Universidade Federal do Rio Grande do Norte – UFRN
Centro de Ensino Superior do Seridó – CERES
Departamento de Ciências Exatas e Aplicadas – DCEA
Bacharelado em Sistemas de Informação – BSI

Modelo de Referência no Desenvolvimento de Monografias e Relatórios do LabEPI

Nome Completo do Aluno

Orientador: Prof. Dr. Nome Completo do Professor

Relatório Técnico apresentado ao Curso de Bacharelado em Sistemas de Informação como parte dos requisitos para aprovação na atividade de Estágio Obrigatório.

Laboratório de Elementos do Processamento da Informação – LabEPI
Caicó, RN, 23 de março de 2014

UFRN / Biblioteca Central Zila Mamede.

Catalogação da Publicação na Fonte.

Aluno, Nome Completo do.
Modelo de Referência no Desenvolvimento de Monografias e Relatórios do LabEPI. / Nome Completo do Aluno. – Caicó, RN, 2014.
28 f.: il.

Orientador: Prof. Dr. Nome Completo do Professor.

Relatório Técnico – Universidade Federal do Rio Grande do Norte. Centro de Ensino Superior do Seridó. Bacharelado em Sistemas de Informação.

1. Primeira palavra chave. 2. Segunda palavra chave. 3. Terceira palavra chave. I. Professor, Nome Completo do. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/BCZM CDU 004.7

Resumo

Este trabalho apresenta...

Palavras-chave: Primeira palavra chave; Segunda palavra chave; Terceira palavra chave.

Abstract

This document presents...

Keywords: First keyword; Second keyword; Third keyword.

Sumário

Lista de Algoritmos

Lista de Definições

Lista de Figuras

Lista de Tabelas

Lista de Teoremas

Glossário

Acrônimos

BFS ... *Breadth-First Search*
BGP ... *Border Gateway Protocol*
CAIDA ... *Cooperative Association for Internet Data Analysis*
CDF ... *Cumulative Distribution Function*
DDoS ... *Distributed Denial of Service*
DoS ... *Denial of Service*
FIFO ... *First-In First-Out*
IDS ... *Intrusion Detection System*
IoT ... *Internet of Things*
IP ... *Internet Protocol*
IPv4 ... *Internet Protocol version 4*
IPv6 ... *Internet Protocol version 6*
IPS ... *Intrusion Prevention System*
ISN ... *Initial Sequence Number*
NAPT ... *Network Address and Port Translation*
NAT ... *Network Address Translation*
NAT-PT ... *Network Address Translation – Protocol Translation*
NP ... *Nondeterministic Polynomial Time*
P2P ... *Peer to Peer*
PDF ... *Probability Distribution Function*
PRNG ... *Pseudo-Random Number Generator*
SOM ... *Self-Organizing Map*
TCP ... *Transmission Control Protocol*

Simbologia

C.Q.D. ...... Demarcador contração de ‘como se queria demonstrar’.

$\square$ .... Demarca fim de Algoritmos, Definições, Teoremas, dentre outros.

Representações

$\mathbf{x}$ .... Letras minúsculas em negrito indicam vetores coluna. É possível parametrizar o vetor, por exemplo, $\mathbf{x}(t) = \begin{bmatrix} x_1(t) & \cdots & x_n(t) \end{bmatrix}^\intercal$ indica que o vetor $\mathbf{x}$ é variante no tempo.

$\mathbf{X}$ .... Letras maiúsculas em negrito indicam matrizes. Assim como é possível parametrizar vetores, o mesmo é possível com matrizes, por exemplo, uma matriz variante no tempo pode ser representa por $\mathbf{X}(t)$.

$\mathcal{X}$ .... Letras maiúsculas caligráficas representam variáveis aleatórias.

$\dot{x}(t)$ .... Indica a derivada da função $x(\cdot)$ em relação ao tempo t. Também se aplica a funcionais em vetores e matrizes.

$n!$ .... Operador fatorial, definido recursivamente como $n! = n(n-1)!$ e com caso base $0! = 1$. De forma iterativa também pode ser descrito como

$$n! = \prod_{i=0}^{n-2} (n-i),$$

para $n \geq 2$.

