightarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia
escola
aratuito
ilha
```



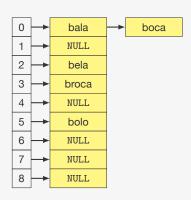
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)





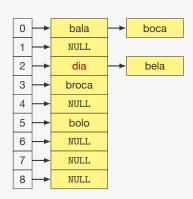
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



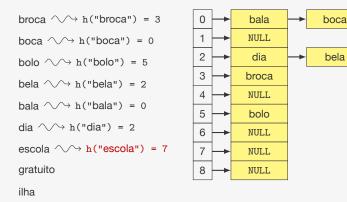


- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

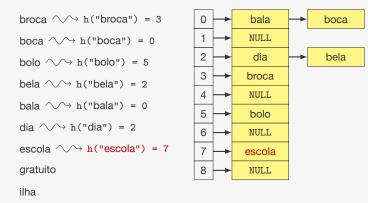




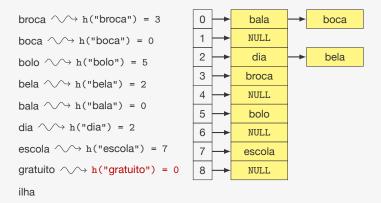
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



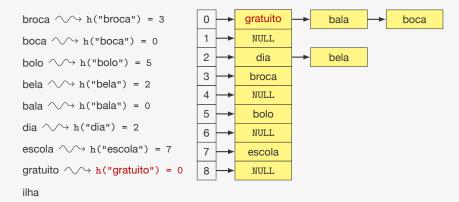
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



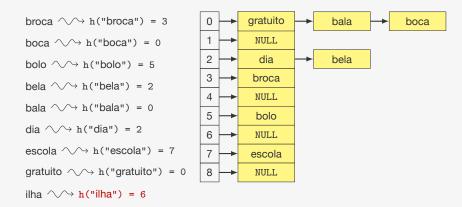
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



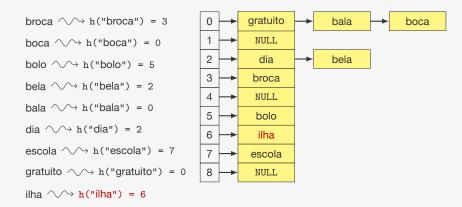
- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)



- vamos tentar espalhar melhor
- usamos um hash da chave (palavra)
- vamos associar a chave a um número inteiro (entre 0 e 8)

Uma função de hashing associa um elemento de um certo conjunto (strings, números, arquivos, etc.) a um número inteiro de tamanho conhecido

Uma função de hashing associa um elemento de um certo conjunto (strings, números, arquivos, etc.) a um número inteiro de tamanho conhecido

Uma tabela de espalhamento é um tipo abstrato de dados para busca em conjuntos dinâmicos cuja implementação tem certas propriedades:

Uma função de hashing associa um elemento de um certo conjunto (strings, números, arquivos, etc.) a um número inteiro de tamanho conhecido

Uma tabela de espalhamento é um tipo abstrato de dados para busca em conjuntos dinâmicos cuja implementação tem certas propriedades:

 os dados são acessado por meio de um vetor de tamanho conhecido

Uma função de hashing associa um elemento de um certo conjunto (strings, números, arquivos, etc.) a um número inteiro de tamanho conhecido

Uma tabela de espalhamento é um tipo abstrato de dados para busca em conjuntos dinâmicos cuja implementação tem certas propriedades:

- os dados são acessado por meio de um vetor de tamanho conhecido
- a posição do vetor é calculada por uma função de hashing

#### Propriedades:

estimativa do tamanho do conjunto de dados deve ser conhecida

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)
    - se temos n itens

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)
    - se temos n itens
    - e uma tabela de tamanho M

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)
    - se temos n itens
    - e uma tabela de tamanho M
    - tempo de acesso é o tempo de calcular a função de hashing + O(n/M)

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)
    - se temos n itens
    - e uma tabela de tamanho M
    - tempo de acesso é o tempo de calcular a função de hashing + O(n/M)
  - chaves agrupadas: pior caso de tempo O(n)

- estimativa do tamanho do conjunto de dados deve ser conhecida
- tempo das operações depende da função de hashing escolhida:
  - chaves bem espalhadas: tempo "quase" O(1)
    - se temos n itens
    - e uma tabela de tamanho M
    - tempo de acesso é o tempo de calcular a função de hashing + O(n/M)
  - chaves agrupadas: pior caso de tempo O(n)
    - Vira uma lista ligada com todos os elementos

## Obtendo funções de hashing

Uma boa função de hashing espalha bem:

## Obtendo funções de hashing

Uma boa função de hashing espalha bem:

• A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- ullet Ou seja, esperamos que cada lista tenha n/M elementos

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- ullet Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

1. Método da divisão

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

- 1. Método da divisão
- 2. Método da multiplicação

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- ullet Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

- 1. Método da divisão
- 2. Método da multiplicação

Hashing perfeito: Se conhecermos todos as chaves a priori, é possível encontrar uma função de hashing injetora

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- ullet Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

- 1. Método da divisão
- 2. Método da multiplicação

Hashing perfeito: Se conhecermos todos as chaves a priori, é possível encontrar uma função de hashing injetora

isto é, não temos colisões

