



Universidade Federal do ABC
Centro de Matemática, Computação e Cognição

**Métodos de compressão de dados com
pré-processamento via clusterização aplicados a
contextos linguísticos**

Lucas Silva Amorim

Santo André - SP, Agosto de 2022

Lucas Silva Amorim

Métodos de compressão de dados com pré-processamento via clusterização aplicados a contextos linguísticos

Projeto de Graduação apresentado ao Centro de Matemática, Computação e Cognição, como parte dos requisitos necessários para a obtenção do Título de Bacharel em Ciência da Computação.

Universidade Federal do ABC – UFABC
Centro de Matemática, Computação e Cognição
Bacharelado em Ciência da Computação.

Orientador: Prof.^a Dr.^a Cristiane M. Sato

Santo André - SP
Agosto de 2022

Resumo

Segundo a ABNT, o resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento. A ordem e a extensão destes itens dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. O resumo deve ser precedido da referência do documento, com exceção do resumo inserido no próprio documento. Umas 10 linhas (...) As palavras-chave devem figurar logo abaixo do resumo, antecidas da expressão Palavras-chave:, separadas entre si por ponto e finalizadas também por ponto.

Palavras-chaves: latex. abntex. editoração de texto.

Abstract

This is the english abstract.

Keywords: latex. abntex. text editoration.

Sumário

I	FUNDAMENTAÇÃO TEÓRICA	3
1	CONCEITOS E DEFINIÇÕES FUNDAMENTAIS EM COMPRESSÃO DE DADOS	5
1.1	Código	5
1.1.1	Códigos unicamente decodificáveis e livres de prefixo	6
1.2	Relações fundamentais com a Teoria da Informação	6
1.2.1	Distribuição de Probabilidade e Esperança	7
1.2.2	Comprimento médio do código	7
1.2.3	Entropia	8
1.2.4	Comprimento de Código e Entropia	8
II	ALGORITMOS	13
2	ALGORITMOS DE COMPRESSÃO SEM PERDA	15
2.1	Código de Huffman	16
2.1.1	Análise Assintótica	16
2.1.2	Corretude	16
	REFERÊNCIAS	19

Introdução

Motivação

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

Objetivos

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

Parte I

Fundamentação Teórica

1 Conceitos e definições fundamentais em compressão de dados

Este capítulo apresenta algumas definições e conceitos fundamentais para o entendimento das técnicas de compressão que serão discutidas em capítulos posteriores.

1.1 Código

Dado um conjunto A , usaremos a notação A^+ para definir o conjunto que contém todas as cadeias formadas pelas possíveis combinações de A . Um **código** C mapeia uma **mensagem** $m \in M$ para uma **cadeia de códigos** do alfabeto W (onde M é o **alfabeto de origem** e W **alfabeto código**). Chamaremos essa cadeia de códigos de **palavra-código**, denotada por w . Dentro deste contexto, definimos o **comprimento** da palavra-código w como $l(w)$, um **inteiro positivo** que representa o tamanho da cadeia que compõe a palavra-código w . Tome como exemplo o alfabeto de origem $M = \{a, b, c\}$ e o alfabeto código $W = \{0, 1\}$ composto somente por valores binários, poderíamos definir o código C da seguinte forma:

Tabela 1 – Tabela do código C

mensagem de origem	palavra-código
a	1
b	01
c	00

Isto é, o código C pode ser representado como uma função $C : M \rightarrow W^+$. Neste exemplo, o **comprimento** da palavra-código associado à mensagem “a” é dado por $l(C(a)) = 1$.

As palavras-código associadas a cada mensagem podem ter um tamanho *fixo* ou *variável*. Códigos nos quais os alfabetos possuem um comprimento fixo são chamados de **códigos de comprimento fixo**, enquanto os que possuem alfabetos de comprimento variáveis são chamados **códigos de comprimento variável**. Provavelmente o exemplo mais conhecido de código de **comprimento fixo** seja código ASCII, que mapeia 64 símbolos alfa-numéricos (ou 256 em sua versão estendida) para palavras-código de 8 bits. Todavia, no contexto de compressão de dados procuramos construir códigos que podem variar em seu comprimento baseados na sua probabilidade associada, afim de reduzir o tamanho médio da *string* original ao codificá-la.

1.1.1 Códigos unicamente decodificáveis e livres de prefixo

Um código é **distinto** se pode ser representado como uma função **bijetora**, i.e, $\forall m_1, m_2 \in M, C(m_1) \neq C(m_2)$. Um código distinto é dito **unicamente decodificável** se qualquer palavra-código pode ser identificada quando imersa em uma sequência de palavras-código.

