Universidade Federal do ABC
Centro de Matemática, Computação e Cognição

# Compressão de Dados e Entropia no Contexto Linguístico

**Lucas Silva Amorim**

**Santo André - SP, Maio de 2022**

Lucas Silva Amorim

# Compressão de Dados e Entropia no Contexto Linguístico

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

Universidade Federal do ABC – UFABC

Centro de Matemática, Computação e Cognição

Bacharelado em Ciências da Computação.

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

Santo André - SP

Maio 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, antecedidas 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

# Introdução

Este documento segue as normas estabelecidas pela **??**, 3.1-3.2).

## Figuras

As normas da **??**, 3.1-3.2) especificam que o caption da figura deve vir abaixo da mesma.

A Figura 1 ilustra...


Figura 1 – Breve explicação sobre a figura. Deve vir abaixo da mesma.

## Tabelas

A Tabela 1 apresenta os resultados...

Tabela 1 – Breve explicação sobre a tabela. Deve vir acima da mesma.

| XX | FF | PP | YY | Yr | xY | Yx | ZZ |
|---|---|---|---|---|---|---|---|
| 615 | 18 | 2558 | 0,9930 | 0,9930 | 0,9930 | 0,9930 | 0,9930 |
| 615 | 18 | 2558 | 0,9930 | 0,9930 | 0,9930 | 0,9930 | 0,9930 |
| 615 | 18 | 2558 | 0,9930 | 0,9930 | 0,9930 | 0,9930 | 0,9930 |
| 615 | 18 | 2558 | 0,9930 | 0,9930 | 0,9930 | 0,9930 | 0,9930 |
| 615 | 18 | 2558 | 0,9930 | 0,9930 | 0,9930 | 0,9930 | 0,9930 |

## Motivação

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aenean nonummy turpis id odio. Integer euismod imperdiet turpis. Ut nec leo nec diam imperdiet lacinia. Etiam eget lacus eget mi ultricies posuere. In placerat tristique tortor. Sed porta vestibulum metus. Nulla iaculis sollicitudin pede. Fusce luctus tellus in dolor. Curabitur auctor velit a sem. Morbi sapien. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Donec adipiscing urna vehicula nunc. Sed ornare leo in leo. In rhoncus leo ut dui. Aenean dolor quam, volutpat nec, fringilla id, consectetuer vel, pede.

## Objetivos

Nulla malesuada risus ut urna. Aenean pretium velit sit amet metus. Duis iaculis. In hac habitasse platea dictumst. Nullam molestie turpis eget nisl. Duis a massa id pede dapibus ultricies. Sed eu leo. In at mauris sit amet tortor bibendum varius. Phasellus justo risus, posuere in, sagittis ac, varius vel, tortor. Quisque id enim. Phasellus consequat, libero pretium nonummy fringilla, tortor lacus vestibulum nunc, ut rhoncus ligula neque id justo. Nullam accumsan euismod nunc. Proin vitae ipsum ac metus dictum tempus. Nam ut wisi. Quisque tortor felis, interdum ac, sodales a, semper a, sem. Curabitur in velit sit amet dui tristique sodales. Vivamus mauris pede, lacinia eget, pellentesque quis, scelerisque eu, est. Aliquam risus. Quisque bibendum pede eu dolor.

# Parte I

# Fundamentação Teórica

# 1 Conceitos e definições fundamentais

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

## 1.1 Código

Um **código** $C$ mapeia uma **mensagem** $m \in M$ para uma cadeia de **palavras código** em $W^+$,onde $M$ é chamado **alfabeto de origem** e $W^+$ **alfabeto de palavras código**. Vamos utilizar a notação $A^+$ para se referir ao conjunto que contém todas as cadeias de $A$, *i.e*, $A^+ = \bigcup_{i \geq 1} A^i : A^i = (a_1, ..., a_i), a \in A$. Deste modo, podemos representar um código como uma função $\boldsymbol{C : M \rightarrow W^+}$. O **comprimento** da palavra código $w$, definido pela função $l(w)$, representa o número de bits de $w$

Os elementos dos alfabetos de origem e de palavras código podem ter um comprimento 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, a compressão de dados utiliza apenas códigos de comprimento variável, mas especificamente códigos que variam o comprimento de acordo com a probabilidade associada à mensagem (o tema será melhor detalhado em seções posteriores).