Uma boa função de hashing espalha bem:

- A probabilidade de uma chave ter um hash específico é (aproximadamente) 1/M
- Ou seja, esperamos que cada lista tenha n/M elementos

Métodos genéricos (funcionam bem na prática):

- 1. Método da divisão
- 2. Método da multiplicação

Hashing perfeito: Se conhecermos todos as chaves a priori, é possível encontrar uma função de hashing injetora

- isto é, não temos colisões
- tais funções podem ser difíceis de encontrar

Pressupomos que as chaves são números inteiros

Pressupomos que as chaves são números inteiros

E se não for?

Pressupomos que as chaves são números inteiros

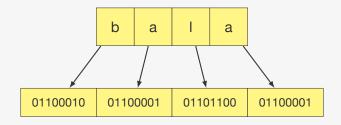
E se não for?

• Reinterpretamos a chave como uma sequência de bits

Pressupomos que as chaves são números inteiros

#### E se não for?

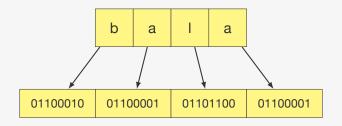
• Reinterpretamos a chave como uma sequência de bits



Pressupomos que as chaves são números inteiros

#### E se não for?

• Reinterpretamos a chave como uma sequência de bits



Assim, "bala" se torna o número 1.650.551.905

obtemos o resto da divisão pelo tamanho M do hashing

obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \operatorname{mod} M$$

ullet obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \bmod M$$

$$h(\text{"bala"}) = 1.650.551.905 \text{ mod } 1783 = 277$$

ullet obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \bmod M$$

Exemplo:

$$h(\text{"bala"}) = 1.650.551.905 \, \text{mod} \, 1783 = 277$$

Escolhendo *M*:

ullet obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \bmod M$$

#### Exemplo:

$$h(\text{"bala"}) = 1.650.551.905 \text{ mod } 1783 = 277$$

#### Escolhendo M:

ullet escolher M como uma potência de 2 não é uma boa ideia

obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \bmod M$$

#### Exemplo:

$$h(\text{"bala"}) = 1.650.551.905 \text{ mod } 1783 = 277$$

#### Escolhendo M:

- ullet escolher M como uma potência de 2 não é uma boa ideia
  - considera apenas os bits menos significativos

obtemos o resto da divisão pelo tamanho M do hashing

$$h(x) = x \bmod M$$

#### Exemplo:

$$h(\text{"bala"}) = 1.650.551.905 \text{ mod } 1783 = 277$$

#### Escolhendo M:

- escolher M como uma potência de 2 não é uma boa ideia
   considera apenas os bits menos significativos
- normalmente escolhemos M como um número primo longe de uma potência de 2

 multiplicamos por um certo valor real A e obtemos a parte fracionária

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

$$h(\text{``bala''}) = \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \ \text{mod} \ 1] \rfloor$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

$$\begin{split} h(\text{``bala''}) &= \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot [1020097177, 4858876 \text{ mod } 1] \rfloor \end{split}$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

$$\begin{split} h(\text{``bala''}) &= \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot [1020097177,4858876 \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot 0,4858876 \rfloor \end{split}$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

$$\begin{split} h(\text{``bala''}) &= \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot [1020097177,4858876 \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot 0,4858876 \rfloor \\ &= \lfloor 497,5489024 \rfloor \end{split}$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

$$\begin{split} h(\text{``bala''}) &= \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot [1020097177,4858876 \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot 0,4858876 \rfloor \\ &= \lfloor 497,5489024 \rfloor = 497 \end{split}$$

- multiplicamos por um certo valor real A e obtemos a parte fracionária
- escolhemos A conveniente, por exemplo  $A = (\sqrt{5} 1)/2$
- posição relativa no vetor não depende de M (pode ser M=1024)

$$h(x) = \lfloor M \left( A \cdot x \bmod 1 \right) \rfloor$$

#### Exemplo:

$$\begin{split} h(\text{``bala''}) &= \lfloor 1024 \cdot [((\sqrt{5}-1)/2 \cdot 1.650.551.905) \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot [1020097177,4858876 \text{ mod } 1] \rfloor \\ &= \lfloor 1024 \cdot 0,4858876 \rfloor \\ &= \lfloor 497,5489024 \rfloor = 497 \end{split}$$

O uso da razão áurea como valor de A é sugestão de Knuth

#### Interface do TAD