Um **código livre de prefixo** é um código unicamente decodificável em que nenhuma palavra-código é prefixo de outra. Por exemplo, o código que possui sua imagem no conjunto de palavras-código $W^+ := \{1, 01, 000, 001\}$ não possui nenhuma cadeia que é prefixo de outra, portanto é considerado um **código livre de prefixo**. Códigos livres de prefixo podem ser *decodificados instantaneamente*, pois, ao processar uma cadeia de sequência de palavras-código podemos decodificar cada uma delas sem precisar verificar o início da seguinte.

Um código livre de prefixo em que $W := \{0, 1\}$ pode ser modelado por uma **árvore binária**. Imagine que cada mensagem $m \in M$ é uma folha. A palavra-código $C(m)$ é o caminho p da raiz até a folha m , de maneira em que, para cada nó percorrido concatenamos um bit a p ("0" quando o nó está a esquerda e "1" quando está a direita), tal árvore é chamada **árvore do código livre de prefixo**. Tomando como exemplo o código representado pela Tabela 1 (claramente um código livre de prefixo), podemos representá-lo por uma árvore livre de prefixo da seguinte forma:

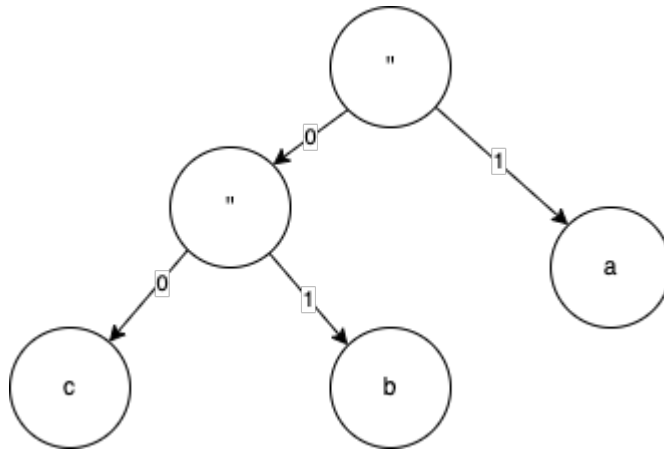


Figura 1 – Árvore livre de prefixo

1.2 Relações fundamentais com a Teoria da Informação

A codificação é comumente dividida em duas componentes diferentes: *modelo* e *codificador*. O *modelo* identifica a distribuição de probabilidade das mensagens baseado em sua semântica e estrutura. O *codificador* toma vantagem de um possível *bias* apontado pela modelagem, e utiliza as probabilidades associadas para reduzir a quantidade de dados necessária para representar a mesma informação (substituindo as mensagens que

ocorrem com maior frequência por símbolos menores). Isso significa que, a codificação está diretamente ligada as probabilidades associadas a cada mensagem.

Nesta seção, vamos construir o embasamento teórico necessário para entender a relação entre as probabilidades associadas e o comprimento das mensagens, e consequentemente criar uma noção dos parâmetros que devem ser maximizados para alcançar uma codificação eficiente.

1.2.1 Distribuição de Probabilidade e Esperança

Dado um experimento e um espaço amostral Ω , uma **variável aleatória** X associa um número real a cada um dos possíveis resultados em Ω . Em outras palavras, X é uma função que mapeia os elementos do espaço amostral para números reais. Uma variável aleatória é chamada discreta quando os valores dos experimentos associados a ela são números finitos ou ao menos infinitos que podem ser contados. Podemos descrever melhor uma variável aleatória, atribuindo probabilidades sobre os valores que esta pode assumir. Esses valores são atribuídos pela **função de densidade de probabilidade**, denotada por p_X . Portanto, a probabilidade do evento $\{ X = x \}$ é a função de distribuição de probabilidade aplicada a x , *i.e.*, $p_X(x)$.

