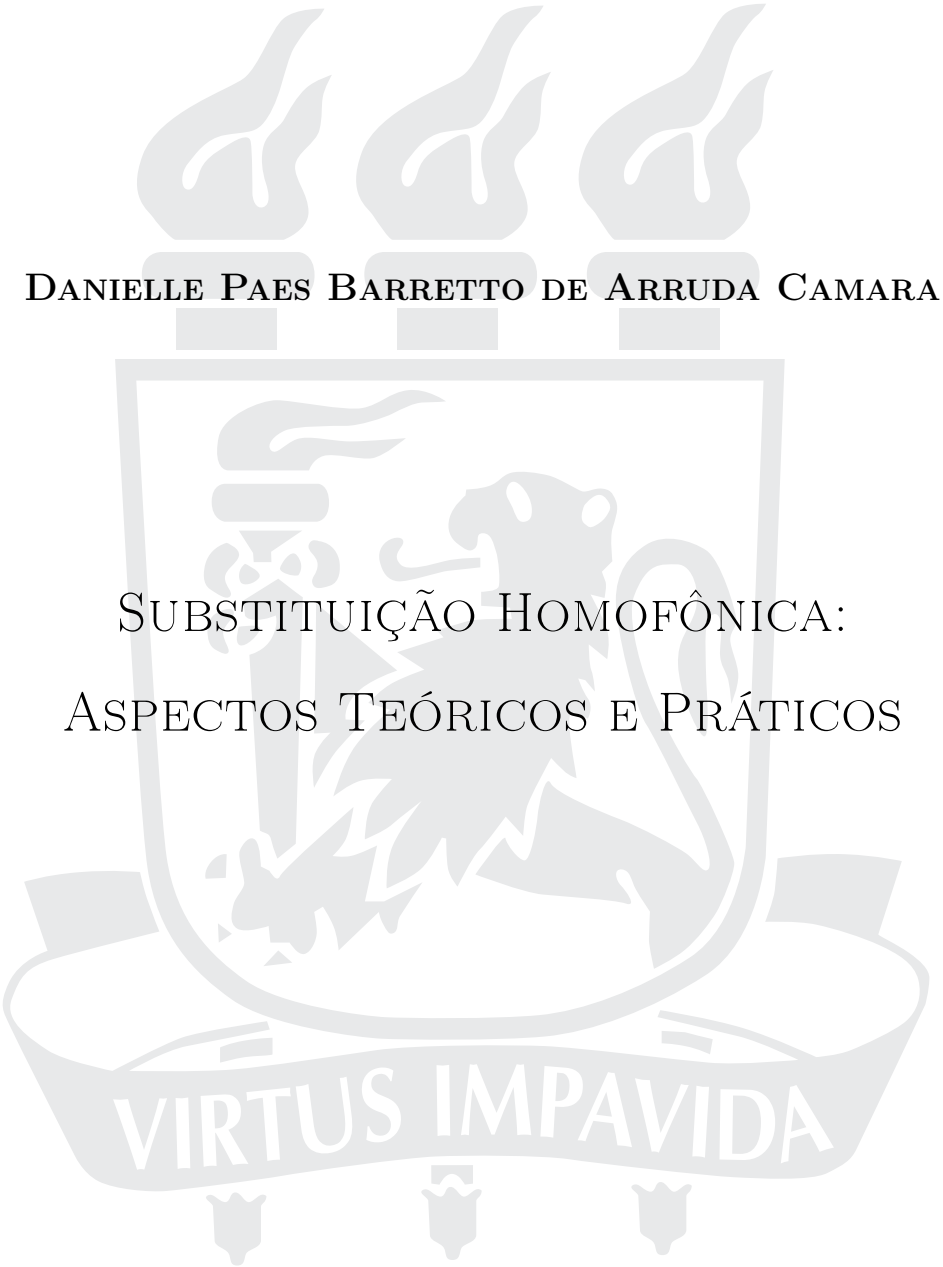
Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Programa de Pós-graduação em Engenharia Elétrica



Danielle Paes Barretto de Arruda Camara

Substituição Homofônica: Aspectos Teóricos e Práticos

Recife, Dezembro de 2006.

Danielle Paes Barretto de Arruda Camara

Substituição Homofônica: Aspectos Teóricos e Práticos

Tese submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Doutor em Engenharia Elétrica**

Orientador: Prof. Valdemar Cardoso da Rocha Jr., Ph.D.

Recife, Dezembro de 2006.

C172s **Camara, Danielle Paes Barretto de Arruda**

Substituição homofônica: aspectos teóricos e práticos / Danielle Paes Barretto de Arruda Camara. – Recife: O Autor, 2006.

221 f.; il., gráfs., tabs.

Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2006.

Inclui referências e apêndices.

1. Engenharia Elétrica. 2. Substituição Homofônica. 3. Teoria da Informação. 3. Criptografia. 4. Geração de Números Aleatórios I. Título.

621.3 CDD (22.ed.) **UFPE/BCTG/2007-66**

Universidade Federal de Pernambuco

Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE TESE DE DOUTORADO

DANIELLE PAES BARRETTO DE ARRUDA CAMARA

TÍTULO

"SUBSTITUIÇÃO HOMOFÔNICA: ASPECTOS TEÓRICOS E PRÁTICOS"

A comissão examinadora composta pelos professores: VALDEMAR CARDOSO DA ROCHA JÚNIOR, DES/UFPE, CECÍLIO JOSÉ LINS PIMENTEL, DES/UFPE, RAFAEL DUEIRE LINS, DES/UFPE, FRANCISO MARCOS DE ASSIS, DEE/UFCG e MARCELO SAMPAIO DE ALENCAR, DEE/UFCG, sob a presidência do primeiro, consideram a candidata **DANIELLE PAES BARRETTO DE ARRUDA CAMARA APROVADA**.

Recife, 27 de dezembro de 2006.

JOAQUIM FERREIRA MARTINS FILHO

VALDEMAR CARDOSO DA ROCHA JÚNIOR
Orientador e Membro Titular Interno

FRANCISCO MARCOS DE ASSIS
Membro Titular Externo

CECÍLIO JOSÉ LINS PIMENTEL
Membro Titular Interno

MARCELO SAMPAIO DE ALENCAR
Membro Titular Externo

RAFAEL DUEIRE LINS
Membro Titular Interno

À minha mãe,
Eunice Paes Barretto de Arruda Camara

Agradecimentos

Agradeço a Deus por mais esta etapa concluída, dando forças através de meus amigos e familiares a fim de superar as dificuldades. Em especial, agradeço por ter me feito evoluir como pessoa, tentando sempre compreender o verdadeiro significado das coisas, procurando dar a devida importância às mesmas e acima de tudo procurando sempre melhorar.

A minha mãe, Eunice Paes Barretto de Arruda Camara, pela mulher forte e eterno exemplo de vida, em quem procuro sempre me espelhar. Minha eterna gratidão por todo carinho, companheirismo, amizade e amor incondicionais. Meus pedidos de perdão pelas ausências (mesmo estando no quarto ao lado), meus estresses e qualquer outra falha que tenha cometido (sei que são muitas).

Ao meu orientador, Prof. Valdemar Cardoso da Rocha Jr., por sua orientação, sua disponibilidade, exemplo de perseverança, dedicação e profissionalismo. Guardarei seu exemplo por toda a vida, obrigada.

Ao Prof. Cecilio Pimentel pela disponibilidade e pelas conversas sempre frutíferas.

Aos professores do DES, em especial aos professores do grupo de Comunicações com os quais tive o prazer de compartilhar muitos desses anos desde a graduação. Meus sinceros agradecimentos pelo exemplo de dedicação, por enfrentar todas as dificuldades em prol do desenvolvimento tecnológico e científico, muitas vezes não obtendo o merecido reconhecimento.

A todos os colegas com os quais tive o privilégio de compartilhar esses anos do doutorado, dentre os quais alguns se tornaram mais que colegas e que sei que farão parte da minha vida eternamente. Obrigada pela amizade, carinho, pelo ombro amigo quando precisei e pelas conversas de fundo científico ou não.

A todos que fazem o DES e que de alguma forma tiveram participação direta ou indireta neste momento da minha vida.

Meus agradecimentos especiais ao coordenador Prof. Joaquim Ferreira Martins Filho e a secretária Andréa Tenório pela atenção e auxílio nos momentos que precisei.

A todos os meus amigos e familiares pelo estímulo, por acreditarem em mim e através de suas palavras e gestos de carinho ter feito com que eu não perecesse diante dos desafios a mim impostos durante esta caminhada. Desculpem-me pela falta de tempo e ausências, saibam que apesar do contato, muitas vezes pouco freqüente, guardo todos no meu coração.

Ao CNPq pelo apoio financeiro sem o qual provavelmente não seria possível a conclusão deste doutorado, assim como a participação em alguns eventos científicos durante este período.

Danielle Paes Barretto de Arruda Camara

Universidade Federal de Pernambuco

27 de Dezembro de 2006

Resumo da Tese apresentada à UFPE como parte dos requisitos necessários para a obtenção do grau de Doutor em Engenharia Elétrica

Substituição Homofônica: Aspectos Teóricos e Práticos

Danielle Paes Barretto de Arruda Camara

Dezembro/2006

Orientador: Prof. Valdemar Cardoso da Rocha Jr., Ph.D.
Área de Concentração: Comunicações
Palavras-chave: substituição homofônica, teoria da informação, criptografia, geração de números aleatórios.
Número de páginas: 221

O presente trabalho de investigação teve como objetivos: a) rever o tratamento de Teoria da Informação dado ao tipo de substituição homofônica de Günther, b) propor seu aprimoramento, c) investigar a implementação prática da substituição homofônica, considerando que as probabilidades dos símbolos do texto-claro são números racionais. O conceito de Shannon de cripto-sistema fortemente ideal é enfocado neste estudo pelo fato de prover a motivação para o uso de qualquer tipo de substituição homofônica. A definição de substituição homofônica de comprimento variável é revista juntamente com a condição necessária e suficiente para tal substituição ser perfeita, isto é, para criar uma seqüência completamente aleatória. Algumas técnicas de substituição homofônica padrão assim como de subs-tituição homofônica com restrição foram analisadas, sendo introduzidas duas novas técnicas de substituição homofônica padrão que pertencem a uma classe denominada de Substituição Homofônica Símbolo-a-Símbolo. Uma técnica de substituição homofônica com restrição foi proposta, assim como uma solução alternativa para o problema clássico de geração de uma distribuição de probabilidade discreta uniforme usando duas ou mais moedas desbalanceadas por meio do uso de técnicas de substituição homofônica com restrição. Observa-se, então que as técnicas aqui introduzidas contribuem não só para a obtenção de cripto-sistemas simétricos mais resistentes à criptoanálise, como para a geração de números aleatórios, podendo ser utilizadas também em testes e simulações de sistemas de comunicações, assim como em outras aplicações computacionais.

Abstract of Thesis presented to UFPE as a partial fulfillment of the requirements for the degree of Doctor in Electrical Engineering

Homophonic Substitution: Theoretical and Practical Aspects

Danielle Paes Barretto de Arruda Camara

December/2006

Supervisor: Prof. Valdemar Cardoso da Rocha Jr., Ph.D.
Area of Concentration: Communications
Keywords: homophonic substitution, information theory, cryptography, random numbers generation.
Number of pages: 221

This thesis has as main purposes: a) to review the information-theoretic treatment given to the Günther's type of homophonic substitution, b) to propose improvements of this approach, c) to investigate the practical implementation of homophonic substitution systems, considering that the plaintext symbol probabilities are rational numbers. The concept of strongly ideal cryptosystems introduced by Shannon is focused since it provides the motivation for any type of homophonic substitution. The definition of variable-length homophonic substitution is revisited together with the necessary and sufficient condition for such substitution to be perfect, i.e., to create a completely random sequence. Some standard homophonic substitution schemes as well as some constrained homophonic substitution schemes are analyzed. Two new standard homophonic substitution schemes are introduced. A constrained homophonic substitution scheme is proposed as well as an alternative solution to the classical problem of generating a discrete uniform probability distribution using two or more biased coins using this type of scheme. The techniques presented in this thesis contribute not only to obtain cryptosystems more resistant to cryptanalysis but also to random number generation which is used to perform tests and simulation of communication systems as well as other computational applications.