```
1 #define MAX 1783
2
3 typedef struct {
4    char chave[10];
5    int dado;
6    No * prox;
7 } No;
```

#### Interface do TAD

```
1 #define MAX 1783
2
3 typedef struct {
4   char chave[10];
5   int dado;
6   No * prox;
7 } No;
8
9 typedef No * p_no;
10
11 typedef struct {
12   p_no vetor[MAX];
13 } Hash;
```

#### Interface do TAD

```
1 #define MAX 1783
3 typedef struct {
    char chave[10];
5 int dado;
6 No * prox;
7 } No;
8
9 typedef No * p no;
10
11 typedef struct {
12  p_no vetor[MAX];
13 } Hash:
14
15 typedef Hash * p_hash;
16
17 p_hash criar_hash();
18
19 void destruir_hash(p_hash t);
20
21 void inserir(p_hash t, char *chave, int dado);
22
23 void remover(p_hash t, char *chave);
24
25 p_no buscar(p_hash t, char *chave);
                                    16
```

## Exemplo de implementação

```
1 int hash(char *chave) {
```

### Exemplo de implementação

```
1 int hash(char *chave) {
2  int i, n = 0;
```

```
1 int hash(char *chave) {
2   int i, n = 0;
3   for (i = 0; i < strlen(chave); i++)
4    n = (256 * n + chave[i]) % MAX;</pre>
```

```
1 int hash(char *chave) {
2   int i, n = 0;
3   for (i = 0; i < strlen(chave); i++)
4    n = (256 * n + chave[i]) % MAX;
5   return n;
6 }</pre>
```

```
1 int hash(char *chave) {
2   int i, n = 0;
3   for (i = 0; i < strlen(chave); i++)
4    n = (256 * n + chave[i]) % MAX;
5   return n;
6 }
7
8 void inserir(p_hash t, char *chave, int dado) {</pre>
```

```
1 int hash(char *chave) {
2    int i, n = 0;
3    for (i = 0; i < strlen(chave); i++)
4        n = (256 * n + chave[i]) % MAX;
5    return n;
6 }
7
8 void inserir(p_hash t, char *chave, int dado) {
9    int n = hash(chave);
10    t->vetor[n] = inserir_lista(t->vetor[n], chave, dado);
11 }
```

```
1 int hash(char *chave) {
2   int i, n = 0;
3   for (i = 0; i < strlen(chave); i++)
4    n = (256 * n + chave[i]) % MAX;
5   return n;
6 }
7
8 void inserir(p_hash t, char *chave, int dado) {
9   int n = hash(chave);
10   t->vetor[n] = inserir_lista(t->vetor[n], chave, dado);
11 }
12
13 void remover(p_hash t, char *chave) {
```

```
1 int hash(char *chave) {
2 int i, n = 0;
3 for (i = 0; i < strlen(chave); i++)</pre>
      n = (256 * n + chave[i]) \% MAX;
5
    return n:
6 }
7
8 void inserir(p_hash t, char *chave, int dado) {
    int n = hash(chave);
10 t->vetor[n] = inserir_lista(t->vetor[n], chave, dado);
11 }
12
13 void remover(p_hash t, char *chave) {
14 int n = hash(chave);
t->vetor[n] = remover lista(t->vetor[n], chave);
16 }
```

Sabendo a função de hashing, podemos prejudicar o programa:

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Sabendo a função de hashing, podemos prejudicar o programa:

insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Sabendo a função de hashing, podemos prejudicar o programa:

insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

Sabendo a função de hashing, podemos prejudicar o programa:

insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

Uma boa função de hashing aleatória:

fixe p um primo maior do que M

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

- fixe p um primo maior do que M
- escolha  $\mathbf{a} \in \{1, \dots, p\}$  e  $\mathbf{b} \in \{0, \dots, p\}$  uniform. ao acaso

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

- fixe p um primo maior do que M
- escolha  $\mathbf{a} \in \{1, \dots, p\}$  e  $\mathbf{b} \in \{0, \dots, p\}$  uniform. ao acaso
- defina  $h_{a,b}(k) = ((ak+b) \mod p) \mod M$

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

- fixe p um primo maior do que M
- escolha  $\mathbf{a} \in \{1, \dots, p\}$  e  $\mathbf{b} \in \{0, \dots, p\}$  uniform. ao acaso
- defina  $h_{a,b}(k) = ((ak+b) \mod p) \mod M$
- sabemos que essa função espalha bem

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

- fixe p um primo maior do que M
- escolha  $\mathbf{a} \in \{1, \dots, p\}$  e  $\mathbf{b} \in \{0, \dots, p\}$  uniform. ao acaso
- defina  $h_{a,b}(k) = ((ak+b) \mod p) \mod M$
- sabemos que essa função espalha bem
  - a probabilidade de colisão é no máximo 1/M

Sabendo a função de hashing, podemos prejudicar o programa:

• insira muitos elementos com o mesmo hash

Como nos proteger de um adversário malicioso?

Podemos escolher a função de hashing aleatoriamente

- fixe p um primo maior do que M
- escolha  $\mathbf{a} \in \{1, \dots, p\}$  e  $\mathbf{b} \in \{0, \dots, p\}$  uniform. ao acaso
- defina  $h_{a,b}(k) = ((ak+b) \mod p) \mod M$
- sabemos que essa função espalha bem
  - a probabilidade de colisão é no máximo 1/M
  - é um hashing universal

Existe uma alternativa para a implementação de tabela de espalhamento

Existe uma alternativa para a implementação de tabela de espalhamento

Endereçamento aberto:

Existe uma alternativa para a implementação de tabela de espalhamento

Endereçamento aberto:

os dados são guardados no próprio vetor

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

#### Características:

 evita percorrer usando ponteiros e alocação e deslocação de memória (malloc e free)

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

- evita percorrer usando ponteiros e alocação e deslocação de memória (malloc e free)
- se a tabela encher, deve recriar uma tabela maior

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

- evita percorrer usando ponteiros e alocação e deslocação de memória (malloc e free)
- se a tabela encher, deve recriar uma tabela maior
  - e mudar a função de hashing

Existe uma alternativa para a implementação de tabela de espalhamento

### Endereçamento aberto:

- os dados são guardados no próprio vetor
- colisões são colocadas em posições livres da tabela

- evita percorrer usando ponteiros e alocação e deslocação de memória (malloc e free)
- se a tabela encher, deve recriar uma tabela maior
  - e mudar a função de hashing
- remoção é mais complicada

broca boca

bolo

bela

bala

dia

escola

gratuito

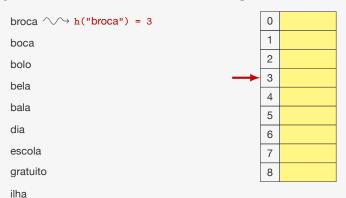
ilha