$$p_X(x) = P(\{X = x\}) \quad (1.1)$$

Note que, a variável aleatória pode assumir qualquer um dos valores no espaço amostral que possuem uma probabilidade $P > 0$, portanto

$$\sum_{x \in im_X} p_X(x) = 1. \quad (1.2)$$

O **valor esperado** (ou **esperança**) da variável aleatória X é definido como

$$\mathbf{E}[X] = \sum_{x \in im_X} xp_X(x). \quad (1.3)$$

1.2.2 Comprimento médio do código

Seja p a distribuição de probabilidade associada ao alfabeto de origem M . Assuma que C é um código tal que $C(m) = w$, definimos o **tamanho médio** de C como:

$$l_a(C) = \sum_{m \in M} p(m)l(C(m)) \quad (1.4)$$

Um código C unicamente decodificável é **ótimo** se $l_a(C)$ é mínimo, isto é, para qualquer código unicamente decodificável C' temos que:

$$l_a(C) \leq l_a(C') \quad (1.5)$$

1.2.3 Entropia

A **entropia de Shannon** aplica as noções de entropia física (que representa a aleatoriedade de um sistema) à Teoria da Informação. Dado um espaço de probabilidade X e a função p sendo a distribuição de probabilidade associada a X , definimos **entropia** como:

$$H(X, p) = \sum_{x \in X} p(x) \log_2 \frac{1}{p(x)} \quad (1.6)$$

Por esta definição temos que quanto menor o *bias* da função de distribuição de probabilidade relacionada ao sistema, maior a sua entropia. Em outras palavras, a entropia de um sistema esta intimamente ligada a sua "desordem".

Shannon (incluir referencia papper do Shannon) aplica o mesmo conceito de entropia no contexto da Teoria da Informação, "substituindo" o conjunto de estados S pelo conjunto de mensagem M , isto é, M é interpretado como um conjunto de possíveis mensagens, tendo como $p(m)$ a probabilidade de $m \in M$. Baseado na mesma premissa, Shannon mede a informação contida em uma mensagem da seguinte forma:

$$i(m) = \log_2 \frac{1}{p(m)}. \quad (1.7)$$

1.2.4 Comprimento de Código e Entropia

Nas seções anteriores, o comprimento médio de um código foi definido em função da distribuição de probabilidade associada ao seu alfabeto de origem. Da mesma forma, as noções de **entropia** relacionada a um conjunto de mensagens, têm ligação direta com as probabilidades associadas a estas. A seguir, será mostrado como podemos relacionar o comprimento médio de um código a sua entropia através da **Desigualdade de Kraft-McMillan**, e por consequência estabelecer uma relação direta entre a **entropia de um conjunto de mensagens e a otimalidade do código associada a estas mensagens**.

Lema 1 (Desigualdade de Kraft-McMillan). ***Kraft..** Para qualquer conjunto L de comprimento códigos que satisfaça:*

$$\sum_{l \in L} 2^{-l} \leq 1.$$

Existe ao menos um código livre de prefixo tal que, $|w_i| = l_i$, $\forall w \in W^+$.

Kraft-McMillan. Para todo código binário unicamente decodificável $C : M \rightarrow W^+$.

$$\sum_{w \in W^+} 2^{-l(w)} \leq 1.$$

Demonstração.

Desigualdade de Kraft Sem perda de generalidade, suponha que os elementos de L estão ordenados de maneira em que:

$$l_1 \leq l_2 \leq \dots \leq l_n$$

Agora vamos construir um código livre de prefixo em uma ordem crescente de tamanho, de maneira em que $l(w_i) = l_i$. Sabemos que um código é livre de prefixo se e somente se, existe uma palavra-código w_j tal que nenhuma das palavras-código anteriores (w_1, w_2, w_{j-1}) são prefixo de w_j .

Sem as restrições de prefixo, uma palavra-código de tamanho l_j poderia ser construída de 2^{l_j} maneiras diferentes. Com a restrição apresentada anteriormente, considerando uma palavra w_k anterior a w_j (i.e, $k < j$), existem $2^{l_j-l_k}$ possíveis palavras-código em que w_k seria um prefixo, e que portanto não podem pertencer ao código. Chamaremos tal conjunto de "palavras-código proibidas". Vale notar que os elementos do conjunto de palavras-código proibidas são excludentes entre si, pois se duas palavras-código menores que j fossem prefixo da mesma palavra-código, elas seriam prefixos entre si.