$\binom{n}{k}$ .... Coeficiente binomial de n dado k, onde $0 \leq k \leq n$, definido como

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

que pode ser computado de forma eficiente utilizando

$$\binom{n}{k} = \prod_{i=1}^{k} \frac{n-(k-i)}{i},$$

que possui complexidade $\Theta(k)$.

$\delta(t), \delta_{ij}$ .... A função delta de Kronecker, definida como

$$\delta_{ij} \triangleq \begin{cases} 1 & \text{se } i = j \\ 0 & \text{caso contrário} \end{cases},$$

utilizada como contrapartida discreta da função delta de Dirac. Por conveniência, é possível usar a seguinte representação

$$\delta(t) \triangleq \begin{cases} 1 & \text{se } t = 0 \\ 0 & \text{caso contrário} \end{cases}.$$

Dessa forma temos de forma equivalente que o valor $\delta(i-j)$ é 1 se $i = j$ e 0 caso contrário.

H_n .... Indica a soma dos n primeiros termos da série harmônica, representada por

$$\mathrm{H}_n = \sum_{i=1}^{n} \frac{1}{i},$$

que diverge no limite quando $n \to \infty$. Porém, possui a seguinte propriedade assintótica

$$\lim_{n\to\infty} \mathrm{H}_n - \log(n) = \gamma,$$

onde $\gamma \approx 0.57721$ representa a constante de Euler-Mascheroni. Portanto, é possível usar a seguinte igualdade assintótica

$$\mathrm{H}_n \simeq \log(n) + \gamma,$$

onde o logaritmo natural é o da base natural e.

$\{x : p(x)\}$ .... Descrição do conjunto representado pelos elementos x que têm a propriedade, ou predicado, $p(x)$. Adicionalmente, o predicado $p(x)$ pode ser descrito utilizando os operadores da lógica proposicional.

$(\forall x)(p(x))$ ... Quantificação universal em relação aos elementos x que têm a propriedade, ou predicado, $p(x)$. A pertinência dos elementos representados por x também pode ser descrita de forma explicita, por exemplo, $(\forall x \in \mathbb{N})(p(x))$. Que expressa que todos os elementos do conjunto dos números naturais possuem o predicado p. Adicionalmente, o predicado $p(x)$ pode ser descrito utilizando os operadores da lógica proposicional.

$(\exists x)(p(x))$ ... Quantificação existencial em relação aos elementos x que têm a propriedade, ou predicado, $p(x)$. A pertinência dos elementos representados por x também pode ser descrita de forma explicita, por exemplo, $(\exists x \in \mathbb{N})(p(x))$. Que expressa que existe pelo menos um número natural que possui o predicado p. Adicionalmente, o predicado $p(x)$ pode ser descrito utilizando os operadores da lógica proposicional.

Notação assintótica

$\mathrm{O}(\cdot)$ .... Quando é expresso que $f(n) \in \mathrm{O}(g(n))$[i], dize-se que existe uma constante k, tal que a função $f(n)$, para todo valor de $n > n_0$, é sempre limitada superiormente por $kg(n)$.

$\Omega(\cdot)$ .... Quando é expresso que $f(n) \in \Omega(g(n))$, dize-se que existe uma constante k, tal que a função $f(n)$, para todo valor de $n > n_0$, é sempre limitada inferiormente por $kg(n)$.

[i] Utiliza-se o símbolo de pertinência $\in$ pois interpreta-se que o operador $\mathrm{O}(\cdot)$ representa o conjunto das funções que são limitadas superiormente pelo seu argumento, no caso a função $g(\cdot)$. O mesmo princípio pode ser aplicada aos outros operadores assintóticos apresentados em sequência.

$\Theta(\cdot)$ .... Quando é expresso que $f(n) \in \Theta(g(n))$, dize-se que existe uma constante k_1, tal que a função $f(n)$, para todo valor de $n > n_0$, é sempre limitada inferiormente por $k_1 g(n)$, e também existe uma outra constante k_2, tal que a função $f(n)$, para todo valor de $n > n_0$, é sempre limitada superiormente por $k_2 g(n)$. De forma equivalente, define-se que $f(n) \in \Theta(g(n))$ se e somente se

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = c,$$

para $g(n)$ diferente de zero ou, pelo menos, sempre maior de que zero a partir de algum ponto e para $0 < c < \infty$.

Igualdades matemáticas

$\approx$ .... Valor aproximado.