Lista de Figuras

Lista de Tabelas

Sumário

capítulo 1

Introdução

1.1 Motivação

Devido ao grande desenvolvimento na área de telecomunicações nas últimas décadas, a comunicação que antes acontecia em sua grande parte a curtas distâncias, pode ser feita para quaisquer distâncias por meio digital. Tal meio traz muitas vantagens, como, por exemplo, armazenamento mais compacto, a possibilidade do uso de códigos corretores de erros a fim de proporcionar detecção e/ou correção de erro, tornando a comunicação mais confiável. Todo esse desenvolvimento contribuiu sem precedentes para a era globalizada que se vive hoje. Porém, como tudo, há desvantagens, principalmente, ligadas à segurança das informações que circulam pelo meio digital, um exemplo bem conhecido e de certa forma freqüente é a invasão de *hackers* a empresas com motivos que vão de simples vandalismo à espionagem industrial, sem contar com a nova modalidade de roubo a bancos, o roubo virtual, sem que seja necessário qualquer tipo de violência física, uso de armas, seqüestro, etc, bastando apenas certa inteligência e um computador ligado à Internet. Na *RSA Conference 2007*, evento ocorrido em São Francisco - EUA, o Brasil foi apontado como líder em golpe via e-mail, "o volume e a variedade de mensagens com cavalos-de-tróia produzidos no país com objetivo de roubar informações bancárias têm crescido muito e já superam o de qualquer outro país, de acordo com Mark Harris, diretor mundial do SophosLabs" [1]. Segundo o relatório *2006 CSI/FBI Computer Crime and Security Survey* [2] o prejuízo ultrapassou US$52 milhões em 2006 (Figura 1.1).

Desta forma é importante que as informações que circulam por meio digital possam ser

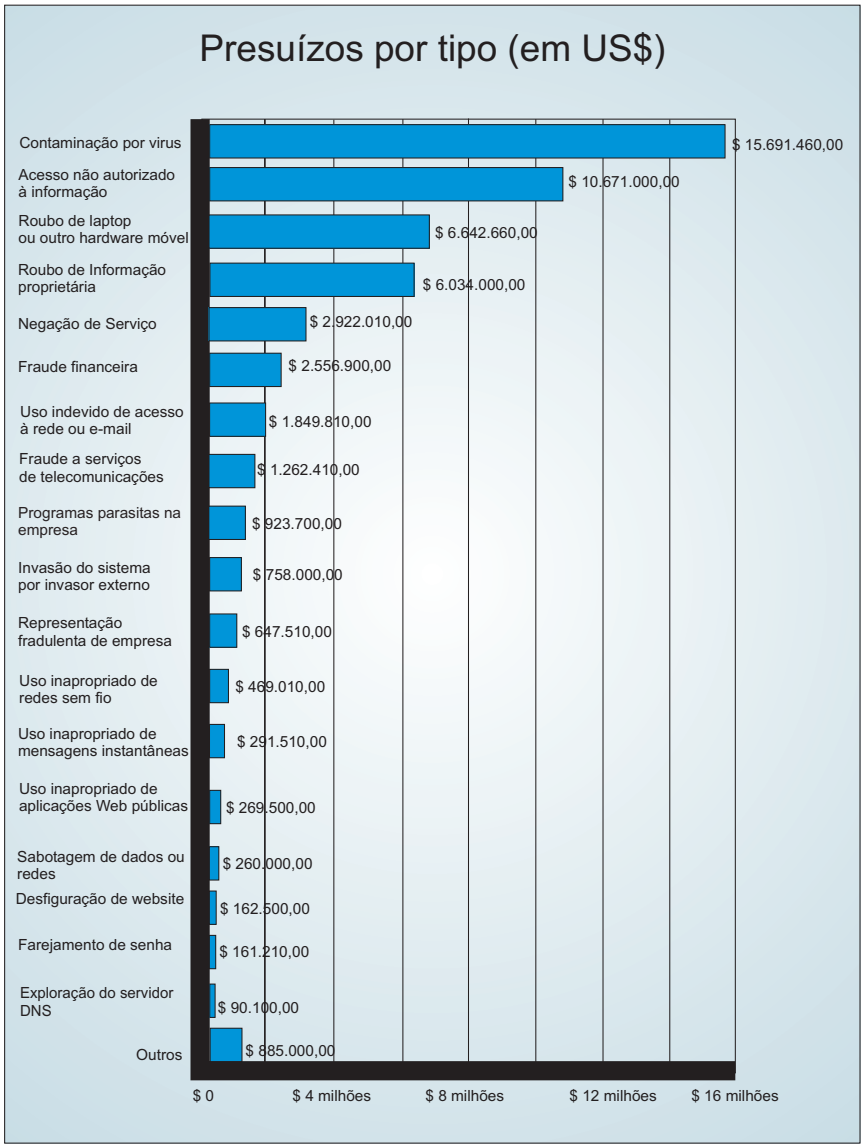


Figura 1.1: Prejuízo estimado em US$ no ano de 2006 por diferentes tipos de incidentes de segurança.

armazenadas, assim como transmitidas de forma segura, sendo protegidas de serem reveladas, alteradas, substituídas ou destruídas por pessoas não autorizadas.

Uma das ferramentas utilizadas para tais fins é a criptografia. Diferentemente de outras ferramentas usadas para a segurança de dados, os cripto-sistemas são aqueles que se mostram mais completos até o momento, proporcionando alto nível de segurança com mais flexibilidade [3].

Inicialmente, a criptografia era usada apenas para fins militares e diplomáticos. Porém, devido ao grande desenvolvimento nos meios de comunicação, o que era um privilégio de militares e diplomatas passou a se disseminar para outras áreas. Durante a Segunda Guerra

Mundial houve um grande desenvolvimento na área, novas técnicas foram criadas e máquinas foram usadas no processo de cifragem e decifragem [4]. “Avanços significativos em criptoanálise, por exemplo ao quebra a cifra alemã ENIGMA durante a Segunda Guerra Mundial, levou a necessidade de se desenvolver cripto-sistemas mais avançados"[5].

Atualmente um cidadão comum tem a possibilidade de utilizar tais técnicas para se comunicar e armazenar seus dados de forma segura.

Historicamente vários sistemas criptográficos de chave secreta foram quebrados explorando o desvio da estatística do texto-claro daquela de uma seqüência aleatória. Cripto-sistemas de chave secreta para os quais a mensagem a ser cifrada contém pouca ou nenhuma redundância são mais difíceis de serem quebrados [6]. A substituição homofônica é uma técnica criptográfica usada para reduzir a redundância de uma mensagem a ser cifrada tendo como custo alguma expansão do texto-claro.

Além disso, essa técnica tem utilidade também na área de geração de números aleatórios, o que não só é de interesse atual na área de criptografia como também em testes e simulações de sistemas de comunicação.

1.2 Contribuição

Desta forma, com o exposto na seção 1.1, os objetivos deste trabalho são contribuir para tornar os cripto-sistemas de chave secreta, também chamados cripto-sistemas simétricos, mais resistentes à criptoanálise com o uso de técnicas de substituição homofônica, assim como proporcionar uma solução alternativa para o problema clássico de geração de uma distribuição discreta uniforme usando duas ou mais moedas desbalanceadas, proporcionando assim um método alternativo para a geração de números aleatórios.

1.3 Estrutura da tese

O Capítulo 2 é dedicado à substituição homofônica padrão. Inicialmente é feita uma breve introdução sobre substituição homofônica seguida da descrição do tratamento de Teoria da Informação dado à substituição homofônica por H. N. Jendal, Y. J. B. Kuhn and J. L. Massey [6] (seção 2.2). Na seção seguinte (seção 2.3) são introduzidos os conceitos de eficiência e redundância como medidas para comparação de técnicas de substituição homofônica, mostrando o porquê de serem preferidos como um tipo de índice de comparação em vez do uso da expan-

são do texto-claro que era usado anteriormente. Na seção 2.4 é feito um estudo de algumas técnicas de substituição homofônica padrão já conhecidas (JKM [6], Rocha-Massey (RM) [7], JKM modificada [8]) e na seção seguinte (seção 2.5) uma classe denominada de Substituição Homofônica Símbolo-a-Símbolo é apresentada. A primeira tentativa de uma técnica nesta classe (Substituição Homofônica Símbolo-a-Símbolo 1) não apresentou o resultado esperado, uma vez que em uma análise posterior foi observado que nesta técnica há uma dependência estatística entre os símbolos devido aos valores de probabilidade escolhidos para o símbolo mudo, e, portanto esta técnica é uma técnica de substituição homofônica não-perfeita. Como o interesse aqui é investigar alternativas de técnicas de substituição homofônica perfeitas que mostrem melhor desempenho que as técnicas de substituição homofônica perfeitas conhecidas como, por exemplo, as técnicas RM [7] e JKM [6], uma investigação visando obter uma alternativa que fosse perfeita resultou na técnica de substituição homofônica símbolo-a-símbolo (Substituição Homofônica Símbolo-a-Símbolo 2) que é introduzida na seção 2.5.1.

Já no Capítulo 3 são abordadas basicamente as técnicas de substituição homofônica com restrição nas quais, diferentemente das técnicas de substituição homofônica padrão os símbolos que constituem as palavras-código dos homofonemas obedecem a uma distribuição de probabilidade arbitrária, i.e., não necessariamente uniforme, como é o caso das técnicas de codificação homofônica padrão. Na seção 3.2 algumas técnicas de substituição homofônica com restrição são abordadas para que na seção seguinte (seção 3.3) seja introduzida e analisada uma nova técnica denominada Técnica de Codificação Homofônica com Restrição Símbolo-a-Símbolo. O Capítulo 3 é finalizado com uma proposta para a solução do problema clássico de geração de uma distribuição discreta uniforme usando duas ou mais moedas desbalanceadas. Para finalizar, o Capítulo 4 traz conclusões e propostas para trabalhos futuros.

Além dos capítulos citados existem oito apêndices. Os dois primeiros se referem a conceitos básicos relacionados às áreas de Teoria da Informação (Apêndice A) e Criptografia (Apêndice B). O intuito aqui é proporcionar a base necessária para a compreensão do restante do texto. Os dois apêndices seguintes trazem a descrição detalhada de dois algoritmos de técnicas de substituição homofônica com restrição: MAX-ENT por passo (Apêndice C) e MIN-ENT por passo (Apêndice D). Os outros apêndices são constituídos de cópias de trabalhos aceitos e publicados em simpósios durante o período do doutorado (Apêndices E - H).

capítulo 2

Substituição homofônica

2.1 Introdução

Historicamente vários sistemas criptográficos de chave secreta foram quebrados explorando desvios da estatística do texto claro. A **substituição (ou codificação) homofônica** é uma técnica antiga utilizada para converter uma seqüência de texto claro em uma seqüência (mais) aleatória. Esta técnica consiste na substituição (*one-to-many*) de cada letra da mensagem original por um substituto ou **homofonema** pertencente a um alfabeto maior, com o intuito de formar o texto claro que é então cifrado. Cada homofonema é então codificado de forma a produzir símbolos uniformemente distribuídos e estatisticamente independentes. Tal técnica, como será visto nas seções seguintes, torna um cripto-sistema simétrico não-expansível (vide Apêndice B) mais seguro, uma vez que aumenta a distância de unicidade da cifra (Definição 34), porém isso tem um custo: a expansão do texto claro. Em 1988, Günther [9] fez uma importante contribuição na área introduzindo o que foi denominado **substituição homofônica de comprimento variável**. Tanto a idéia de substituição homofônica clássica como a de comprimento variável são abordadas na seção 2.2 deste capítulo.

As técnicas de substituição homofônica são subdivididas em técnicas de substituição homofônica padrão e técnicas de substituição homofônica com restrição. Nas técnicas de **substituição homofônica padrão**, os símbolos que compõem as palavras-código dos homofonemas são independentes, identicamente distribuídos e equiprováveis, i.e., são variáveis aleatórias obedecendo a uma distribuição uniforme. Já nas técnicas de **substituição homofônica com restrição** os símbolos que constituem as palavras-código dos homofonemas obedecem a uma

distribuição de probabilidade arbitrária, i.e., não necessariamente uniforme, sendo, portanto uma generalização da substituição homofônica padrão, encontrando aplicação em casos em que o custo de armazenar ou transmitir os símbolos não é o mesmo para todos os símbolos. Estas técnicas são vistas com maiores detalhes no Capítulo 3.

Na seção 2.2 é revisto o tratamento de Teoria da Informação dado por Jendal, Kuhn e Massey em [6] ao tipo de substituição homofônica proposto por Günther [9], enfocando o conceito de Shannon de cripto-sistema fortemente ideal (Definição 30), uma vez que ele proporciona a motivação para o uso de qualquer tipo de substituição homofônica.