```
broca \rightsquigarrow h("broca") = 3
boca
bolo
bela
bala
dia
escola
gratuito
ilha
```

0	
1	
2	
3	
4	
5	
6	
7	
8	

### Inserindo:

procuramos posição



- procuramos posição
- se houver espaço, guardamos

```
broca \rightsquigarrow h("broca") = 3
boca
bolo
bela
bala
dia
escola
gratuito
ilha
```

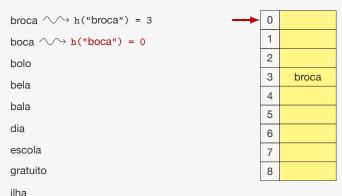
0	
1	
2	
3	broca
4	
5	
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos

```
broca \rightsquigarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo
bela
bala
dia
escola
gratuito
ilha
```

0	
1	
2	
3	broca
4	
5	
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos



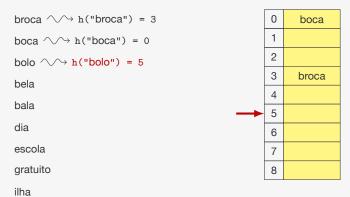
- procuramos posição
- se houver espaço, guardamos

0	boca
1	
2	
3	broca
4	
5	
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos

0	boca
1	
2	
3	broca
4	
5	
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos



- procuramos posição
- se houver espaço, guardamos

```
broca \rightsquigarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela
hala
dia
escola
gratuito
ilha
```

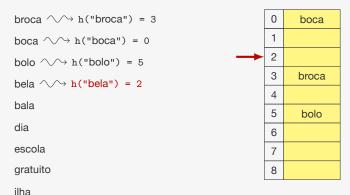
0	boca
1	
2	
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos

```
broca \rightsquigarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \rightsquigarrow h("bela") = 2
hala
dia
escola
gratuito
ilha
```

0	boca
1	
2	
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos



- procuramos posição
- se houver espaço, guardamos

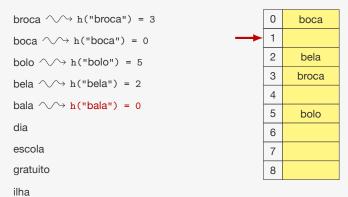
```
broca \rightsquigarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \rightsquigarrow h("bela") = 2
hala
dia
escola
gratuito
ilha
```

0	boca
1	
2	bela
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos

broca √→ h("broca") = 3	0	boca
boca $\rightsquigarrow$ h("boca") = 0	1	
bolo	2	bela
bela ∕ h("bela") = 2	3	broca
	4	
$bala \longrightarrow h("bala") = 0$	5	bolo
dia	6	
escola	7	
gratuito	8	
ilha		

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)



- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia
escola
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia
escola
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \land \land \rightarrow h("dia") = 2
escola
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \land \land \rightarrow h("dia") = 2
escola
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

broca $\rightsquigarrow$ h("broca") = 3	0	boca
boca $\rightsquigarrow$ h("boca") = 0	1	bala
bolo	2	bela
bela ∕ h("bela") = 2	3	broca
	4	
$bala \wedge h("bala") = 0$	5	bolo
$dia \wedge h("dia") = 2$	6	
escola	7	
gratuito	8	

#### Inserindo:

ilha

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                         0
                                                                                 boca
                                                                                  bala
boca \rightsquigarrow h("boca") = 0
                                                                                  bela
bolo \rightsquigarrow h("bolo") = 5
                                                                                 broca
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
                                                                                  bolo
dia \land \land \rightarrow h("dia") = 2
                                                                         6
escola
                                                                         7
aratuito
                                                                         8
ilha
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                         0
                                                                                 boca
                                                                                  bala
boca \rightsquigarrow h("boca") = 0
                                                                                  bela
bolo \rightsquigarrow h("bolo") = 5
                                                                         3
                                                                                 broca
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
                                                                                  bolo
dia \land \land \rightarrow h("dia") = 2
                                                                         6
escola
                                                                         7
aratuito
                                                                         8
ilha
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \land \land \rightarrow h("dia") = 2
escola
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \sim h("dia") = 2
escola \wedge \rightarrow h("escola") = 7
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	
7	
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                     0
                                                                            boca
                                                                             bala
boca \rightsquigarrow h("boca") = 0
                                                                             bela
bolo \rightsquigarrow h("bolo") = 5
                                                                     3
                                                                            broca
bela \wedge \wedge \rightarrow h("bela") = 2
                                                                              dia
bala \rightsquigarrow h("bala") = 0
                                                                             bolo
dia \sim h("dia") = 2
                                                                     6
escola \wedge \rightarrow h("escola") = 7
aratuito
                                                                     8
ilha
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \sim h("dia") = 2
escola \wedge \rightarrow h("escola") = 7
gratuito
ilha
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	
7	escola
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \sim h("dia") = 2
escola \wedge \rightarrow h("escola") = 7
gratuito \wedge \rightarrow h("gratuito") = 0
ilha
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	
7	escola
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

broca $\sim h("broca") = 3$
boca $\sim h("boca") = 0$
bolo \square h("bolo") = 5
bela $\wedge \rightarrow h("bela") = 2$
bala $\wedge \rightarrow h("bala") = 0$
$dia \wedge h("dia") = 2$
escola $\wedge \rightarrow h("escola") = 7$
gratuito $\wedge \rightarrow h("gratuito") = 0$
ilha

<b>&gt;</b>	0	boca
	1	bala
	2	bela
	3	broca
	4	dia
	5	bolo
	6	
	7	escola
	8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

broca $\rightsquigarrow$ h("broca") = 3	0	boca
boca $\rightsquigarrow$ h("boca") = 0	1	bala
bolo $\rightsquigarrow$ h("bolo") = 5	2	bela
bela ∕∕→ h("bela") = 2	3	broca
, , , ,	4	dia
bala $\rightsquigarrow$ h("bala") = 0	5	bolo
$dia \wedge h("dia") = 2$	6	
escola $\sim h("escola") = 7$	7	escola
gratuito $\rightsquigarrow h("gratuito") = 0$	8	
ilha		

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo  $\underline{M}$ )

broca $\rightsquigarrow$ h("broca") = 3	0	boca
boca $\rightsquigarrow$ h("boca") = 0	1	bala
bolo	2	bela
bela	3	broca
	4	dia
$bala \wedge h("bala") = 0$	5	bolo
$dia \wedge h("dia") = 2$	6	
escola \square h("escola") = 7	7	escola
gratuito $\rightsquigarrow h("gratuito") = 0$	8	
ilha		

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                    0
                                                                            boca
                                                                             bala
boca \rightsquigarrow h("boca") = 0
                                                                             bela
bolo \rightsquigarrow h("bolo") = 5
                                                                            broca
bela \wedge \wedge \rightarrow h("bela") = 2
                                                                             dia
bala \rightsquigarrow h("bala") = 0
                                                                             bolo
dia \sim h("dia") = 2
                                                                    6
escola \rightsquigarrow h("escola") = 7
                                                                    7
                                                                           escola
gratuito \wedge \rightarrow h("gratuito") = 0
                                                                    8
ilha
```