$\simeq$ .... Igualdade assintótica, isto é, se $f(n) \simeq g(n)$ então

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1,$$

para $g(\cdot)$ infinitamente diferente de zero.

$\propto$ .... Proporcionalidade, isto é, se $f(n) \propto g(n)$, então existe uma constante k tal que $f(n) = kg(n)$. De forma generalista, pode considerar também a igualdade assintótica.

$\triangleq$ .... Igualdade por definição, por exemplo,

$$\frac{d\mathbf{x}(t)}{dt} \triangleq \begin{bmatrix} \frac{dx_1(t)}{dt} & \cdots & \frac{dx_n(t)}{dt} \end{bmatrix}^{\mathsf{T}},$$

onde $\mathbf{x}(t)$ é um vetor coluna.

$\equiv$ .... Equivalência, por exemplo, $x \equiv y$ significa que x é definido como sendo logicamente igual à y.

Notação estatística

$\sim$ .... Indicador de distribuição de probabilidade, por exemplo $\mathcal{X} \sim N(\mu, \sigma)$ indica que a variável aleatória $\mathcal{X}$ segue uma distribuição de probabilidade normal com média μ e desvio padrão σ.

$\mathcal{X}_\zeta$ .... Resultado ou realização ζ da variável aleatória $\mathcal{X}$.

$\mathrm{P}(\mathcal{X}_\zeta)$ .... Probabilidade da variável aleatória $\mathcal{X}$ assumir a realização ζ.

$\mathrm{P}(\mathcal{X}_\zeta \mid p)$ ..... Probabilidade da variável aleatória $\mathcal{X}$ assumir a realização ζ dado que o predicado p é verdadeiro.

$\mathrm{E}\{\mathcal{X}\}$ .... Valor esperado da variável aleatória $\mathcal{X}$. No caso discreto é definido como

$$\mathrm{E}\{\mathcal{X}\} = \sum_{\{\zeta \in \mho\}} \mathcal{X}_\zeta \, \mathrm{P}(\mathcal{X}_\zeta),$$

onde $\mho$ é o conjunto de possíveis realizações da variável aleatória.

$\mathrm{E}\{\mathcal{X} \mid p\}$ ..... Valor esperado da variável aleatória $\mathcal{X}$ dado que o predicado p é verdadeiro. No caso discreto é definido como

$$\mathrm{E}\{\mathcal{X}\} = \sum_{\{\zeta \in \mho\}} \mathcal{X}_\zeta \, \mathrm{P}(\mathcal{X}_\zeta \mid p),$$

onde $\mho$ é o conjunto de possíveis realizações da variável aleatória.

Operadores matemáticos

$|\cdot|$ .... Se for aplicado a um escalar, indica o seu valor absoluto. Caso seja aplicado a um conjunto, indica sua cardinalidade.

$\lfloor\cdot\rfloor$ .... O maior valor inteiro menor ou igual ao escalar.

$\lceil\cdot\rceil$ .... O menor valor inteiro maior ou igual ao escalar.

$\rho(\cdot)$ .... Posto de uma matriz, por exemplo dada uma matriz identidade $\mathbf{I}_{n\times n}$, $\rho(\mathbf{I}) = n$.

$\mathbf{X}^\mathsf{T}$ .... Operação de transposição da matriz $\mathbf{X}$, isto é, troca dos elementos x_{ij} pelos elementos x_{ji}. Também pode ser aplicada a vetores, no qual transforma vetores coluna em vetores linha, e vice-versa.

$X - Y$ ...... Subtração de elementos de conjuntos. Utilizando a notação de conjuntos pode ser definido por

$$X - Y \triangleq \{z : (z \in X) \wedge (z \notin Y)\},$$

que representa o conjunto resultante da retirada dos elementos em X que também estão em Y.

$X \times Y$ ...... Produto cartesiano entre dois conjuntos X e Y. Utilizando a notação de conjuntos pode ser definido por

$$X \times Y \triangleq \{(x, y) : (x \in X) \wedge (y \in Y)\},$$

que representa todas as possíveis combinações de pares ordenados entres os elementos de X e de Y.

Operadores lógicos

$\neg$ .... Operador unário de negação.

$\vee$ .... Operador binário de disjunção, definido como ‘ou inclusivo’.

$\wedge$ .... Operador binário de conjunção, definido com valor lógico ‘e’.