Nas seções seguintes são apresentadas de forma sucinta algumas das técnicas de substituição homofônica padrão como: **JKM** [6], **Rocha-Massey (RM)** [7], **JKM modificada** [8], além de ser feita a introdução de algumas definições que se mostram úteis na comparação de técnicas de substituição homofônica [10].

Na seção 2.5 é apresentada uma nova classe de técnicas de substituição homofônica denominada **Substituição Homofônica Símbolo-a-Símbolo(SAS)**. A primeira técnica introduzida pertencente a esta classe que foi denominada **Substituição Homofônica Símbolo-a-Símbolo 1 (SH-SAS1)**. Foi verificado após uma análise posterior que nesta técnica há uma dependência estatística entre os símbolos devido aos valores de probabilidade escolhidos para o símbolo mudo, e, portanto esta técnica é uma técnica de substituição homofônica não-perfeita (vide Definição 1). Ao se investigar uma alternativa nesta classe que fosse perfeita chegou-se à técnica que foi denominada **Substituição Homofônica Símbolo-a-Símbolo 2 (SH-SAS2)**, que é abordada na seção 2.5.1.

2.2 Um tratamento de Teoria da Informação para substituição homofônica

A fim de ilustrar o propósito da substituição homofônica considere um cripto-sistema de chave secreta como ilustrado na Figura 2.1. Na figura em questão X^n e Y^n denotam, respectivamente, as seqüências de texto claro $[X_1, X_2, \ldots, X_n]$ e texto cifrado $[Y_1, Y_2, \ldots, Y_n]$, e Z denota a chave secreta, a qual, como ocorre geralmente e como sugere a figura em questão, é estatisticamente independente da seqüência de texto claro, X^n, $\forall n$.

Uma seqüência D-ária é dita completamente aleatória se cada um dos seus dígitos é estatisticamente independente dos dígitos precedentes e a escolha dos D possíveis valores é equiprovável.

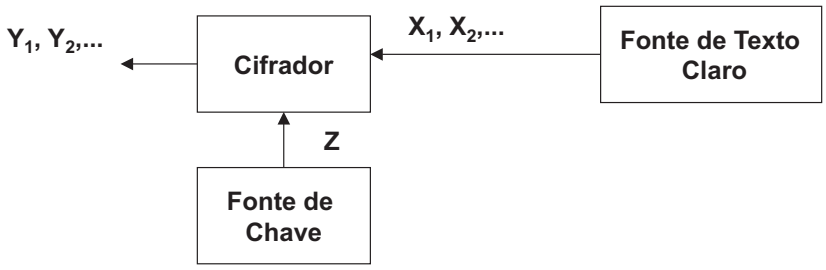


Figura 2.1: Cripto-sistema de chave secreta.

Proposição 1 *Se uma seqüência de texto claro cifrada por uma cifra de chave secreta não-expansível é completamente aleatória, então a seqüência de texto cifrado também é completamente aleatória e estatisticamente independente da chave secreta.*

Demonstração: De (A.21),

$$\begin{aligned} H(X^n, Y^n, Z) &= H(X^n) + H(Z|X^n) + H(Y^n|X^n, Z) \\ &= H(Y^n) + H(Z|Y^n) + H(X^n|Y^n, Z). \end{aligned}$$

$$\begin{aligned} H(Y^n) &= H(X^n) + H(Z|X^n) - H(Z|Y^n) \\ &= H(X^n) + H(Z) - H(Z|Y^n)^*. \end{aligned}$$

Como X^n é completamente aleatória então, $H(X^n) = n \log D$ o que implica que $H(Y^n) \geq n \log D$.

Por outro lado,

$H(Y^n) \leq n \log D$.

Então, $H(Y^n) = n \log D = H(X^n)$ e $H(Z|Y^n) = H(Z)$, i.e., Y^n é completamente aleatória e independente de Z. ■

A partir da Proposição 1 e da definição da função equivocação de chave (Definição 30), chega-se ao seguinte corolário.

Corolário 1 *Se uma seqüência de texto claro cifrada por uma cifra de chave secreta não-expansível é completamente aleatória, então o cripto-sistema é dito fortemente ideal.*

□

Cifras de chave secreta como ilustradas na Figura 2.1 são não-degenerativas†, i.e., $H(X^n|Y^n) \approx H(Z)$ para todo n suficientemente grande e todas as distribuições de probabilidade de X^n,

†Cifras de chave secreta como ilustradas na Figura 2.1 são não-degenerativas, o que significa que mudando o valor de Z, sem mudar o valor da seqüência de texto claro, X^n, o valor da seqüência de texto cifrado Y^n mudará para todo n suficientemente grande.

quando todos os possíveis valores da chave secreta Z são equiprováveis. Além disso, para todo n quando a seqüência de texto claro $X_1, X_2, ...$ é completamente aleatória $H(X^n|Y^n) = H(Y^n|X^n)$. Assim, a seguinte conclusão é imediata.

Corolário 2 *Se uma seqüência de texto claro cifrada por uma cifra de chave-secreta não-expansível é completamente aleatória e todos os possíveis valores de chave secreta Z são equiprováveis, então a entropia condicional do texto claro dado o texto cifrado satisfaz*

$$H(X^n|Y^n) \approx H(Z), \tag{2.1}$$

para n suficientemente grande.

□

Desta forma, dado que a fonte de texto claro emite uma seqüência completamente aleatória, qualquer cifra de chave secreta que segue o modelo ilustrado na Figura 2.1 pode, com o uso da técnica de substituição homofônica, ser transformada no que Shannon denominou uma cifra fortemente ideal. Sendo esse, exatamente, o objetivo da substituição homofônica: transformar uma fonte que não emite uma seqüência completamente aleatória numa que o faça.

2.2.1 Substituição homofônica de comprimento variável

Conclui-se a partir do Corolário 1 da Proposição 1 que quando a seqüência de texto claro consiste de dígitos estatisticamente independentes e uniformemente distribuídos, é uma tarefa trivial obter-se um cripto-sistema de chave secreta fortemente ideal e portanto inquebrável.

Considere a Figura 2.2, na qual o texto claro é resultado da codificação da seqüência de símbolos, denotados por $U_1, U_2, \ldots$, que saem da fonte de mensagem, numa seqüência de símbolos D-ários, $X_1, X_2, \ldots$. Admite-se que as variáveis aleatórias U_i recebem valores num alfabeto de L letras, em que $2 \leq L < \infty$.

Além disso, assume-se, por simplicidade, que a fonte é sem memória e estacionária, i.e., $U_1, U_2, \ldots$, é uma seqüência L-ária independente e identicamente distribuída, reduzindo assim o problema de codificação da fonte de mensagem ao problema de codificação de uma única variável aleatória $U = U_1$. Lembrando, que a teoria descrita é passível de modificação para que sejam consideradas fontes discretas com memória, bastando para isso substituir a distribuição de probabilidade de U_i pela distribuição de probabilidade condicional de U_i dados os valores

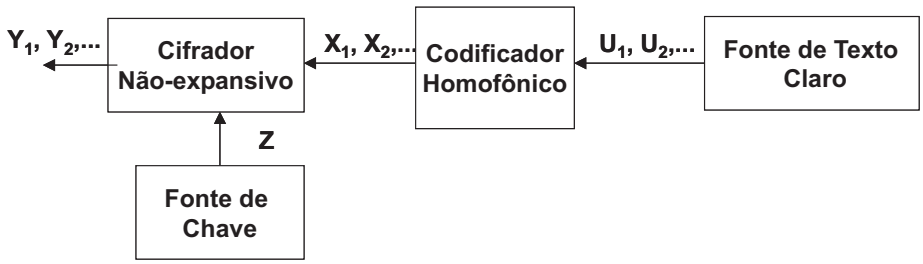


Figura 2.2: Uso da substituição homofônica num cripto-sistema de chave secreta.

observados $U_1, U_2, \ldots, U_{i-1}$. A fim de evitar complicações desnecessárias, supõe-se também que todos os L valores de D têm probabilidade não nula.

Note que, quando $L = D^W$ para W inteiro positivo e quando todos os valores de U são equiprováveis, uma técnica simples de codificação relaciona cada uma das D^W seqüências D-árias de comprimento W a cada valor de U o que faz que a palavra-código $X_1X_2X_3...X_W$ seja completamente aleatória.

Quando os valores de U não são equiprováveis, a substituição homofônica clássica tenta obter o mesmo resultado escolhendo (se possível) um W apropriado com $D^W > L$, particionando as D^W seqüências D-árias de comprimento W em L subconjuntos, relacionando a cada um desses subconjuntos um valor de U de modo que o número de seqüências em cada subconjunto seja (aproximadamente) proporcional à probabilidade do correspondente valor de U. A partir daí a palavra-código para um valor particular u de U é obtida por uma escolha equiprovável do subconjunto de seqüências correspondentes a u. Quando tal partição das seqüências D-árias de comprimento W é possível, a palavra-código $X_1X_2...X_W$ pode assumir, de forma equiprovável, quaisquer das seqüências D-árias de comprimento W de modo que a seqüência $X_1X_2 \ldots X_W$ é completamente aleatória. Como conseqüência, nota-se que nesse caso a distribuição de probabilidade dos homofonemas segue uma distribuição uniforme e suas palavras-código têm o mesmo comprimento. Embora esse procedimento alcance o objetivo da substituição homofônica, que é produzir símbolos das palavras-código dos homofonemas estatisticamente independentes, ele se mostra ao mesmo tempo ineficiente ao se tratar de números de *bits* extras necessários em média para representar cada homofonema.

Em 1988, Günther [9] introduziu a substituição homofônica de comprimento variável. Em tal técnica as seqüências D-árias podem ter comprimentos diferentes (W pode, portanto, ser uma variável aleatória), e as probabilidades de seleção de homofonemas associados a um dado valor u de U podem ser diferentes. Günther mostrou que essa técnica pode ser usada para

esconder na seqüência codificada homofonicamente toda a redundância no texto claro original e assim ser usada para construir o que Shannon denominou uma cifra fortemente ideal [11] reduzindo ao mesmo tempo a expansão do texto claro, e portanto, se mostrando mais eficiente que a técnica clássica.

Considere a Figura 2.3, na qual o canal homofônico é um canal sem memória cujo alfabeto de entrada $\{u_1, u_2, ..., u_L\}$ coincide com o conjunto de possíveis valores de U, o alfabeto de saída V pode ser finito ou infinito contável, e as probabilidades de transição $P_{V|U}(v_{ij}|u_i)$ têm a propriedade que para cada j existe exatamente um i tal que $P_{V|U}(v_{ij}|u_i) \neq 0$, observa-se desta forma que H(U|V)=0. Em geral, os v_{ij} para os quais $P_{V|U}(v_{ij}|u_i) > 0$ serão considerados homofonemas de u_i.

O codificador D-ário livre de prefixo da Figura 2.3 é um mecanismo que associa uma seqüência D-ária a cada v_{ij}, de modo que a palavra-código associada seja distinta das outras palavras-código e também não seja prefixo de outra palavra-código mais longa, o que garante que em uma seqüência de palavras-código o fim de cada palavra-código possa ser identificado imediatamente sem que seja necessária a verificação de quaisquer outros símbolos na seqüência.

Figura 2.3: Um esquema geral para substituição homofônica.

Como visto anteriormente, pela descrição de um canal homofônico, ele é um canal sem ruído (H(U|V)=0) (Definição 28). Quando, além disso, o canal homofônico da Figura 2.3 é determinístico ($H(V|U) = 0$)(Definição 29), i.e., todas as probabilidades de transição não nulas são iguais a 1 ($V = U$), então a Figura 2.3 descreve uma situação de codificação de fonte usual (ou “compressão de dados") considerada em Teoria da Informação. Quando o canal homofônico é não trivial, mas a codificação binária é trivialmente livre de prefixo porque todas as palavras-código possuem o mesmo comprimento, a Figura 2.3 descreve uma técnica de **substituição homofônica clássica**. Já quando a codificação livre de prefixo é não-trivial, a Figura 2.3 ilustra a técnica de **substituição homofônica de comprimento variável**introduzida por Günther.

As Figuras 2.4 e 2.5, ilustram respectivamente, a técnica de substituição homofônica clássica e a técnica de substituição homofônica de comprimento variável.