Dito isto, podemos definir o tamanho do conjunto de palavras-código proibida para w_j .

$$\sum_{i=1}^{j-1} 2^{l_j-l_i}$$

A construção do código livre de prefixo é possível se e somente se, existir ao menos uma palavra-código de tamanho $j > 1$ que não está contida no conjunto das palavras-código proibidas.

$$2^{l_j} > \sum_{i=1}^{j-1} 2^{l_j-l_i}$$

Como o domínio do problema apresentado está restrito aos inteiros não negativos, podemos afirmar que:

$$\begin{aligned} 2^{l_j} &> \sum_{i=1}^{j-1} 2^{l_j-l_i} = 2^{l_j} \geq \sum_{i=1}^{j-1} 2^{l_j-l_i} + 1 \\ &= 2^{l_j} \geq \sum_{i=1}^j 2^{l_j-l_i} \\ &= 1 \geq \sum_{i=1}^j 2^{-l_i} \\ &= \sum_{i=1}^j 2^{-l_i} \leq 1 \end{aligned}$$

Substituindo n em j , chegamos a desigualdade de Kraft.

$$\sum_{l \in L} 2^{-l} \leq 1.$$

Note que os argumentos utilizados para a construção da prova possuem dupla-equivalência, portando concluem a prova nos dois sentidos.

Kraft-McMillan Suponha um código **unicamente decodificável** C qualquer, e faça $l_{max} = \max_w l(w)$.

Agora considere uma sequência de k palavras-código de $C : M \rightarrow W^+$ (onde k é um inteiro positivo). Observe que:

$$\begin{aligned}
 \left(\sum_{w \in W^+} 2^{-l(w)} \right)^k &= \left(\sum_{w_1} 2^{-l(w_1)} \right) \cdot \left(\sum_{w_2} 2^{-l(w_2)} \right) \cdot \dots \cdot \left(\sum_{w_k} 2^{-l(w_k)} \right) \\
 &= \sum_{w_1} \sum_{w_2} \dots \sum_{w_k} \prod_{j=1}^k 2^{-l(w_j)} \\
 &= \sum_{w_1, \dots, w_k} 2^{-\sum_{j=1}^k l(w_j)} \\
 &= \sum_{w_k} 2^{-l(w^k)} \\
 &= \sum_{j=1}^{k \cdot l_{max}} |\{w_k | l(w_k) = j\}| \cdot 2^{-j}.
 \end{aligned}$$

Sabemos que existem 2^j palavras-código de tamanho j , isto é, $|\{w_k | l(w_k) = j\}| = 2^j$. Para que o código seja unicamente decodificável obtemos o seguinte limite superior:

$$\left(\sum_{w \in W^+} 2^{-l(w)} \right)^k \leq \sum_{j=1}^{k \cdot l_{max}} 2^j \cdot 2^{-j} = k \cdot l_{max}$$

Logo,

$$\sum_{w \in W^+} 2^{-l(w)} \leq (k \cdot l_{max})^{\frac{1}{k}}$$

Note que a desigualdade é válida para qualquer $k > 0$ inteiro. Aproximando k ao infinito, obtemos a desigualdade de Kraft-McMillan.

$$\sum_{w \in W^+} 2^{-l(w)} \leq \lim_{k \rightarrow \infty} (k \cdot l_{max})^{\frac{1}{k}} = 1.$$

□

Lema 2 (Entropia como limite inferior para o comprimento médio). *Dado um conjunto de mensagens M associado a uma distribuição de probabilidades p e um código unicamente decodificável C .*

$$H(M, p) \leq l_a(C)$$

Demonstração. Queremos provar que $H(M, p) - l_a(C) \leq 0$, dado que $H(M, p) \leq l_a(C) \Leftrightarrow H(M, p) - l_a(C) \leq 0$.

Substituindo a equação 1.6 em $H(M, p)$ e 1.4 em $l_a(C)$, temos:

$$\begin{aligned}
 H(M, p) - l_a(C) &= \sum_{m \in M} p(m) \log_2 \frac{1}{p(m)} - \sum_{m \in M, w \in W^+} p(m) l(w) \\
 &= \sum_{m \in M, w \in W^+} p(m) \left(\log_2 \frac{1}{p(m)} - l(w) \right) \\
 &= \sum_{m \in M, w \in W^+} p(m) \left(\log_2 \frac{1}{p(m)} - \log_2 2^{l(w)} \right) \\
 &= \sum_{m \in M, w \in W^+} p(m) \log_2 \frac{2^{-l(w)}}{p(m)}
 \end{aligned}$$

A **Desigualdade de Jansen** afirma que se uma função $f(x)$ é côncava, então $\sum_i p_i f(x_i) \leq f(\sum_i p_i x_i)$. Como a função \log_2 é côncava, podemos aplicar a Desigualdade de Jansen ao resultado obtido anteriormente.

$$\sum_{m \in M, w \in W^+} p(m) \log_2 \frac{2^{-l(w)}}{p(m)} \leq \log_2 \left(\sum_{m \in M, w \in W^+} 2^{-l(w)} \right)$$