$\Rightarrow$ .... Operador binário de implicação, por exemplo, $(a \Rightarrow b)$, onde a é denominado antecedente e b consequente. Único operador binário não comutativo.

$\Leftrightarrow$ .... Operador binário de bi-implicação. Onde $(a \Leftrightarrow b)$ é logicamente equivalente a representação $((a \Rightarrow b) \wedge (b \Rightarrow a))$.

1. Introdução

"If knowledge can create problems,
it is not through ignorance that we can solve them."
Isaac Asimov

Paragrafo introdutório.

Este Capítulo está organizado da seguinte forma...

1.1 Motivação

(Cormen et al., 2009)

1.2 Objetivos

1.3 Trabalhos relacionados

Autor	País
Whittaker (1915)	Reino Unido
Nyquist (1928)	Suécia
Kotelnikov (1933)	Rússia
Shannon (1949)	Estados Unidos

Tabela 1.1: Autores da teoria da amostragem e suas nacionalidades.

1.4 Contribuições

1.5 Organização do trabalho

1.6 Publicações relacionadas

Durante o desenvolvimento desta tese, foram publicados capítulos de livros, artigos em conferências e em periódicos. As publicações relacionados à esta tese são listadas a seguir.

Capítulos de livros

1. Medeiros, J.P.S.; Borges Neto, J.B.; Queiroz, G.S.D.; Pires, P.S.M. **Intelligent Remote Operating System Detection**, Case Studies in Intelligent Computing: Achievements and Trends, ISBN 978-1-4822-0703-3, CRC Press, Taylor and Francis, 2014.

Conferências

1. Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **A New Method for Recognizing Operating Systems of Automation Devices**, 14th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2009. Proceedings of ETFA 2009, ISSN 1946-0759, pages 1-4, ISBN 978-1-4244-2727-7, 2009.

Periódicos

1. Medeiros, J.P.S.; Santos, S.R.; Brito Júnior, A.M.; Pires, P.S.M. **Advances in Network Topology Security Visualisation**, International Journal of System of Systems Engineering (IJSSE), ISSN 1748-0671, Inderscience, volume 1, number 4, pages 387-400, 2009.

2. Levantamento bibliográfico

"We can only see a short distance ahead,
but we can see plenty there that needs to be done."
Alan Mathison Turing

O entendimento dos fundamentos...

Este Capítulo está organizado da seguinte forma...

2.1 Introdução

(Brassard and Bratley, 1996)

2.2 Fundamentação

Definição 2.1 (Grafo direcionado com pesos)**.** (Cormen et al., 2009) Um grafo direcionado com pesos G é composto por uma tripla ordenada $G = \langle N, E, \omega \rangle$, onde N representa o conjunto de vértices (ou nós) do grafo e E o conjunto de arestas ao qual se atribui as seguintes propriedades: (i) cada aresta é composta por um par ordenado de nós (v_1, v_2), que indica que existe uma ligação saindo do nó v_1 em direção ao nó v_2 e (ii) para cada aresta $e \in E$ existe um peso que é associado por uma função $\omega(\cdot)$, que realiza o mapeamento dos pesos de cada aresta para um número real, ou seja, $\omega \colon E \mapsto \mathbb{R}$. $\square$

Algoritmo 2.1 (Cálculo dos graus de entrada e saída de cada nó)**.** É possível calcular os graus de entrada e saída de cada nó da rede de forma iterativa com base na representação por lista de adjacência.

algoritmo graus(L)
{Lista de adjacência L de um grafo direcionado $G = \langle N, E \rangle$.}
$g_{\text{in}} \leftarrow$ novo-vetor($|N|, 0$) {Vetor de $|N|$ posições preenchidas com zero.}
$g_{\text{out}} \leftarrow$ novo-vetor($|N|, 0$)
para i de 1 até $|N|$ **faça**
    para cada $(v_j, p) \in L[i]$ **faça**
        {Nó adjacente v_j e peso p da aresta.}
        $g_{\text{out}}[i] \leftarrow g_{\text{out}}[i] + 1$
        $g_{\text{in}}[j] \leftarrow g_{\text{in}}[j] + 1$
    fim para
fim para
retorne $\langle g_{\text{in}}, g_{\text{out}} \rangle$ {Vetores com os graus de entrada e saída de cada nó da rede.}

Considera-se que os vetores g_{in} e g_{out} são indexados a partir de 1. A complexidade do algoritmo é da ordem de $\Theta(n\,\mathrm{E}\{\mathcal{G}^{\text{out}}\})$ em tempo e $\Theta(n)$ em memória. $\square$

2.3 Objetivos específicos

2.4 Metodologia

O procedimento metodológico utilizado no desenvolvimento deste trabalho possui uma abordagem dividida em 5 estágios. Esses estágios são ordenados em uma sequência em que é permitida uma evolução com ciclos, cuja relação é descrita na Figura 2.1.