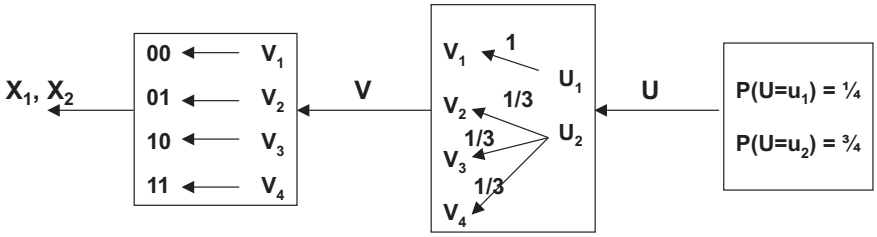


Figura 2.4: Técnica de substituição homofônica clássica.

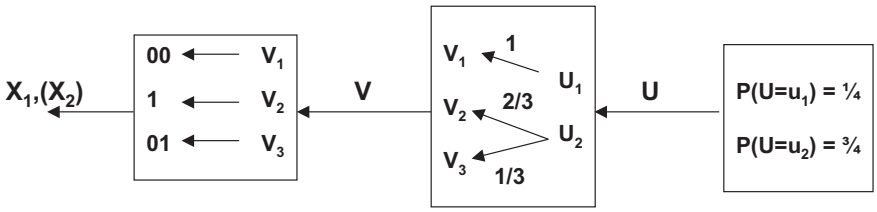


Figura 2.5: Técnica de substituição homofônica de comprimento variável.

Definição 1 *Uma substituição homofônica é dita perfeita se os símbolos D-ários que formam o homofonema, $X_1, X_2, \ldots, X_W$ são independentes e uniformemente distribuídos, i.e., a palavra-código $X_1 X_2 \ldots X_W$ é completamente aleatória.*

□

Proposição 2 *Para a técnica de substituição homofônica ilustrada na Figura 2.3,*

$$H(U) \leq H(V) \leq E(W) \log D, \tag{2.2}$$

com igualdade à esquerda, se e somente se, o canal homofônico é determinístico, e com igualdade à direita, se e somente se, a técnica de substituição homofônica é perfeita. Além disso, existe uma codificação D-ária livre de prefixo de V, tal que a técnica é perfeita, se e somente se, $P_V(v_i) = D^{-l_i}\ \forall i$.

Demonstração:

Parte 1: $H(V) \leq E(W) \log D$.

$$E(W) = \sum_{i=1}^{L} P_i l_i. \text{ (Comprimento médio do código)}$$

$$\sum_{i=1}^{L} D^{-l_i} \leq 1. \text{ (Desigualdade de Kraft)}$$

$$H(V) = -\sum_{i=1}^{L} P_i \log P_i. \tag{2.3}$$

Sejam $Q_1, Q_2, ..., Q_q$ números tais que $Q_i \geq 0 \ \forall i$ e $\sum_{i=1}^{L} Q_i = 1$.

A desigualdade (A.7),

$$\sum_{i=1}^{L} P_i \log \frac{1}{P_i} \leq \sum_{i=1}^{L} P_i \log \frac{1}{Q_i}.$$

aplicada na equação (2.3) produz

$$H(V) \leq -\sum_{i=1}^{L} P_i \log Q_i. \tag{2.4}$$

com igualdade, se e só se, $P_i = Q_i$, $\forall i$.

Como $\sum_{i=1}^{L} Q_i = 1$, pode-se escolher

$$Q_i = \frac{D^{-l_i}}{\sum_{j=1}^{L} D^{-l_j}}. \tag{2.5}$$

Assim, usando (2.5) em (2.4),

$$H(V) \leq -\sum_{i=1}^{L} P_i \log D^{-l_i} + \sum_{i=1}^{L} P_i (\log \sum_{j=1}^{L} D^{-l_j}).$$

$$\leq \log D \sum_{i=1}^{L} P_i l_i + \log \sum_{j=1}^{L} D^{-l_j} \Rightarrow \boxed{H(V) \leq E(W) \log D.}$$

Foi visto que, para que haja igualdade em (2.4), deve-se ter $P_i = Q_i$, i.e.,

$$P_i = \frac{D^{-l_i}}{\sum_{j=1}^{L} D^{-l_j}}.$$

Como $\sum_{j=1}^{L} D^{-l_j} = 1$ o que implica $\boxed{P_i = D^{-l_i}, \forall i.}$

Parte 2: $H(U) \leq H(V)$.

Usando a regra da cadeia para incerteza (equação (A.21)) para U e V, tem-se

$H(V,U) = H(U) + H(V|U) = H(V) + H(U|V)$, sendo o canal considerado sem ruído, i.e., $H(U|V) = 0$

$$H(V) = H(U) + H(V|U).$$

Como $H(V|U) \geq 0$, $\boxed{H(V) \geq H(U).}$

Caso, além de sem ruído o canal seja determinístico ($H(V|U) = 0$) , então $\boxed{H(V) = H(U).}$

■

2.3 Redundância em substituição homofônica

A expansão de texto claro foi definida anteriormente [6] como o comprimento médio do homofonema menos a entropia da fonte, i.e., $E(W) - H(U)$, sendo assumido implicitamente que $H(U|V) = 0$. Esta definição de expansão de texto claro é útil ao se comparar dois sistemas de codificação homofônica que produzem o mesmo número de *bits* por símbolo na saída do canal homofônico e possivelmente possuem valores distintos para $E(W)$.

No contexto de codificação de fonte, para uma dada fonte sem memória U e um código unicamente decodificável (Definição 14) associado a ela, a eficiência do código η é definida [12, p.86] como a razão entre a entropia da fonte $H(U)$ e o comprimento médio da palavra-código $E(W)$, i.e., $\eta = H(U)/E(W)$ (Definição 20) e como conseqüência, a redundância ρ é definida como $\rho = 1-\eta$, i.e. $\rho = [E(W)-H(U)]/E(W)$ (Definição 21). Assim, considerando R a taxa de transmissão de informação numa dada técnica de codificação homofônica, i.e., R denota o número de *bits* por símbolo produzido por uma dada técnica de codificação homofônica na saída de um canal homofônico [‡], são introduzidas a seguir as definições de **redundância** e **eficiência** de uma técnica de codificação homofônica.

Definição 2 *A redundância ρ de uma técnica de codificação homofônica é definida como a razão entre a expansão do texto claro $E(W) - R$ e o comprimento médio de um homofonema $E(W)$, i.e.,*

$$\rho = [E(W) - R]/E(W) = 1 - R/E(W). \tag{2.6}$$

Definição 3 *A eficiência η de uma técnica de codificação homofônica é definida como*

$$\eta = 1 - \rho = R/E(W). \tag{2.7}$$

Jendal-Kuhn-Massey (JKM) [6] definiram codificação homofônica como **perfeita** se a nova seqüência de texto claro é não-redundante e como **ótima** se ela além de perfeita minimizar

[‡]Note que, no caso da técnica JKM [6] R coincide com a entropia da fonte, i.e., $R = H(U)$.

a expansão de texto claro. Ao se comparar uma codificação homofônica para fontes distintas nota-se que uma menor expansão de texto claro não resulta necessariamente numa redundância menor, o que será ilustrado no exemplo a seguir.

Exemplo 1 *Uma técnica de codificação homofônica com taxa* $R_1 = 8$ *e comprimento médio* $E(W_1) = 10$ *tem uma expansão de texto claro* $E(W_1) - R_1 = 2$ *e uma redundância* $[E(W_1) - R_1]/E(W_1) = 0,2$*, enquanto que uma técnica de codificação homofônica com taxa* $R_2 = 3$ *e comprimento médio* $E(W_2) = 4$ *tem uma expansão de texto claro* $E(W_2) - R_2 = 1$ *e uma redundância* $[E(W_2) - R_2]/E(W_2) = 0,25$.

Uma redundância menor significa mais *bits* de entropia por homofonema (dígito de código homofônico binário) enquanto que uma expansão de texto claro menor por se só não fornece uma interpretação objetiva. Este fato ilustra a relevância da nova definição de redundância (Definição 2) na comparação de técnicas de codificação homofônica para fontes distintas.

Desta forma é introduzida a seguir a definição de uma técnica de codificação homofônica **ótima**.

Definição 4 *Uma técnica de substituição (codificação) homofônica é definida como ótima se ela é perfeita e sua redundância é a menor possível.*

2.4 Algumas técnicas de substituição homofônica padrão

2.4.1 Técnica JKM

A título de simplificação, será usado $D = 2$ nesta e em seções subsequentes. Os canais homofônicos binários ($D = 2$) são caracterizados pelo fato que, para cada valor u de U, as probabilidades dos homofonemas para u formam a decomposição de $P_U(u)$ como uma soma de potências inteiras negativas de 2. Por exemplo, na Figura 2.4, $P_U(u_2) = 3/4$ é decomposto como 1/4+1/4+1/4, enquanto que na Figura 2.5, $P_U(u_2) = 3/4$ é decomposto como 1/2+1/4.

Desta forma, a técnica de substituição homofônica ilustrada na Figura 2.5 apresenta um menor $E(W)$, sendo esta a substituição homofônica ótima (considerando que, para este caso, estes são os únicos canais homofônicos possíveis), apesar de ambos os exemplos apresentarem técnicas de substituição homofônica perfeitas. Note que para ambos os casos (Fig. 2.4 e Fig. 2.5), a fonte considerada é a mesma, portanto em ambos os casos $R = H(U) = h(1/4) =$

$0,8113$, em que $h(.)$ denota a entropia binária, e pela equação (2.6) para o esquema da Figura 2.4 tem-se $\rho = 0,5944$ enquanto que para o esquema da Figura 2.5 $\rho = 0,4591$.

O que foi ilustrado por meio dos exemplos das Figuras 2.4 e 2.5 é que, considerando a mesma fonte, se a técnica de substituição homofônica é ótima então a decomposição de $P_U(u)$ para cada u deve consistir de potências negativas distintas de 2. Este fato ocorre, pois dois termos iguais a 2^{-n} contribuem com $2(-2^{-n}\log 2^{-n}) = n2^{(-n+1)}$ para $H(V)$, enquanto que trocando os dois termos 2^{-n} por um único termo formado pela soma deles, $2^{(-n+1)}$, contribui apenas com $-2^{(-n+1)}\log 2^{(-n+1)} = (n-1)2^{(-n+1)}$, que é sempre menor. Desta forma para uma mesma fonte, tendo, portanto $R = H(U)$, expansões com elementos distintos implicam em $E(W)$ menores verificando desta forma pela equação (2.6) que uma menor redundância é alcançada e por conseqüência uma codificação homofônica ótima.

Ao admitir que $L \geq 2$ e que todos os L possíveis valores de U possuem probabilidade não nula assegura que $0 < P_U(u) < 1\ \forall u$. Mas qualquer número real r satisfazendo $0 < r < 1$, ou não possui decomposição como uma soma com uma quantidade finita de potências negativas distintas de 2 (caso em que tal decomposição é única) ou possui uma decomposição com número finito de potências negativas de 2 juntamente com uma única decomposição na forma de somatório formado por um número infinito de potências negativas distintas de 2, nela a menor potência negativa de dois da decomposição com número finito de termos é substituída por uma soma com infinitas potências negativas sucessivas de 2. Por exemplo, 3/8 pode ser decomposto como $1/4 + 1/8$ ou como $1/4 + 1/16 + 1/32 + 1/64 + ...$ Esta decomposição com número de termos finito (quando possível) sempre contribui menos para $H(V)$ do que a decomposição com número infinito de termos, isto porque

$$-\sum_{n=k+1}^{\infty} 2^{-n}\log(2^{-n}) = (k+2)2^{-k} > -2^{-k}\log(2^{-k}) = k2^{-k}.$$

Proposição 3 *Uma técnica de codificação homofônica é dita ótima para uma dada fonte U, se e só se, $\forall u_i$ de U, as probabilidades condicionais $P_{V|U}(v_{ij}|u_i)$ dos homofonemas para u_i são tais que as probabilidades $P_V(v_{ij}) = P_{V,U}(v_{ij}, u_i) = P_{V|U}(v_{ij}|u_i)P_U(u_i)$ desses homofonemas são iguais (em alguma ordem) aos termos na única decomposição de $P_U(u_i)$ como uma soma com número finito de potências negativas distintas de 2 quando $P_U(u_i) = j/2^n$ para j e n inteiros positivos, e caso contrário, como uma soma com número infinito de potências negativas distintas de 2.*

□

Assim, no caso da decomposição finita o homofonema é selecionado lançando uma moeda honesta no máximo a quantidade indicada pelo expoente da potência de 2 no denominador de $P_U(u_i)$, caso contrário não existe cota superior para a quantidade de lançamentos necessários.