Agora aplicamos a desigualdade de Kraft-McMillan, e concluímos que:

$$H(M, p) - l_a(C) \leq \log_2 \left(\sum_{m \in M, w \in W^+} 2^{-l(w)} \right) \Rightarrow H(M, p) - l_a(C) \leq 0.$$

□

Lema 3 (Entropia como limite superior para o comprimento médio de um código livre de prefixo ótimo). *Dado um conjunto de mensagens M associado a uma distribuição de probabilidades p e um código livre de prefixo ótimo C .*

$$l_a(C) \leq H(M, p) + 1$$

Demonstração. Sem perda de generalidade, para cada mensagem $m \in M$ faça $l(m) = \left\lceil \log_2 \frac{1}{p(m)} \right\rceil$. Temos que:

$$\begin{aligned}
 \sum_{m \in M} 2^{-l(m)} &= \sum_{m \in M} 2^{-\left\lceil \log_2 \frac{1}{p(m)} \right\rceil} \\
 &\leq \sum_{m \in M} 2^{-\log_2 \frac{1}{p(m)}} \\
 &= \sum_{m \in M} p(m) \\
 &= 1
 \end{aligned}$$

De acordo com a desigualdade de Kraft-McMillan existe um código livre de prefixo C' com palavras-código de tamanho $l(m)$, portanto:

$$\begin{aligned}
 l_a(C') &= \sum_{m \in M', w \in W'^+} p(m) l(w) \\
 &= \sum_{m \in M', w \in W'^+} p(m) \left\lceil \log_2 \frac{1}{p(m)} \right\rceil \\
 &\leq \sum_{m \in M', w \in W'^+} p(m) (1 + \log_2 \frac{1}{p(m)}) \\
 &= 1 + \sum_{m \in M', w \in W'^+} p(m) \log_2 \frac{1}{p(m)} \\
 &= 1 + H(M)
 \end{aligned}$$

Pela definição de código livre de prefixo ótimo, $l_a(C) \leq l_a(C')$, isto é:

$$l_a(C) \leq H(M, p) + 1$$

□

Parte II

Algoritmos

2 Algoritmos de compressão sem perda

Com no que foi apresentado no capítulo anterior, a compressão de dados pode ser vista como uma sub-área da teoria da informação. O principal objeto de estudo é o desenvolvimento métodos e ferramental (ou otimização dos já existentes) que reduzam a quantidade de dados necessários para representar uma determinada informação.

Os algoritmos de compressão podem ser categorizadas em duas diferentes classes: os de compressão **com perda** e **sem perda**. Os **algoritmos de compressão sem perda** admitem uma baixa porcentagem de perda de informações durante a codificação para obter maior performance, muito uteis na transmissão de dados em streaming por exemplo. Nos **algoritmos de compressão com perda** o processo de codificação deve ser capaz de recuperar os dados em sua totalidade, geralmente utilizados em casos onde não pode haver perda de informações (como por exemplo, compressão de arquivos de texto).

2.1 Código de Huffman

O **algoritmo de Huffman** (desenvolvido por David Huffman em 1952) é um dos componentes mais utilizados em algoritmos de compressão sem perda, servindo como base para algoritmos como o Deflate (utilizado amplamente na web). Os códigos gerados a partir do algoritmos de Huffman são chamados **Códigos de Huffman**.

O código de Huffman é descrito em termos de como ele gera uma árvore de código livre de prefixo. Considere o conjunto de mensagens M , com p_i sendo a probabilidade associada a m_i

Algorithm 1 Algoritmo de Huffman

```

Forest  $\leftarrow []$ 

for all  $m_i \in M$  do                                      $\triangleright$  Inicializando floresta
     $T \leftarrow newTree()$ 
     $node \leftarrow newNode()$ 
     $node.weight \leftarrow p_i$                                 $\triangleright w_i = p_i$ 
     $T.root \leftarrow node$ 
     $Forest.append(T)$                                         $\triangleright$  Adiciona um nova arvore mna floresta
end for

while  $Forest.size > 1$  do
     $T1 \leftarrow ExtractMin(Forest)$                         $\triangleright$  Retorna a árvore cuja raiz é mínima, e retira da floresta
     $T2 \leftarrow ExtractMin(Forest)$ 
     $HTree \leftarrow newTree()$ 
     $HTree.root \leftarrow newNode()$ 

     $HTree.root.left \leftarrow T1.root$ 
     $HTree.root.right \leftarrow T2.root$ 
     $HTree.root.weight \leftarrow T1.root.weight + T2.root.weight$ 
     $Forest.append(HTree)$ 
end while
  
```

2.1.1 Análise Assintótica

Seja n o tamanho do conjunto de mensagens M . Para que o algoritmo percorra toda a floresta, formada por uma árvore para cada $m \in M$, serão necessárias n interações. Considerando que as funções $ExtractMin()$ e $.append()$ foram construídas a partir de uma fila de prioridades de **heap**, o algoritmo será executado em $O(n \log_2 n)$.