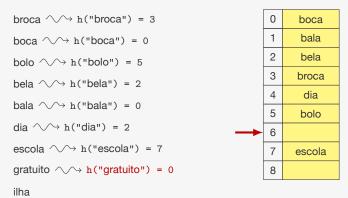
- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                    0
                                                                            boca
                                                                             bala
boca \rightsquigarrow h("boca") = 0
                                                                             bela
bolo \rightsquigarrow h("bolo") = 5
                                                                    3
                                                                            broca
bela \wedge \wedge \rightarrow h("bela") = 2
                                                                             dia
bala \rightsquigarrow h("bala") = 0
                                                                             bolo
dia \sim h("dia") = 2
                                                                    6
escola \rightsquigarrow h("escola") = 7
                                                                    7
                                                                           escola
gratuito \wedge \rightarrow h("gratuito") = 0
                                                                    8
ilha
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                    0
                                                                            boca
                                                                             bala
boca \rightsquigarrow h("boca") = 0
                                                                             bela
bolo \rightsquigarrow h("bolo") = 5
                                                                    3
                                                                            broca
bela \wedge \wedge \rightarrow h("bela") = 2
                                                                             dia
bala \rightsquigarrow h("bala") = 0
                                                                             bolo
dia \sim h("dia") = 2
                                                                    6
escola \rightsquigarrow h("escola") = 7
                                                                    7
                                                                           escola
gratuito \wedge \rightarrow h("gratuito") = 0
                                                                    8
ilha
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)



- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \wedge \rightarrow h("bela") = 2
bala \rightsquigarrow h("bala") = 0
dia \sim h("dia") = 2
escola \wedge \rightarrow h("escola") = 7
gratuito \wedge \rightarrow h("gratuito") = 0
ilha
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	gratuito
7	escola
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \rightarrow h("bela") = 2
bala \wedge \wedge \rightarrow h("bala") = 0
dia \sim h("dia") = 2
escola \rightsquigarrow h("escola") = 7
\alpha aratuito \wedge \wedge \rightarrow h(\alpha + 1) = 0
ilha \wedge \wedge \rightarrow h("ilha") = 6
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	gratuito
7	escola
8	