Neste mesmo trabalho [6], uma cota superior foi introduzida com relação à redundância a qual teve sua prova em [13]. Tal resultado é mostrado na proposição a seguir.

Proposição 4 *Para uma técnica de substituição homofônica ótima binária,*

$$H(U) \leq H(V) = E(W) < H(U) + 2. \tag{2.8}$$

Demonstração:

Seja $p_1^{(1)}, p_2^{(1)}, ..., p_{L^{(1)}}^{(1)}$ a distribuição de probabilidade $P_{V|U}(.|u)$.

Lembrando que o canal homofônico é um canal sem memória cujo alfabeto de entrada $\{u_1, u_2, ..., u_L\}$ coincide com o conjunto de possíveis valores de U, o alfabeto de saída V pode ser finito ou infinito contável, e as probabilidades de transição $P_{V|U}(v_{ij}|u_i)$ têm a propriedade que para cada j existe exatamente um i tal que $P_{V|U}(v_{ij}|u_i) \neq 0$. Portanto, a notação simplificada $P_{V|U}(.|u)$ usada indica que u recebe valores u_i onde $0 < i \leq L$ e os homofonemas v_{ij} relacionados a cada u_i podem ser de número finito ou finito contável.

Do modo como os homofonemas são gerados, tem-se que,

$$p_{i+1}^{(1)} \leq p_i^{(1)}/2 \text{ para } 1 \leq i < L^{(1)}.$$

O que implica em $p_1^{(1)} > 1/2$.

Pelo "Refinamento" de Shannon

$$H(p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}) = H(p_1^{(1)}, 1 - p_1^{(1)}) + (1 - p_1^{(1)}) H(p_1^{(2)}, p_2^{(2)}, \ldots, p_{L^{(2)}}^{(2)}).$$

Sendo,

$$p_i^{(2)} = p_{i+1}^{(1)}/(1 - p_1^{(1)}) \text{ e } L^{(2)} = L^{(1)} - 1.$$

Assim,

$$H(p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}) < 1 + \frac{1}{2} H(p_1^{(2)}, p_2^{(2)}, \ldots, p_{L^{(2)}}^{(2)}).$$

Mas a distribuição de probabilidade $p_1^{(2)}, p_2^{(2)}, \ldots, p_{L^{(2)}}^{(2)}$ herda as propriedades anteriores de $p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}$, logo

$$p_{i+1}^{(2)} \leq p_i^{(2)}/2 \text{ para } 1 \leq i < L^{(2)} \text{ e } p_1^{(2)} > 1/2.$$

Aplicando o mesmo argumento novamente, tem-se,

$$H(p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}) < 1 + \frac{1}{2}\left[1 + \frac{1}{2}H(p_1^{(3)}, p_2^{(3)}, \ldots, p_{L^{(3)}}^{(3)})\right].$$

Repetindo o argumento um total de $L^{(1)} - 2$ vezes, chega-se a,

$$H(p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}) < 1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^{L^{(1)}-3}} + \frac{1}{2^{L^{(1)}-2}}H(p_1^{(L^{(1)}-1)}, p_2^{(L^{(1)}-1)})$$

e portanto,

$$H(p_1^{(1)}, p_2^{(1)}, \ldots, p_{L^{(1)}}^{(1)}) < 1 + \tfrac{1}{2} + \tfrac{1}{4} + \cdots + \tfrac{1}{2^{L^{(1)}-3}} + \tfrac{1}{2^{L^{(1)}-2}} < 2 \textit{ bits.}$$

Ou seja,

$$H(V|U) < 2.$$

Logo,

$$\boxed{\text{H(V)<H(U)+ 2.}} \tag{2.9}$$

■

Concluindo desta forma a partir da Proposição 4 que numa técnica de substituição (codificação) homofônica ótima a entropia da entrada nunca é aumentada em mais de 2 *bits*, não importando quão grande é $H(U)$.

Vale salientar que todos os resultados obtidos na seção 2.4.1 são generalizados para o caso D-ário, $D > 2$. Na Proposição 3, "2" deve ser substituído por "D" e "distinto" por "ocorrendo no máximo D-1 vezes". As desigualdades na Proposição 4 tornam-se $H(U) \leq E(W)\log D < H(U) + \frac{D}{D-1}\log D$.

2.4.2 Codificação homofônica Rocha-Massey

A técnica de substituição homofônica Rocha-Massey (RM) introduzida pelos professores Valdemar C. da Rocha Jr e James Massey em [7] foi criada com o intuito de superar o problema da falta de cota superior com relação ao número de lançamentos necessários para a escolha do homofonema na técnica JKM quando $P_U(u_i)$ é decomposto como uma soma com número infinito de termos.

A solução proposta consiste na expansão do alfabeto original com a inserção de um símbolo mudo, Δ, tal que todos os símbolos possuam probabilidades da forma $P_U(u_i) = 1/2^N$, não havendo, portanto a ausência de cota superior para o número de lançamentos necessários para a escolha do homofonema.

Descrição da técnica

Admite-se que U tem uma distribuição de probabilidade racional e que n é o menor denominador comum dessas probabilidades, i.e., $P_U(u_i) = m_i/n$, $1 \leq i \leq L$, em que m_i e n são inteiros positivos e n é o menor possível.

Se n é uma potência de 2, a técnica JKM se mostra eficiente, havendo cota superior para o número de lançamentos de moedas honestas a fim de determinar o homofonema.

O interesse, portanto, está no caso em que n não é uma potência de 2. Neste caso, a técnica RM consiste na expansão do alfabeto original $U = \{u_1, u_2, ..., u_L\}$, inserido o símbolo Δ, obtendo como resultado o alfabeto expandido, $\tilde{U} = \{u_1, u_2, ..., u_L, \Delta\}$, tal que $P_{\tilde{U}}(\Delta) = (2^N - n)/2^N$, em que $N = \lceil \log_2 n \rceil$. Fazendo com que $P_{\tilde{U}}(u_i) = (n/2^N)P_U(u_i) = m_i/2^N$ para $1 \leq i \leq K$.

Assim, todos os símbolos da fonte expandida têm probabilidades com denominador comum 2^N. Segue-se, portanto que no máximo N lançamentos de moedas honestas são necessários na escolha do homofonema se uma técnica de substituição homofônica padrão [6] for usada na saída da fonte expandida.

Exemplo 2 *Considere $P_U(u_1) = 1/3$ e $P_U(u_2) = 2/3$. A técnica JKM descrita na seção 2.4.1 usa uma decomposição com uma quantidade infinita de potências negativas distintas de 2 para $P_U(u_1)$ e $P_U(u_2)$. Assim, procedendo a decomposição das probabilidades dos símbolos da fonte, considerando a técnica descrita em [14], obtém-se,*

$$P_U(u_1) = \frac{1}{3} = \frac{\left(\frac{1}{3}\right)\left(\frac{3}{4}\right)}{\left(\frac{3}{4}\right)} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

$$P_U(u_2) = \frac{2}{3} = \frac{\left(\frac{2}{3}\right)\left(\frac{3}{4}\right)}{\left(\frac{3}{4}\right)} = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

Assim, o comprimento médio é dado por $E(W) = \sum_i P_U(u_i) l_i = 2$*, e portanto, a eficiência,* $\eta = \dfrac{H(U)}{E(W)} = \dfrac{0,9183}{2} = 0,4591$ *e conseqüentemente, redundância igual a* $\rho = 0,5409$.

Expandindo esta fonte com um símbolo mudo, Δ*, de probabilidade* $P_{\tilde{U}}(\Delta) = 1/4$*, tem-se* $P_{\tilde{U}}(u_1) = (3/4)(1/3) = 1/4$ *e* $P_{\tilde{U}}(u_2) = (3/4)(2/3) = 1/2$*. Desta forma são necessários no máximo 2 lançamentos de moeda honesta a fim de selecionar qualquer homofonema.*

Como as probabilidades dos símbolos da fonte expandida são potências inteiras negativas de 2, $E(\tilde{W}) = H(\tilde{U}) = \left(\dfrac{1}{2}\right) \cdot 1 + \left(\dfrac{1}{4}\right) \cdot 2 + \left(\dfrac{1}{4}\right) \cdot 2 = 1,5$*, sendo a eficiência dada por* $\tilde{\eta} = \dfrac{(1 - P(\Delta))H(U)}{E(W)} = \dfrac{\left(\frac{3}{4}\right) 0,9183}{1,5} \Rightarrow \tilde{\eta} = 0,4591$ *e redundância* $\tilde{\rho} = 0,5409$.

□

Note que caso fosse usado o critério de expansão de texto claro, i.e., $E(W) - H(U)$, a técnica RM mostraria um resultado substancialmente melhor que a técnica JKM uma vez que para esse exemplo que usa a técnica JKM a expansão de texto claro seria dada por 1,082, enquanto que para a técnica RM seria de 0,8115. Já pelo critério da redundância, cuja definição foi introduzida na seção 2.3, nota-se que as duas obtém o mesmo valor, porém vale salientar que a técnica RM possui a vantagem de limitar o número de experimentos a fim de selecionar o homofonema.

Implementando a técnica Rocha-Massey

A técnica em questão pode ser implementada da seguinte forma:

Inicialmente, usa-se uma moeda honesta para testar a ocorrência de um evento com probabilidade $p = 1 - P_{\tilde{U}}(\Delta) = n/2^N$, o que requer no máximo N lançamentos. Se tal evento ocorre, a fonte emite um símbolo o que será a saída de $\tilde{U}$. Caso contrário, o símbolo mudo, Δ, se torna a saída da fonte $\tilde{U}$. A decodificação é bastante simples, bastando para isto apenas a retirada dos Δ da saída de $\tilde{U}$ a fim de se obter a seqüência de saída de U.

2.4.3 Técnica JKM modificada

A principal queixa com relação ao uso prático da técnica JKM é devido a sua aparente necessidade de armazenar um dicionário com número ilimitado de homofonemas.

A técnica JKM modificada introduzida em [8] consiste basicamente na construção seqüencial de cada palavra-código homofônica (homofonema), como a concatenação de palavras-

código menores apropriadamente selecionadas de um conjunto finito de palavras-código derivadas das probabilidades da fonte.

Descrição da Técnica JKM modificada

A fim de facilitar o entendimento da técnica, a descrição da mesma será feita paralelamente a um exemplo.

Exemplo 3 *Considere as seguintes probabilidades dos elementos de uma fonte discreta binária sem memória,* $P_U(u_1) = 1/5$ *e* $P_U(u_2) = 4/5$.

Passo 1 *Geração das palavras-código derivadas das probabilidades da fonte*

1. *Expandir as probabilidades da fonte como uma soma de potências negativas de* $D = 2$.

   Procedendo a decomposição das probabilidades dos símbolos da fonte segundo a técnica descrita em [14], obtém-se,

$$\begin{aligned} P_U(u_1) &= \frac{1}{5} = \frac{\left(\frac{1}{5}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\left(\frac{1}{8}\right)+\left(\frac{1}{16}\right)}{\left(\frac{15}{16}\right)} \\ &= \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i. \end{aligned} \tag{2.10}$$

$$\begin{aligned} P_U(u_2) &= \frac{4}{5} = \frac{\left(\frac{4}{5}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\left(\frac{1}{2}\right)+\left(\frac{1}{4}\right)}{\left(\frac{15}{16}\right)} \\ &= \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i. \end{aligned} \tag{2.11}$$

2. *Identificar na expansão os componentes periódicos*[§] *e não-periódicos*[¶]

   Nota-se que os elementos periódicos de (2.10) são $\frac{1}{8}, \frac{1}{16}$ *(primeiros termos) e* $\frac{1}{16}$ *(razão). Já em (2.11) os elementos periódicos são* $\frac{1}{2}$, $\frac{1}{4}$ *(primeiros termos) e* $\frac{1}{16}$ *(razão). Não havendo, em ambas as expansões, elementos não-periódicos.*

[§]Periódicos: O conjunto consistindo de termos de uma série geométrica infinita cujo primeiro termo e a razão são potências negativas de 2.

[¶]Não-periódicos: O conjunto consistindo de um número finito de potências negativas de 2.