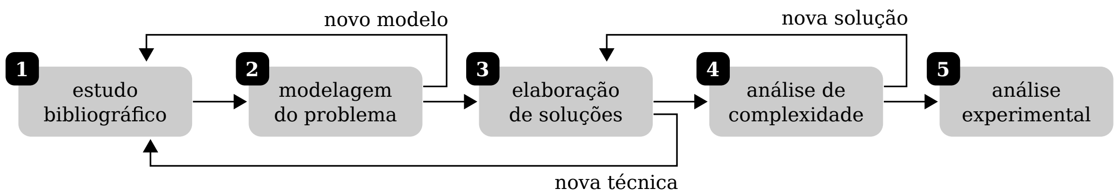

Figura 2.1: Ilustração do procedimento metodológico adotado no desenvolvimento deste trabalho. O processo foi divido em 5 estágios: (1) estudo bibliográfico para fundamentar o desenvolvimento de modelos representativos do problema; (2) modelagem do problema para servir de referência para a elaboração de soluções que, se identificadas como inadequadas, podem remeter novamente ao estudo bibliográfico; (3) elaboração de soluções algorítmicas que serão avaliadas nos próximos estágios; (4) análise de complexidade das soluções que, quando ineficientes, podem remeter a elaboração de uma nova solução e (5) análise experimental dos resultados teóricos.

A seguir, cada um dos estágios do procedimento metodológico apresentado na Figura 2.1 é descrito. Na descrição de cada estágio, são considerados, além de seu objetivo, as possibilidades de evolução de acordo com a ilustração apresentada.

1. **Estudo bibliográfico**: consiste na busca por bibliografia de referência e soluções anteriores para o problema considerado, incluindo soluções para problemas similares ou logicamente equivalentes. Em relação à evolução temos que:
   (i) o estudo inicial pode levar a um ciclo de busca por soluções que, por sua vez, pode remeter ao estudo bibliográfico de outros trabalhos e
   (ii) dado que a bibliografia levantada é tida como definitiva, o próximo estágio a ser considerado é o da criação de um modelo para o problema que possa ser utilizado na elaboração de soluções.
2. **Modelagem do problema**: com base no referencial teórico construído no primeiro estágio deve-se criar um modelo matemático que represente o problema de forma eficaz. Em relação à evolução desse estágio têm-se três opções:
   (i) passar para o estágio de elaboração de soluções quando o modelo é eficaz para o problema em questão;
   (ii) estender a modelagem ao se verificar uma deficiência na abordagem encontrada na literatura e
   (iii) possivelmente, quando a necessidade de extensão ocorre, deve-se recorrer novamente ao estudo bibliográfico, pois essas extensões devem ser cuidadosamente projetadas e validadas.
3. **Elaboração de soluções**: a partir do modelo criado no estágio anterior, é possível elaborar soluções algorítmicas e aplicar métodos de otimização a fim de solucionar

o problema redefinido com base no modelo matemático construído; Em relação à evolução desse estágio têm-se três opções:

(i) passar para o estágio de análise de complexidade da solução, seja essa complexidade associada à necessidade de recursos de tempo ou de memória;

(ii) estender a solução para subproblemas do modelo a fim de verificar propriedades que caracterizam e subsidiam a formação de hipóteses e

(iii) possivelmente, quando a necessidade de uma nova técnica ocorre, deve-se recorrer novamente ao estudo bibliográfico.

4. **Análise de complexidade**: cada solução projetada tem um custo de implementação associado. A princípio, este custo não deve inviabilizar a utilização da solução em termos de tempo e memória, dentre outros recursos, necessários para resolver o problema em questão. Em relação à evolução temos que:

   (i) se as complexidades envolvidas satisfizerem os requisitos, então evolui-se para o estágio de implementação das soluções de forma integrada e

   (ii) se a complexidade for proibitiva, é necessário voltar ao estágio de elaboração para construção de uma outra solução.