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                                  boca
                                                                          0
                                                                                   bala
boca \rightsquigarrow h("boca") = 0
                                                                                   bela
bolo \rightsquigarrow h("bolo") = 5
                                                                          3
                                                                                  broca
bela \wedge \rightarrow h("bela") = 2
                                                                          4
                                                                                    dia
bala \wedge \wedge \rightarrow h("bala") = 0
                                                                                   holo
dia \land \land \rightarrow h("dia") = 2
                                                                                 gratuito
escola \rightsquigarrow h("escola") = 7
                                                                          7
                                                                                 escola
gratuito \rightsquigarrow h("gratuito") = 0
                                                                          8
ilha \wedge \wedge \rightarrow h("ilha") = 6
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                                  boca
                                                                          0
                                                                                   bala
boca \rightsquigarrow h("boca") = 0
                                                                                   bela
bolo \rightsquigarrow h("bolo") = 5
                                                                          3
                                                                                  broca
bela \wedge \rightarrow h("bela") = 2
                                                                          4
                                                                                   dia
bala \wedge \wedge \rightarrow h("bala") = 0
                                                                                   holo
dia \land \land \rightarrow h("dia") = 2
                                                                                gratuito
                                                                          6
escola \rightsquigarrow h("escola") = 7
                                                                                 escola
gratuito \rightsquigarrow h("gratuito") = 0
                                                                          8
ilha \wedge \wedge \rightarrow h("ilha") = 6
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
                                                                                   boca
                                                                          0
                                                                                   bala
boca \rightsquigarrow h("boca") = 0
                                                                                   bela
bolo \rightsquigarrow h("bolo") = 5
                                                                          3
                                                                                  broca
bela \wedge \rightarrow h("bela") = 2
                                                                                    dia
bala \wedge \wedge \rightarrow h("bala") = 0
                                                                                   holo
dia \land \land \rightarrow h("dia") = 2
                                                                                 gratuito
                                                                          6
escola \rightsquigarrow h("escola") = 7
                                                                          7
                                                                                  escola
gratuito \wedge \rightarrow h("gratuito") = 0
ilha \wedge \wedge \rightarrow h("ilha") = 6
```

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