3. *Construir um código C binário livre de prefixo usando como probabilidades das palavras-código, os componentes não-periódicos, e o primeiro termo e razão do componente periódico, obtidos em (1.) e (2.)*[‖].

$$1^{os} termos = \begin{cases} \frac{1}{2} & 0 \\ \frac{1}{4} & 10 \\ \frac{1}{8} & 110 \\ \frac{1}{16} & 1110 \end{cases}$$

$$Razão \rightarrow \frac{1}{16} \quad 1111$$

Passo 2 *Construção dos homofonemas utilizando as palavras-código geradas no Passo 1.*

Em geral, faz-se com que a fonte U emita um símbolo u_i e então, um experimento é feito a fim de selecionar o homofonema que será associado a u_i. Nesta nova técnica é introduzida uma pequena, mas significativa variação. Em vez de considerar no início o conjunto de todos homofonemas correspondentes a $U = u_i$, este conjunto é particionado em subconjuntos. Cada termo não-periódico corresponde a um subconjunto com um único homofonema e cada elemento periódico corresponde a um subconjunto com número infinito contável de homofonemas. A seleção do homofonema é, então, feita em duas partes: Primeiro seleciona-se o subconjunto e a seguir um homofonema pertencente ao subconjunto é selecionado.

Assim,

1. *A fonte emite o símbolo u_i.*
2. *Seleciona-se o subconjunto:*
   (a) *Se o homofonema a ser selecionado corresponde a um componente não-periódico, então a saída V será a palavra-código do subconjunto.*
   (b) *Se o homofonema a ser selecionado corresponde a um dos termos do j-ésimo componente periódico, $j = 1, 2, \ldots$, então um experimento binário é feito.*

   Descrição do experimento binário:

   $P(E_j) = 1 - P(\Delta_{ij})$

   $P(\overline{E}_j) = P(\Delta_{ij})$,

[‖] Obs: razões idênticas são associadas à mesma palavra-código.

sendo $P(\Delta_{ij})$ a razão da série geométrica correspondente, e Δ_{ij} o símbolo mudo associado ao j-ésimo componente periódico da expansão de $P_U(u_i)$.

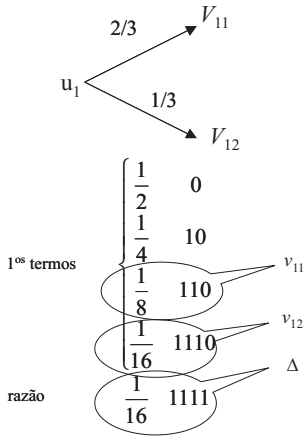
- *Se E_j é o resultado do experimento, então a saída de V será a palavra-código correspondente ao primeiro termo do j-ésimo componente periódico da expansão de $P_U(u_i)$, correspondendo ao homofonema v_{ij}.*
- *Se $\overline{E}_j$ é o resultado do experimento, então u_i é armazenado, a palavra-código associada à razão da série geométrica (Δ_{ij}). O experimento é repetido até que E_j ocorra e v_{ij} se torne o último símbolo do homofonema $\Delta_{ij}\Delta_{ij}...\Delta_{ij}v_{ij}$ que será a saída de V.*

  Considerando a expansão (2.10),

$$P_V(V_{11}) = \sum_{i=0}^{\infty} \left(\frac{1}{8}\right)\left(\frac{1}{16}\right)^i = \frac{2}{15}. \tag{2.12}$$

$$P_V(V_{12}) = \sum_{i=0}^{\infty} \left(\frac{1}{16}\right)\left(\frac{1}{16}\right)^i = \frac{1}{15}. \tag{2.13}$$

  Assim, dado $U = u_1$



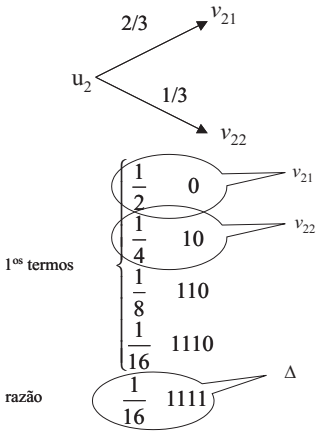
$V_{11} = \{v_{11}, \Delta v_{11}, \Delta\Delta v_{11}, \dots\} = \{110, 1111|110, 1111|1111|110, \dots\}.$
$V_{12} = \{v_{12}, \Delta v_{12}, \Delta\Delta v_{12}, ...\} = \{1110, 1111|1110, 1111|1111|1110, ...\}.$

  Para a expansão (2.11),

$$P_V(V_{21}) = \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)\left(\frac{1}{16}\right)^i = \frac{8}{15}. \tag{2.14}$$

$$P_V(V_{22}) = \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)\left(\frac{1}{16}\right)^i = \frac{4}{15}. \tag{2.15}$$

Assim, dado $U = u_2$



$$V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, ...\} = \{0, 1111|0, 1111|1111|0, ...\}.$$
$$V_{22} = \{v_{22}, \Delta v_{22}, \Delta\Delta v_{22}, ...\} = \{10, 1111|10, 1111|1111|10, ...\}.$$

Note que v_{11} *é mapeado em* 110 *no conjunto* V_{11}*,* v_{12} *é mapeado em* 1110 *no conjunto* V_{12}*,* v_{21} *é mapeado em* 0 *no conjunto* V_{21} *e* v_{22} *é mapeado em* 10 *no conjunto* V_{22}*. Sem esquecer que* Δ *é mapeado em* 1111*, e que "*$a|b$*"denota a concatenado com* b*.*

□

O sucesso da implementação seqüencial da técnica JKM depende da veracidade da seguinte proposição:

Proposição 5 *Em qualquer distribuição de probabilidade com apenas entradas racionais, uma probabilidade pode sempre ser decomposta em base 2 como uma soma de um número finito de componentes distintos não-periódicos mais um número finito de componentes periódicos distintos (série geométrica distinta) cujo primeiro termo e a razão são potências negativas de 2.*

□

Exemplo 4 *Considere uma fonte discreta binária sem memória com* $P_U(u_1) = 7/10$ *e* $P_U(u_2) = 3/10$.

Procedendo a decomposição das probabilidades dos símbolos da fonte, usando a técnica em [14] obtém-se,

$$P_U(u_1) = \frac{7}{10} = \left(\frac{1}{2}\right)\left(\frac{7}{5}\right) = \left(\frac{1}{2}\right)\left[1 + \frac{2}{5}\right] = \frac{1}{2} + \frac{1}{5}.$$

Do exemplo 3,

$$\frac{1}{5} = \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Logo,

$$P_U(u_1) = \frac{7}{10} = \frac{1}{2} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Para o símbolo u_2*,*

$$P_U(u_2) = \frac{3}{10} = \left(\frac{1}{2}\right)\left(\frac{3}{5}\right).$$

Por sua vez,

$$\left(\frac{3}{5}\right) = \frac{\left(\frac{3}{5}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\left(\frac{1}{2}\right) + \left(\frac{1}{16}\right)}{\left(\frac{15}{16}\right)} = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Logo,

$$P_U(u_2) = \frac{3}{10} = \left(\frac{1}{2}\right)\left(\frac{3}{5}\right) = \left(\frac{1}{2}\right)\left[\left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i\right] \Rightarrow$$

$$P_U(u_2) = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Aplicando a técnica JKM para esta fonte obtém-se $\rho = [1-H(U)/E(W)] = [1-h(3/10)/2] = 1-0,8813/2 = 0,5594$, *enquanto que usando a técnica RM,* $\tilde{\rho} = [1-(15/16)H(U)/E(\tilde{W})] = [1-0,8262/(31/16)] = 0,5736$ *com* $P_{\tilde{U}}(\Delta) = 1/16$.

□

Esse exemplo mostra que nem sempre a técnica RM produz menor redundância que a técnica JKM. A razão pela qual a técnica JKM supera a técnica RM, nesse caso, se deve ao fato de haver um componente não-periódico na expansão binária de uma das probabilidades dos símbolos da fonte.

Mostra-se a seguir que, em geral, para qualquer canal K-ário discreto sem memória cujos símbolos da fonte possuem probabilidades que são números racionais, a técnica RM apresenta menor redundância que a JKM, se e só se, cada uma das probabilidades dos símbolos da fonte tiverem apenas componentes periódicos. Tal resultado é mostrado na proposição a seguir [15].

Proposição 6 *Para uma fonte discreta sem memória com distribuição de probabilidade cujas probabilidades são apenas números da forma racional, de modo que cada uma dessas probabilidades seja expandida apenas com componentes periódicos, a redundância*

$$\tilde{\rho} = [E(\tilde{W}) - \left(1-2^{-m}\right)H(\tilde{U})]/E(\tilde{W}) \tag{2.16}$$

da técnica RM será igual à redundância

$$\rho = [E(W) - H(U)]/E(W) \tag{2.17}$$

da técnica JKM, i.e., $\rho = \tilde{\rho}$.

□

Demonstração:

Suponha que a expansão binária de $P_U(u_i)$, $1 \leq i \leq K$, tem apenas componentes periódicos, i.e., suponha que

$$P_U(u_i) = \sum_{i=1}^{J_i} \sum_{l=0}^{\infty} 2^{-r_j - lm} = \frac{\sum_{i=1}^{J_i} 2^{-r_j}}{1 - 2^{-m}}$$

Segue-se da técnica RM que $P_{\tilde{U}}(u_i) = (1 - 2^{-m})P_U(u_i) = \sum_{i=1}^{J_i} 2^{-r_j}$, $1 \leq i \leq K$.

Para substituição homofônica padrão segue-se que

$$H(V) = H(U) + H(V|U) \tag{2.18}$$

e similarmente, para a fonte expandida da técnica RM segue-se que

$$H(\tilde{V}) = H(\tilde{U}) + H(\tilde{V}|\tilde{U}) \tag{2.19}$$

Como na técnica RM

$$H(\tilde{U}) = (1 - 2^{-m})H(U) + h(2^{-m}). \tag{2.20}$$

Combinando (2.18), (2.19) e (2.20), e fazendo $\beta_m = 1 - 2^m$, obtém-se

$$\begin{aligned} H(\tilde{V}) &= \beta_m H(V) + h(2^{-m}) \\ &- [\beta_m H(V|U) - H(\tilde{V}|\tilde{U})] \qquad (2.21) \\ &= \beta_m H(V) + h(2^{-m}) \\ &- \beta_m \sum_{i=1}^{K} P_U(u_i)[H(V|U = u_i) - H(\tilde{V}|\tilde{U} = u_i)], \qquad (2.22) \end{aligned}$$

em que em (2.22) usou-se o fato que $P_{\tilde{U}}(u_i) = (1-2^{-m})P_U(u_i)$. Observa-se em (2.22), porém, que os termos na expressão para $H_{\tilde{V}|\tilde{U}}(.|u_i)$ estão contidos na expressão para $H_{V|U}(.|u_i)$, e como ambas as entropias $H_{\tilde{V}|\tilde{U}}(.|u_i)$ e $H_{V|U}(.|u_i)$ são não negativas, segue-se que $H_{V|U}(.|u_i) \geq H_{\tilde{V}|\tilde{U}}(.|u_i)$. Como $P_{\tilde{U}}(u_i) = \sum_{i=1}^{J_i} 2^{-r_j}$, em que J_i e r_i são inteiros positivos, segue-se que para cada j, $1 \leq j \leq J_i$, $\tilde{V} = v_{ij}$ com probabilidade $P_{\tilde{V}}(v_{ij}) = 2^{-r_j}$, e assim pode-se escrever $P_{\tilde{V}|\tilde{U}}(v_{ij}|u_i) = 2^{-r_j}/[(1 - 2^{-m})P_U(u_i)] = \alpha_{ij}$.