### 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 é dito **unicamente decodificável** quando $C(m) = w \leftrightarrow C^{-1}(w) = m$, com $m \in M$ e $w \in W^+$.

Vamos definir $C^+$ como a **codificação** correspondente ao código $C$, tal que $C^+(m^n) = C(m_1)C(m_2)...C(m_n) : m^n = m_1m_2...m_n$, *i.e*, $C^+ : M^+ \rightarrow W^+$. A função de **decodificação** $D^+ : W^+ \rightarrow M^+$ se refere a operação inversa da codificação, de modo que dado um código **unicamente decodificável** $C$, $D^+(C^+(m^n)) = m^n$.

Um **código livre de prefixo** é um código $C'$ em que $\nexists w_1, w_2 \in W^+ \mid w_1$ é **prefixo** de $w_2$, por exemplo, o conjunto de palavras código $W^+ := \{1, 01, 000, 001\}$ não possui nenhuma cadeia que é prefixo de outra dentro do conjunto. Códigos livres de prefixo podem ser *decodificados instantaneamente*, ou seja, podemos decodificar uma palavra código sem precisar verificar o início da seguinte.

Um código livre de prefixo pode ser modelado por uma arvore 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 correspondente a $m$, de maneira em que, para cada nó percorrido concatene um bit à $p$ (0 quando o nó está à esquerda e 1 quando está à direita). Chamamos tal árvore de **árvore do código livre de prefixo**.

## 1.2 Relações fundamentais com a Teoria da Informação

A codificação é comumente divida 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 usa uma estratégia gulosa em relação a probabilidade associada às mensagens para reduzir seu tamanho. (substituindo as mensagens que ocorrem com maior frequência por símbolos menores).

Desta forma, é evidente que os algoritmos de compressão sempre devem tomar vantagem de alguma distribuição de probabilidades "desbalanceada"sobre as mensagens para efetivamente reduzir o tamanho destas, portanto, a compressão é fortemente relacionada com a probabilidade. 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 $\Omega$, uma **variável aleatória** $X$ associa um número real a cada um dos possíveis resultados em $\Omega$. Em outras palavras, $X$ é uma função que mapeia os elementos do espaço amostral para números reais. Quando a imagem de $X$ pode assumir um número finito de valores, dizemos que $X$ é uma **variável aleatória discreta**.

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*, $p_X(x)$.

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

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

$$\sum_x p_X(x) = 1. \tag{1.2}$$

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

$$\mathbf{E}[\ X]\ = \sum_x x p_X(x). \tag{1.3}$$

### 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:

$$l_a(C) = \sum_{m \in M, w \in W^+} p(m) l(w) \tag{1.4}$$

Um código $C$ livre de prefixo é **ótimo** se $l_a(C)$ é mínimo, isto é, para qualquer código livre de prefixo $C'$ temos que

$$l_a(C) \leq l_a(C') \tag{1.5}$$

### 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 sistema $S$ e a função $p$ sendo a distribuição de probabilidade associada a $S$, definimos **Entropia** como:

$$H(S) = \sum_{s \in S} p(s) \log_2 \frac{1}{p(s)} \tag{1.6}$$

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:

$$i(s) = \log_2 \frac{1}{p(s)}. \tag{1.7}$$

### 1.2.4 Comprimento de Código e Entropia

Nas secções 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, tem 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* $\mathbf{C : M \rightarrow W^+}$ .

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

*Demonstração.*

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

$$l_1 \leq l_2 \leq ... \leq l_n$$

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 $\boldsymbol{C : M \rightarrow W^+}$ (onde $k$ é um inteiro positivo). Observe que:

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

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:

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

Logo,

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

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

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

□

**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*.*

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

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

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

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

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.

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

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

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

□

**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*.*

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

*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:

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

□

# 2 Algoritmos de compressão sem perda

## 2.1 Códigos 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 GZIP (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** ▷ Inicializando floresta
  $T \leftarrow newTree()$
  $node \leftarrow newNode()$
  $node.weight \leftarrow p_i$ ▷ $w_i = p_i$
  $T.root \leftarrow node$
  $Forest.append(T)$ ▷ Adiciona um nova arvore mna floresta
**end for**

**while** $Forest.size > 1$ **do**
  $T1 \leftarrow ExtractMin(Forest)$ ▷ 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* $\{p_1, p_2, ..., p_n\}$ *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 construi 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. □

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

*Demonstração.* A prova se dará por indução sob 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 5 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). Por estes 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:

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

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. □

# 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.