```
broca \wedge \wedge \rightarrow h("broca") = 3
boca \rightsquigarrow h("boca") = 0
bolo \rightsquigarrow h("bolo") = 5
bela \wedge \rightarrow h("bela") = 2
bala \wedge \wedge \rightarrow h("bala") = 0
dia \sim h("dia") = 2
escola \rightsquigarrow h("escola") = 7
\alpha aratuito \wedge \wedge \rightarrow h(\alpha + 1) = 0
ilha \wedge \wedge \rightarrow h("ilha") = 6
```

0	boca
1	bala
2	bela
3	broca
4	dia
5	bolo
6	gratuito
7	escola
8	ilha

- procuramos posição
- se houver espaço, guardamos
- se não houver espaço, procuramos a próxima posição livre (módulo M)

Como fazer uma busca com endereçamento aberto?

Basta simular a inserção:

- Basta simular a inserção:
  - Calcule a função de hashing

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

Como fazer uma busca com endereçamento aberto?

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

Como fazer uma busca com endereçamento aberto?

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

O que é um espaço vazio em um vetor?

Se for um vetor de ponteiros, pode ser NULL

### Como fazer uma busca com endereçamento aberto?

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

- Se for um vetor de ponteiros, pode ser NULL
- Se n\u00e3o for um vetor de ponteiros, precisa ser um elemento dummy

### Como fazer uma busca com endereçamento aberto?

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

- Se for um vetor de ponteiros, pode ser NULL
- Se n\u00e3o for um vetor de ponteiros, precisa ser um elemento dummy
  - Ou um valor que nunca será usado

### Como fazer uma busca com endereçamento aberto?

- Basta simular a inserção:
  - Calcule a função de hashing
  - Percorra a tabela em sequência procurando pela chave
  - Se encontrar a chave, devolva o item correspondente
  - Se encontrar um espaço vazio, devolva NULL

- Se for um vetor de ponteiros, pode ser NULL
- Se n\u00e3o for um vetor de ponteiros, precisa ser um elemento dummy
  - Ou um valor que nunca será usado
  - Ou ter um campo indicando que é dummy

Como fazer a remoção com endereçamento aberto?

• Não podemos apenas remover os elementos da tabela

- Não podemos apenas remover os elementos da tabela
  - Por que?

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco
  - reinserimos os mesmos no hash para ir para a posição correta

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco
  - reinserimos os mesmos no hash para ir para a posição correta
  - é custoso e tem que ser implementado com cuidado

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco
  - reinserimos os mesmos no hash para ir para a posição correta
  - é custoso e tem que ser implementado com cuidado
- Opção 2: trocamos por um item dummy indicando que o item foi removido

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco
  - reinserimos os mesmos no hash para ir para a posição correta
  - é custoso e tem que ser implementado com cuidado
- Opção 2: trocamos por um item dummy indicando que o item foi removido
  - mas não pode ser o mesmo que indica espaço vazio

- Não podemos apenas remover os elementos da tabela
  - Por que?
    - Quebraria a busca...
- Opção 1: fazemos o rehash de todos os elementos que estão a seguir no mesmo bloco
  - reinserimos os mesmos no hash para ir para a posição correta
  - é custoso e tem que ser implementado com cuidado
- Opção 2: trocamos por um item dummy indicando que o item foi removido
  - mas não pode ser o mesmo que indica espaço vazio
- Opção 3: marcamos o item como removido usando um campo adicional

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

Inserção:

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

### Inserção:

Calculamos a função hashing e temos um resultado h

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

#### Busca:

Calculamos a função hashing e temos um resultado h

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

- Calculamos a função hashing e temos um resultado h
- Procuramos o item em sequência

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

- Calculamos a função hashing e temos um resultado h
- Procuramos o item em sequência
  - Veja se ao encontrar o item, ele não foi removido

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

- Calculamos a função hashing e temos um resultado h
- Procuramos o item em sequência
  - Veja se ao encontrar o item, ele não foi removido
- Pare ao encontrar uma posição vazia

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

- Calculamos a função hashing e temos um resultado h
- Procuramos o item em sequência
  - Veja se ao encontrar o item, ele não foi removido
- Pare ao encontrar uma posição vazia
  - Passe por cima de itens removidos

Se fizermos a remoção marcando o item como removido, precisamos mudar a inserção e a busca

## Inserção:

- Calculamos a função hashing e temos um resultado h
- Inserimos na primeira posição vazia ou com item removido a partir de h

- Calculamos a função hashing e temos um resultado h
- Procuramos o item em sequência
  - Veja se ao encontrar o item, ele n\u00e3o foi removido
- Pare ao encontrar uma posição vazia
  - Passe por cima de itens removidos
- Cuidado para não ciclar...

É como a sondagem linear:

É como a sondagem linear:

• Quando detectamos conflito, ao invés de dar um pulo de 1

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

Cuidados:

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

hash<sub>2</sub>(k) nunca pode ser zero

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

- $hash_2(k)$  nunca pode ser zero
- hash<sub>2</sub>(k) precisa ser co-primo com M

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

- $hash_2(k)$  nunca pode ser zero
- hash<sub>2</sub>(k) precisa ser co-primo com M
  - garante que as sequências são longas

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

- $hash_2(k)$  nunca pode ser zero
- hash<sub>2</sub>(k) precisa ser co-primo com M
  - garante que as sequências são longas

## Exemplos:

É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

- $hash_2(k)$  nunca pode ser zero
- hash<sub>2</sub>(k) precisa ser co-primo com M
  - garante que as sequências são longas

### Exemplos:

• Escolha M como uma potência de 2 e faça que  $hash_2(k)$  seja sempre ímpar

## Hashing duplo

## É como a sondagem linear:

- Quando detectamos conflito, ao invés de dar um pulo de 1
- damos um pulo h(k,i) calculado a partir de uma segunda função de hashing

Isto é,

$$h(k,i) = (hash_1(k) + i \cdot hash_2(k)) \mod M$$

#### Cuidados:

- $hash_2(k)$  nunca pode ser zero
- hash<sub>2</sub>(k) precisa ser co-primo com M
  - garante que as sequências são longas

### Exemplos:

• Escolha M como uma potência de 2 e faça que  $hash_2(k)$  seja sempre ímpar

24

 Escolha M como um número primo e faça que hash<sub>2</sub>(k) < M</li>

Sondagem linear - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.5	2.0	3.0	5.5
sem sucesso	2.5	5.0	8.5	55.5

25

<sup>&</sup>lt;sup>1</sup>Baseado em Sedgewick, R. Algorithms in C, third edition, Addison-Wesley. 1998.

Sondagem linear - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.5	2.0	3.0	5.5
sem sucesso	2.5	5.0	8.5	55.5