Da técnica RM,

$$H_{\tilde{V}|\tilde{U}}(.|u_i) = -\sum_{i=1}^{J_i} \alpha_{ij} \log \alpha ij \tag{2.23}$$

$$= \sum_{i=1}^{J_i} r_j \alpha_{ij} - \log \frac{1}{P_U(u_i)} + \log(1 - 2^{-m}). \tag{2.24}$$

Similarmente, desde que, $P_U(u_i) = \sum_{j=1}^{J_i} \sum_{l=0}^{\infty} 2^{-r_j - lm}$, segue-se que $P_{V|U}(v_{i,j+lm}|u_i) = 2^{-r_j - lm}/P_U(u_i)$, e pode-se escrever para codificação homofônica padrão,

$$H_{V|U}(.|u_i) = -\sum_{l=0}^{\infty} \sum_{j=1}^{J_i} \frac{2^{-r_j - lm}}{P_U(u_i)} \log \frac{2^{-r_j - lm}}{P_U(u_i)}$$

$$= \sum_{j=1}^{J_i} r_j \alpha_{ij} - \log \frac{1}{P_U(u_i)} + \frac{m 2^{-m}}{1 - 2^{-m}}. \tag{2.25}$$

Subtraindo (2.23) de (2.25) e multiplicando o resultado por $(1 - 2^{-m})P_U(u_i)$, tem-se,

$$(1 - 2^{-m})P_U(u_i)[H_{V|U}(.|u_i) - H_{\tilde{V}|\tilde{U}}(.|u_i)] = P_U(u_i)h(2^{-m}). \tag{2.26}$$

Finalmente, com (2.26) em (2.21) segue-se que,

$$H(\tilde{V}) = (1 - 2^{-m})H(V). \tag{2.27}$$

Entretanto, como todas as probabilidades tanto em V quanto em $\tilde{V}$ são potências negativas de 2, segue-se que $E(W) = H(V)$ e que $E(\tilde{W}) = H(\tilde{V})$, e assim (2.27) pode ser reescrita como

$$E(\tilde{W}) = (1 - 2^{-m})E(W). \tag{2.28}$$

Sob a suposição feita sobre $P_U(u_i), 1 \leq i \leq K$ no início da prova, de (2.28) conclui-se que a redundância da técnica RM é dada por,

$$\tilde{\rho} = [E(\tilde{W}) - (1 - 2^{-m})H(U)]/E(\tilde{W}), \tag{2.29}$$

enquanto que a redundância correspondente à técnica JKM é dada por

$$\rho = [E(W) - H(U)]/E(W). \tag{2.30}$$

Rearrumando (2.30), tem-se que $H(U)$ é dado por

$$H(U) = E(W) - \rho E(W). \tag{2.31}$$

Com (2.31) em (2.29) chega-se a,

$$\tilde{\rho} = \frac{E(\tilde{W}) - (1 - 2^{-m})[E(W) - \rho E(W)]}{E(\tilde{W})}. \tag{2.32}$$

Usando (2.28) em (2.32),

$$\tilde{\rho} = \frac{E(\tilde{W}) - E(\tilde{W}) + \rho E(\tilde{W})}{E(\tilde{W})} \Rightarrow \tilde{\rho} = \rho.$$

Concluindo assim que quando a expansão binária de $P_U(u_i)$, $1 \leq i \leq K$, tem apenas componentes periódicos, as redundâncias para as técnicas JKM [6] e RM [7] são iguais.

■

2.5 Codificação homofônica símbolo-a-símbolo

Nesta seção é introduzida uma nova classe de técnicas de substituição homofônica denominada **Substituição Homofônica Símbolo-a-Símbolo(SAS)**. A primeira tentativa de uma técnica nessa classe, que foi denominada **Substituição Homofônica Símbolo-a-Símbolo 1 (SH-SAS1)**, apresentou uma dependência estatística entre os símbolos dos homofonemas devido aos valores de probabilidade escolhidos para o símbolo mudo, sendo, portanto uma técnica de substituição homofônica não-perfeita. Como o objetivo aqui é procurar alternativas que proporcionem de alguma forma melhor desempenho em comparação com as técnicas de substituição homofônica perfeitas conhecidas como, por exemplo, as técnicas RM [7] e JKM [6], uma investigação visando obter uma alternativa que mostrasse independência estatística entre os símbolos dos homofonemas resultou na técnica de substituição homofônica símbolo-a-símbolo que é introduzida na seção 2.5.1.

2.5.1 Técnica de substituição homofônica símbolo-a-símbolo 2 (SH-SAS2)

Como citado anteriormente a técnica denominada SH-SAS1 não é uma técnica de substituição homofônica perfeita, como por exemplo, as técnicas RM [7] e JKM [6], apesar de inicialmente ter se pensado nela como uma alternativa de técnica de substituição homofônica para os casos em que um ou mais elementos da fonte não possuem probabilidade de ocorrência da forma $m_i/2^{s_i}$, em que s_i é um inteiro positivo. Como conseqüência, ao se investigar

uma alternativa que mostrasse um melhor desempenho, se comparado com a eficiência (η) alcançada pelas técnicas existentes, chegou-se à técnica que será abordada nesta seção, a qual foi denominada **Substituição Homofônica Símbolo-a-Símbolo 2**.

Considere mais uma vez, uma fonte U discreta sem memória tal que sua distribuição de probabilidade é formada por números racionais $P_U(u_i) = m_i/n_i, 1 \leq i \leq K$, em que m_i e n_i são números inteiros positivos e n_i é o menor possível. Se n_i é uma potência D-ária, i.e., $n_i = D^{l_i}$, a técnica JKM [6], como visto na Seção 2.4.1, opera com cota superior finita requerendo um número finito de experimentos a fim de selecionar um homofonema associado ao elemento u_i da fonte U, o que não ocorre no caso em que $n_i \neq D^{l_i}$. Caso este de interesse já tendo sido abordado anteriormente, como por exemplo em [7, 15].

O objetivo desta seção é introduzir uma nova técnica de substituição homofônica padrão que mostra desempenho equivalente ao obtido utilizando a técnica JKM [6] (seção 2.4.1), considerando como parâmetro a eficiência η (Definição 3).

De modo similar à técnica JKM modificada [8] (seção 2.4.3), na nova técnica, cada palavra-código homofônica é construída como a concatenação de palavras-código mais curtas derivadas a partir das probabilidades da fonte, resolvendo desta forma o problema de ter que armazenar um número infinito contável de palavras-código homofônicas, no caso em que n_i não é uma potência de D.

Observa-se que diferentemente da técnica JKM modificada (seção 2.4.3), na técnica SH-SAS2 pode-se optar para ter apenas um símbolo mudo, i.e., independente da expansão do símbolo da fonte apenas uma palavra-código será associada ao símbolo mudo. O que é ilustrado no Exemplo 10.

Na técnica SH-SAS 2, a fonte é requisitada a emitir um símbolo u_i e a partir daí um procedimento é feito a fim de determinar o homofonema associado a este símbolo. Tal procedimento é descrito a seguir.

Descrição da técnica SH-SAS 2

Com a finalidade de simplificar a descrição, é considerado o caso binário, i.e., $D = 2$.

a) Para cada símbolo da fonte $U = u_i$, $1 \leq i \leq K$, com probabilidade $P_U(u_i) = m_i/2^{s_i}$, i.e., para o qual $n_i = 2^{s_i}$, em que s_i é um inteiro positivo, escreve-se m_i na base 2 e a cada termo desta decomposição em base 2 associa-se um homofonema, tal que $P_V(v_{ij}) = 2^{-l_j}$.

b) Para cada símbolo da fonte $U = u_i$, $1 \leq i \leq K$, com probabilidade $P_U(u_i) = m_i/n_i$, para

o qual $n_i \neq 2^{s_i}$, associam-se dois tipos de símbolos chamados, respectivamente, **símbolo homofonema** e **homofonema mudo**.

Considere que n é o menor denominador comum dessas probabilidades. Sendo $n = 2^r n'$ em que n' é o produto dos fatores ímpares de n e r um inteiro positivo, escolha s tal que $n' | 2^s - 1$.

1. Se a decomposição das probabilidades de todos os símbolos da fonte possui apenas termos periódicos, então, dado que a fonte U seleciona um símbolo u_i, um experimento é feito em que o símbolo mudo tem probabilidade $P(\Delta) = P(\Delta|u_i) = 1/2^s$, e desta forma o homofonema é selecionado com probabilidade $P_{V|U}(v_{ij}|u_i) = P_{ij}/P_U(u_i)$, observando que P_{ij} é o j-ésimo termo da decomposição em potências negativas de 2 de $\dfrac{m_i \cdot d}{2^s}$ em que d é um número inteiro positivo e $P_U(u_i)(1 - 2^{-s}) = \left(\dfrac{2^s - 1}{2^s}\right)\left(\dfrac{m_i}{n_i}\right) = \dfrac{m_i \cdot d}{2^s}$. Assim V é uma fonte discreta sem memória tendo como símbolos os símbolos homofonemas de U com probabilidade $P_V(v_{ij}) = P_U(u_i)P_{V|U}(v_{ij}|u_i)$ e um homofonema mudo com probabilidade $P(\Delta) = P(\Delta|u_i) = 1/2^s$.

2. Se a decomposição da probabilidade de um ou mais símbolos da fonte possui termos não periódicos, cuja probabilidade do termo não periódico associado ao símbolo u_i é 2^{-j_r}, a probabilidade de seleção deste termo é $2^{-j_r}/P_U(u_i)$ e neste caso não há escolha entre o homofonema e o símbolo mudo. Os demais homofonemas são selecionados com probabilidade

$$P_{V|U}(v_{ij}|u_i) = \frac{P_{ij}}{\left[1 - \sum_r \left(\frac{2^{-j_r}}{P_U(u_i)}\right)\right] \cdot P_U(u_i)},$$

observando que P_{ij} é o j-ésimo termo da decomposição em potências negativas de 2 de

$$P_U(u_i) \cdot \left[1 - \sum_r \left(\frac{2^{-j_r}}{P_U(u_i)}\right)\right] \cdot [1 - 2^{-s}],$$

lembrando que o símbolo mudo possui probabilidade 2^{-s}.

Se o termo não periódico não for tratado desta forma, i.e., um termo que ao ser selecionado é imediatamente relacionado a um homofonema, aparecerão termos repetidos na representação do símbolo da fonte, e como já foi mostrado na seção 2.4.1, "considerando a mesma fonte, se a técnica de substituição homofônica é ótima então a decomposição de $P_U(u_i)$ para cada u_i deve consistir de potências negativas distintas de 2", ou seja, ao se considerar a expansão em termos distintos, $E(W)$ é minimizado e portanto η é maximizada para tal fonte. Tal situação é ilustrada na forma de exemplos.

c) A codificação binária nesta técnica é feita da seguinte forma.

1. Inicia-se uma árvore binária associando-se às folhas distantes l_j da raiz os homofonemas cuja probabilidade é igual a $P_V(v_{ij}) = P_U(u_i)P_{V|U}(v_{ij}|u_i) = 2^{-l_j}$.

   Note que a probabilidade do símbolo mudo é probabilidade de transição $P(\Delta|u_i)$ e, portanto nesta técnica está associada à palavra-código terminada num nó intermediário da árvore.

2. As palavras-código são construídas associando aos ramos superiores "0" e inferiores "1", seguindo então, o caminho da raiz à folha associada ao homofonema.

3. A construção da palavra-código associada ao símbolo mudo é feita de forma similar à construção da palavra-código do homofonema, porém vai até o nó associado ao Δ.

   Para evitar que haja problema na decodificação deve-se observar que a palavra-código formada pela concatenação do símbolo mudo e de um homofonema não deve ser igual à outra palavra-código homofônica nem prefixo de uma outra palavra-código homofônica mais longa. Com exceção das palavras-código associadas a homofonemas que não fazem uso do símbolo mudo, i.e., homofonemas associados a símbolos do tipo 2^{-l_j}, uma vez que nesse caso o símbolo mudo nunca precederá tal palavra-código homofônica (observar Exemplos 8 e 9).

   Desta forma tal código é considerado um código unicamente decodificável, tornando a decodificação trivial como visto mais adiante.

d) Quando um homofonema mudo Δ é produzido no passo b), um símbolo mudo Δ é produzido por V e o experimento de seleção é repetido quantas vezes forem necessárias até que o correspondente símbolo homofonema v_{ij}, seja selecionado, tendo como resultado uma seqüência do tipo $\Delta\Delta\Delta\Delta \ldots \Delta v_{ij}$. A fonte U é então requisitada a selecionar o próximo símbolo a ser codificado e assim por diante.

e) A decodificação é imediata, bastando apenas, apagar as palavras-código que representam os símbolos mudos e, em seguida, as palavras-código restantes são mapeadas uma a uma aos símbolos de U.

A seguir a técnica aqui introduzida é ilustrada e comentada com alguns exemplos.