2.1.2 Corretude

O teorema a seguir (escrito por Huffman) mostra a principal propriedade do Algoritmo de Huffman, os códigos de Huffman são códigos ótimos e livres de prefixo.

Lema 4. *Seja C um código ótimo livre de prefixo, com $\{p_1, p_2, \dots, p_n\}$ sendo a distribuição de probabilidades associada ao código. Se $p_i > p_j$ então $l(w_i) \leq l(w_j)$*

Demonstração. Assuma que $l(c_i) > l(c_j)$. Agora vamos construí um novo código C' , trocando w_i por w_j . Dado l_a como o comprimento médio do código C , o código C' terá o seguinte comprimento:

$$\begin{aligned} l'_a &= l_a + p_j(l(w_i) - l(w_j)) + p_i(l(w_j) - l(w_i)) \\ &= l_a + (p_j - p_i)(l(w_i) - l(w_j)) \end{aligned}$$

Pelas suposições feitas anteriormente o termo $(p_j - p_i)(l(w_i) - l(w_j))$ seria negativo, contradizendo o fato do código C ser um código ótimo e livre de prefixo (pois neste caso $l'_a > l_a$).

Nota* : Perceba que em uma árvore de Huffman, o tamanho da palavra código w_i também representa seu nível na árvore. \square

Teorema 5. *O algoritmo de Huffman gera um código ótimo livre de prefixo.*

Demonstração. A prova se dará por indução sobre o número de mensagens pertencentes ao código. Vamos mostrar que se o Algoritmo de Huffman gera um código livre de prefixo ótimo para qualquer distribuição de probabilidades com n mensagens, então o mesmo ocorre para $n + 1$ mensagens.

Caso Base. Para $n = 2$ o teorema é trivialmente satisfeito considerando um código que atribui um bit pra cada mensagem do código.

Passo indutivo. Pelo lema 4 sabemos que as menores probabilidades estão nos menores níveis da árvore de Huffman (por ser uma árvore completa binário, o seu menor nível deve possuir ao menos dois nós). Já que esses nós possuiriam o mesmo tamanho, podemos muda-los de posição sem afetar o tamanho médio do código, concluindo assim que estes são nós **irmãos**.

Agora defina um conjunto de mensagens M de tamanho $n + 1$ onde T é a árvore de prefixo ótima construída a partir do Algoritmo de Huffman aplicado em M . Vamos chamar os dois nós de menor probabilidade na árvore de x e y (que pelo argumento anterior, são nós irmãos). Vamos construir uma nova árvore T' a partir de T removendo os nós x e y , fazendo assim que o pai destes nós, que chamaremos de z , seja o de menor probabilidade (de acordo com a definição do Algoritmo de Huffman, $p_z = p_y + p_x$). Considere k como a profundidade de z , temos:

$$\begin{aligned} l_a(T) &= l_a(T') + p_x(k + 1) + p_y(k + 1) - p_z k \\ &= l_a(T') + p_x + p_y \end{aligned}$$

Sabemos pela hipótese de indução que $l_a(T')$ é mínimo, pois T' tem o tamanho n e foi gerada pelo algoritmo de Huffman. Note que independente da ordem que forem inseridos, os nós x e y irão adicionar a constante $p_z = p_x + p_y$ no peso médio do código. Como $l_a(T')$ é mínimo para um conjunto de mensagens de tamanho n e seu nó de menor peso tem distribuição de probabilidade p_z , $l_a(T)$ também é mínimo para o conjunto de mensagens M e logo T é ótimo e livre de prefixo. \square

Referências

HIRSCHBERG, D.S; LELEWER D.A; *Data compression*, Computing Surveys 19.3, 1987.
Nenhuma citação no texto.

BLELLOCH G.E; *Introduction to Data Compression*, Carnegie Mellon, 2013 Nenhuma
citação no texto.

BERTSEKAS D.P; TSITSIKLIS J.N; *Introduction to Probability* M.I.T, Lecture Notes
Course 6.041-6.431, 2000 Nenhuma citação no texto.