5. **Análise experimental**: se o estágio de análise de complexidade fomenta a utilização da solução proposta, deve-se realizar experimentos com dados reais para validar a solução, ou aplicá-las à instâncias do modelo a fim de extrair conjecturas acerca das propriedades do modelo que indiquem a validade da solução.

3. Desenvolvimento

"Mathematical elegance is not a dispensable luxury
but a factor that decides between success and failure."
Edsger Wybe Dijkstra

O problema...

Este Capítulo está organizado da seguinte forma...

3.1 Introdução

3.2 Modelo proposto

A relação assintótica entre a razão de duas funções pode ser usada no estudo da ordem de crescimento delas. Para isso, utiliza-se a seguinte equação Brassard and Bratley (1996); Cormen et al. (2009):

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \begin{cases} 0 & \Longrightarrow f(n) \in O(g(n)) \\ 0 < c < \infty & \Longrightarrow f(n) \in \Theta(g(n)) \\ \infty & \Longrightarrow f(n) \in \Omega(g(n)) \end{cases}, \tag{3.1}$$

onde c representa uma constante qualquer que satisfaz a inequação $0 < c < \infty$.

Lema 3.1 (Comportamento assintótico de $f(n,m) = (n^{m+1} - n)/(n-1)$)**.** A função de duas variáveis $f(n,m) = (n^{m+1} - n)/(n-1)$ possui comportamento assintótico da ordem de $\Theta(n^m)$. □

Demonstração. Para verificar se duas funções $f(n)$ e $g(n)$ possuem mesmo comportamento assintótico, isto é, $f(n) \in \Theta(g(n))$ e *vice-versa*, deve-se analisar se o limite da razão das duas, como definido pela Equação 3.1, converge para uma constante. Estendendo o uso da Equação 3.1 para funções de duas variáveis tem-se o seguinte limite

$$\lim_{(n,m)\to\infty} \frac{n^{m+1} - n}{(n-1)n^m} = \left[\lim_{(n,m)\to\infty} \frac{n^{m+1}}{(n-1)n^m}\right] - \left[\lim_{(n,m)\to\infty} \frac{n}{(n-1)n^m}\right]. \tag{3.2}$$

Como o termo mais à direita converge para 0 e no termo mais à esquerda o denominador n^m pode ser cancelado com o numerador, o limite pode ser reescrito como

$$\lim_{(n,m)\to\infty} \frac{n}{n-1} = 1. \tag{3.3}$$

Portanto, $f(n,m) \in \Theta(n^m)$. **C.Q.D.**

3.3 Experimentos

3.4 Considerações

Os resultados apresentados neste Capítulo...

4. Conclusões

"If we can really understand the problem,
the answer will come out of it,
because the answer is not separate from the problem."
Jiddu Krishnamurti

Neste trabalho...

4.1 Resultados

4.2 Trabalhos futuros

A. Apêndice

Neste Apêndice, são apresentadas...

Referências Bibliográficas

Brassard, G. and P. Bratley (1996), *Fundamentals of Algorithmics*, Prentice Hall.
(Citado nas páginas 19 e 22)

Cormen, Thomas H., Charles E. Leiserson, Ronald L. Rivest and Clifford Stein (2009), *Introduction to Algorithms*, 3ª edição, The MIT Press.
(Citado nas páginas 17, 19, e 22)

Kotelnikov, Vladimir A. (1933), On the transmission capacity of the 'ether' and of cables in electrical communications, *em* 'Proceedings of the first All-Union Conference on the technological reconstruction of the communications sector and the development of low-current engineering', Moscow, Russian.
(Citado na página 17)

Nyquist, Harry Theodor (1928), 'Certain topics in telegraph transmission theory', *Trans. American Institute of Electrical Engineers* **47**(2), 617–644.
(Citado na página 17)

Shannon, Claude Elwood (1949), 'Communication in the presence of noise', *Proc. Institute of Radio Engineers* **37**(1), 10–21.
(Citado na página 17)

Whittaker, Edmund Taylor (1915), 'On the functions which are represented by the expansions of the interpolation theory', *Proc. Royal Soc. Edinburgh* **35**(A), 481–493.
(Citado na página 17)

Índice Remissivo