Hashing duplo - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.4	1.6	1.8	2.6
sem sucesso	1.5	2.0	3.0	5.5

<sup>&</sup>lt;sup>1</sup>Baseado em Sedgewick, R. Algorithms in C, third edition, Addison-Wesley. 1998.

Sondagem linear - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.5	2.0	3.0	5.5
sem sucesso	2.5	5.0	8.5	55.5

Hashing duplo - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.4	1.6	1.8	2.6
sem sucesso	1.5	2.0	3.0	5.5

De qualquer forma, é muito importante não deixar a tabela encher muito:

<sup>&</sup>lt;sup>1</sup>Baseado em Sedgewick, R. Algorithms in C, third edition, Addison-Wesley. 1998.

Sondagem linear - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.5	2.0	3.0	5.5
sem sucesso	2.5	5.0	8.5	55.5

Hashing duplo - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.4	1.6	1.8	2.6
sem sucesso	1.5	2.0	3.0	5.5

De qualquer forma, é muito importante não deixar a tabela encher muito:

• Você pode aumentar o tamanho da tabela dinamicamente

<sup>&</sup>lt;sup>1</sup>Baseado em Sedgewick, R. Algorithms in C, third edition, Addison-Wesley. 1998.

Sondagem linear - tempo de busca médio

n/M	1/2	2/3	3/4	9/10
com sucesso	1.5	2.0	3.0	5.5
sem sucesso	2.5	5.0	8.5	55.5

Hashing duplo - tempo de busca médio

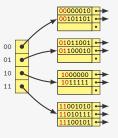
n/M	1/2	2/3	3/4	9/10
com sucesso	1.4	1.6	1.8	2.6
sem sucesso	1.5	2.0	3.0	5.5

De qualquer forma, é muito importante não deixar a tabela encher muito:

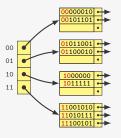
- Você pode aumentar o tamanho da tabela dinamicamente
- Porém, precisa fazer um rehash de cada elemento para a nova tabela

<sup>&</sup>lt;sup>1</sup>Baseado em Sedgewick, R. Algorithms in C, third edition, Addison-Wesley. 1998.

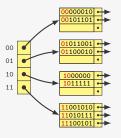
Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



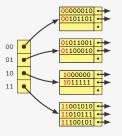
Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



### Espalhamento Extensível:

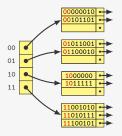
 calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



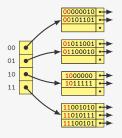
- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



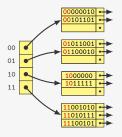
- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório
  - cada entrada do diretório aponta para uma página

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



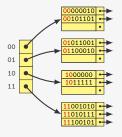
- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório
  - cada entrada do diretório aponta para uma página
  - página tem chaves que coincidem nos primeiros  $k \leq d$  bits

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco



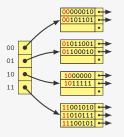
- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório
  - cada entrada do diretório aponta para uma página
  - página tem chaves que coincidem nos primeiros  $k \leq d$  bits
  - várias entradas podem apontar para a mesma página

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco

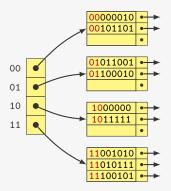


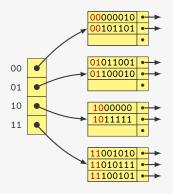
- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório
  - cada entrada do diretório aponta para uma página
  - página tem chaves que coincidem nos primeiros  $k \leq d$  bits
  - várias entradas podem apontar para a mesma página
    - assim não precisamos ter 2<sup>d</sup> páginas

Hashing também pode ser usado para o acesso ou escrita de arquivos em disco

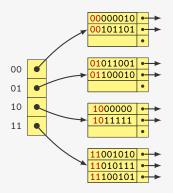


- calcule função de hashing para transformar chave em uma sequências de bits de tamanho fixo
- indexamos pelos primeiros d bits em um diretório
  - cada entrada do diretório aponta para uma página
  - página tem chaves que coincidem nos primeiros  $k \leq d$  bits
  - várias entradas podem apontar para a mesma página
    - assim não precisamos ter 2<sup>d</sup> páginas
- se preciso, aumentamos  $\frac{d}{d}$  na hora de inserir



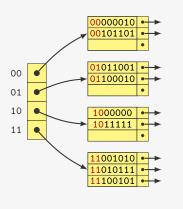


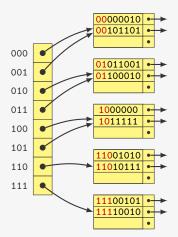
Inserindo 11110010



#### Inserindo 11110010

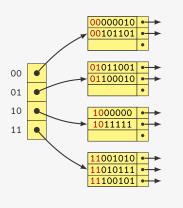
• Precisa expandir o diretório pois não há espaço na página

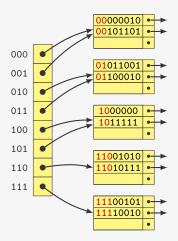




#### Inserindo 11110010

• Precisa expandir o diretório pois não há espaço na página





#### Inserindo 11110010

• Precisa expandir o diretório pois não há espaço na página

27

Para n registros, o Espalhamento Extensível usa 1.44n/M páginas e o diretório tem  $3.92n^{\frac{M+1}{M}}/M$  entradas em média

Hashing é uma boa estrutura de dados para

Hashing é uma boa estrutura de dados para

inserir, remover e buscar dados pela sua chave rapidamente

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

### Escolhendo a implementação:

Sondagem linear é o mais rápido se a tabela for esparsa

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

- Sondagem linear é o mais rápido se a tabela for esparsa
- Hashing duplo usa melhor a memória

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

- Sondagem linear é o mais rápido se a tabela for esparsa
- Hashing duplo usa melhor a memória
  - mas gasta mais tempo para computar a segunda função de hash

Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

- Sondagem linear é o mais rápido se a tabela for esparsa
- Hashing duplo usa melhor a memória
  - mas gasta mais tempo para computar a segunda função de hash
- Encadeamento separado é mais fácil de implementar

### Hashing é uma boa estrutura de dados para

- inserir, remover e buscar dados pela sua chave rapidamente
- com uma boa função de hashing, essas operações levam tempo O(1)
- mas não é boa se quisermos fazer operação relacionadas a ordem das chaves

- Sondagem linear é o mais rápido se a tabela for esparsa
- Hashing duplo usa melhor a memória
  - mas gasta mais tempo para computar a segunda função de hash
- Encadeamento separado é mais fácil de implementar
  - Usa memória a mais para os ponteiros

Além disso, funções de hashing podem ser aplicada em verificações de paridade:

 Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:

- Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:
  - dígitos verificadores

- Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:
  - dígitos verificadores
  - sequências de verificação para arquivos (MD5 e SHA)

- Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:
  - dígitos verificadores
  - sequências de verificação para arquivos (MD5 e SHA)
- Guardamos o hash de uma senha no banco de dados ao invés da senha em si

- Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:
  - dígitos verificadores
  - sequências de verificação para arquivos (MD5 e SHA)
- Guardamos o hash de uma senha no banco de dados ao invés da senha em si
  - evitamos vazamento de informação em caso de ataque

- Para evitar erros de transmissão, podemos, além de informar uma chave, transmitir o resultado da função de hashing. Exemplos:
  - dígitos verificadores
  - sequências de verificação para arquivos (MD5 e SHA)
- Guardamos o hash de uma senha no banco de dados ao invés da senha em si
  - evitamos vazamento de informação em caso de ataque
  - mas temos que garantir que a probabilidade de duas senhas terem o mesmo hash seja ínfima...