Exemplos Ilustrativos

Exemplo 5 *Considere uma fonte discreta binária sem memória com* $K = 2$*, obedecendo a seguinte distribuição de probabilidade* $P_U(u_1) = 1/3$ *e* $P_U(u_2) = 2/3$*.*

Segundo o passo b) da descrição da técnica SH-SAS2, $n = 3$ *e* $s = 2$*, portanto* $P(\Delta) = P(\Delta|u_i) = 1/4$*.*

Observe que,

$$P_U(u_1) = \frac{1}{3} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

$$P_U(u_2) = \frac{2}{3} = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

Como a decomposição das probabilidades dos símbolos apresenta apenas termos periódicos segue-se 1. de b) da descrição da técnica SH-SAS2. Chegando, desta forma à situação ilustrada na Figura 2.6.

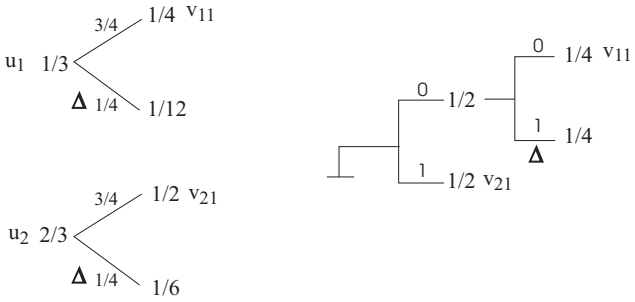


Figura 2.6: Técnica de substituição homofônica símbolo-a-símbolo 2 para a fonte U *com distribuição de probabilidade* $P_U(u_1) = 1/3$ *e* $P_U(u_2) = 2/3$*.*

Segundo a árvore na Figura 2.6 as palavras-código associadas aos homofonemas e ao símbolo mudo são $v_{11} \to 00$*,* $v_{21} \to 1$ *e* $\Delta \to 01$*.*

Como descrito em d) da descrição da técnica SH-SAS2 o experimento para a seleção do homofonema dado o símbolo u_i *da fonte é feito até que um homofonema* v_{ij} *seja selecionado. Desta forma, considerando este exemplo, os homofonemas correspondentes ao símbolo* u_1 *da fonte* U *são os elementos do subconjunto* $V_{11} = \{v_{11}, \Delta v_{11}, \Delta\Delta v_{11}, \dots\}$*, enquanto que os homofonemas correspondentes ao símbolo* u_2 *de* U *pertencem ao subconjunto* $V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, \dots\}$ *e portanto o código resultante para a fonte* V *é representado por* $\{(01)^i 1, (01)^i 00\}$*.*

Assim, o comprimento médio de tal código é dado por

$$E_{SAS2}(W) = \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+2r)\left(\frac{1}{4}\right)^r + \left(\frac{1}{2}\right)\sum_{r=0}^{\infty}(1+2r)\left(\frac{1}{4}\right)^r.$$

E, por conseqüência, dado que $H(U) = h(1/3) = 0,9183$*, a eficiência de tal técnica é*

$$\eta_{SAS2} = \frac{H(U)}{E_{SAS2}(W)} \Rightarrow \eta_{SAS2} = 0,4591.$$

Para fins de comparação, o mesmo problema é abordado tanto pela técnica JKM [6] quanto pela técnica RM [7].

- *JKM*

  Como visto no Exemplo 2 da seção 2.4.2 para essa fonte a eficiência é $\eta_{JKM} = 0,4591$.

- *RM*

  Pela técnica RM [7] é observado no mesmo exemplo (Exemplo 2) que o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/4$ *e a fonte* U *com probabilidade* $3/4$*, desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/4, 1/2, 1/4\}$ *(Figura 2.7), em que*
  $P_{\tilde{U}}(u_1) = \left(\frac{1}{3}\right)\left(\frac{3}{4}\right) = \frac{1}{4}, P_{\tilde{U}}(u_2) = \left(\frac{2}{3}\right)\left(\frac{3}{4}\right) = \frac{1}{2}$ *e* $P(\Delta) = \frac{1}{4}$ *tendo eficiência* $\eta_{RM} = 0,4591$.

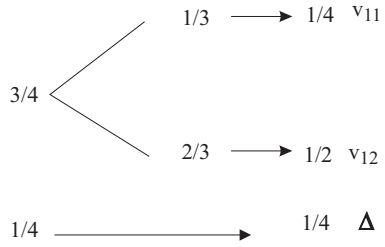


Figura 2.7: Técnica RM para a fonte U *com distribuição de probabilidade* $P_U(u_1) = 1/3$ *e* $P_U(u_2) = 2/3$.

Exemplo 6 *Considere uma fonte discreta binária sem memória com* $K = 2$*, obedecendo a seguinte distribuição de probabilidade* $P_U(u_1) = 1/5$ *e* $P_U(u_2) = 4/5$.

Segundo o passo b) da descrição da técnica SH-SAS2, $n = 5$ *e* $s = 4$*, portanto* $P(\Delta) = P(\Delta|u_i) = 1/16$.

Procedendo a decomposição das probabilidades dos símbolos da fonte, obtém-se:

$$P_U(u_1) = \frac{1}{5} = \frac{\left(\frac{1}{5}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\left(\frac{1}{8}\right) + \left(\frac{1}{16}\right)}{\left(\frac{15}{16}\right)} = \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

$$P_U(u_2) = \frac{4}{5} = \frac{\left(\frac{4}{5}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\left(\frac{1}{2}\right) + \left(\frac{1}{4}\right)}{\left(\frac{15}{16}\right)} = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Mais uma vez os símbolos possuem em suas expansões apenas termos periódicos, portanto por 1. de b) da descrição da técnica SH-SAS 2, chega-se à situação ilustrada na Figura 2.8.

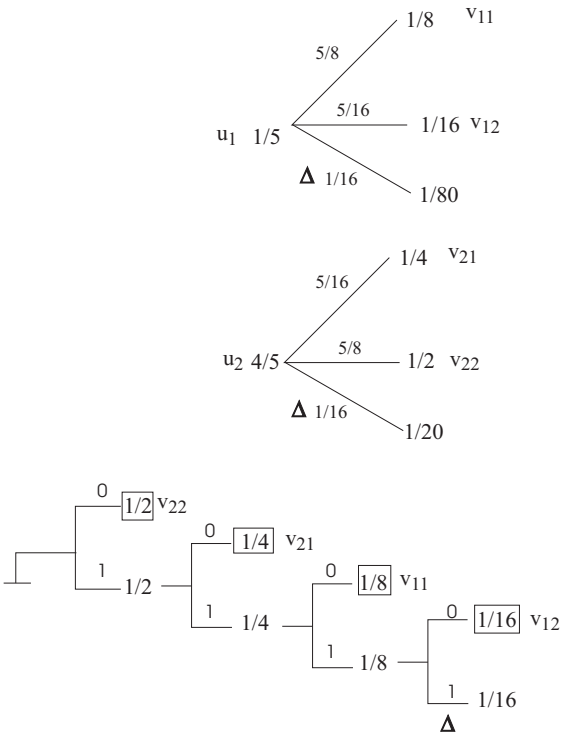


Figura 2.8: Técnica de substituição homofônica símbolo-a-símbolo 2 para a fonte U com distribuição de probabilidade $P_U(u_1) = 1/5$ e $P_U(u_2) = 4/5$.

Observe que segundo a árvore na Figura 2.8 as palavras-código associadas aos homofonemas e ao símbolo mudo são $v_{11} \to 110$, $v_{12} \to 1110$, $v_{21} \to 10$, $v_{22} \to 0$ e $\Delta \to 1111$.

Neste exemplo, os homofonemas correspondentes ao símbolo u_1 da fonte U são escolhidos dentre os elementos pertencentes aos subconjuntos $V_{11} = \{v_{11}, \Delta v_{11}, \Delta\Delta v_{11}, \dots\}$ e $V_{12} = \{v_{12}, \Delta v_{12}, \Delta\Delta v_{12}, \dots\}$ enquanto que os homofonemas correspondentes ao símbolo u_2 de U são escolhidos dentre os elementos pertencentes aos subconjuntos V_{21} e V_{22} com $V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, \dots\}$ e $V_{22} = \{v_{22}, \Delta v_{22}, \Delta\Delta v_{22}, \dots\}$.O código resultante para a fonte V é representado por $\{(1111)^i 110, (1111)^i 1110, (1111)^i 10, (1111)^i 0\}$.

Assim,

$$E_{SAS2}(W) = \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{16}\right)\sum_{r=0}^{\infty}(4+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{2}\right)\sum_{r=0}^{\infty}(1+4r)\left(\frac{1}{16}\right)^r = 2.$$

Por conseqüência, dado que $H(U) = h(1/5) = 0,7219$*, a eficiência de tal técnica é*

$$\eta_{SAS2} = \frac{H(U)}{E_{SAS2}(W)} \Rightarrow \eta_{SAS2} = 0,36095.$$

Abordando agora as técnicas JKM e RM para a mesma fonte.

- *JKM*

  Como,

  $P_U(u_1) = \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$

  $P_U(u_2) = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$

  Assim, o comprimento médio é dado por $E_{JKM}(W) = \sum_i P_U(u_i)l_i = 2$*, e portanto, a eficiência,*$\eta_{JKM} = \frac{H(U)}{E_{JKM}(W)} = \frac{0,7219}{2} \Rightarrow \eta_{JKM} = 0,36095.$

- *RM*

  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/16$ *e a fonte* U *com probabilidade* $15/16$*, desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/8, 1/16, 1/4, 1/2, 1/16\}$ *(Figura 2.9).*

  Assim, o comprimento médio é dado por,

  $$E_{RM}(W) = \left(\frac{1}{2}\right)\cdot 1 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{16}\right)\cdot 4 + \left(\frac{1}{16}\right)\cdot 4 = 1,875.$$

  sendo a eficiência dada por,

  $\eta_{RM} = \frac{(1-P(\Delta))H(U)}{E_{RM}(W)} = \frac{\left(\frac{15}{16}\right)0,7219}{1,875} \Rightarrow \eta_{RM} = 0,36095.$

Exemplo 7 *Considere uma fonte discreta binária sem memória com* $K = 2$*, obedecendo a seguinte distribuição de probabilidade* $P_U(u_1) = 7/10$ *e* $P_U(u_2) = 3/10$.

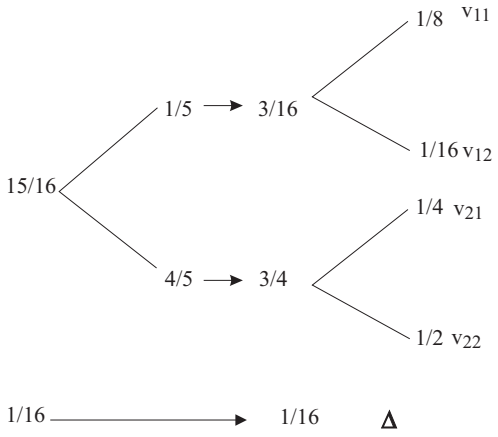


Figura 2.9: Técnica RM para a fonte U com distribuição de probabilidade $P_U(u_1) = 1/5$ *e* $P_U(u_2) = 4/5$.

Segundo o passo b) da descrição da técnica SH-SAS 2, $n = 10 = 2 \cdot 5$*, logo,* $n \acute{} = 5$ *e* $s = 4$*, portanto* $P(\Delta) = P(\Delta|u_i) = 1/16$.

Do Exemplo 4,

$$P_U(u_1) = \frac{7}{10} = \frac{1}{2} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

$$P_U(u_2) = \frac{3}{10} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i$$

Nota-se, portanto, que a decomposição de $P_U(u_i) = 7/10$ *apresenta um termo não-periódico, assim considerando o procedimento em 2. de b) da descrição da técnica SH-SAS2 chega-se ao resultado ilustrado na Figura 2.10. Segundo a árvore obtida chega-se as palavras-código associadas aos homofonemas e ao símbolo mudo são* $v_{11} \rightarrow 0$*,* $v_{12} \rightarrow 1110$*,* $v_{13} \rightarrow 110$*,* $v_{21} \rightarrow 10$*,* $v_{22} \rightarrow 11110$ *e* $\Delta \rightarrow 1111$.

Neste exemplo, os homofonemas correspondentes ao símbolo u_1 *da fonte U são escolhidos dentre os elementos pertencentes aos subconjuntos* V_{11}*,* V_{12} *e* V_{13} *sendo* $V_{11} = \{v_{11}\}$** *,* $V_{12} = \{v_{12}, \Delta v_{12}, \Delta\Delta v_{12}, \dots\}$ *e* $V_{13} = \{v_{13}, \Delta v_{13}, \Delta\Delta v_{13}, \dots\}$*, enquanto que os homofonemas correspondentes ao símbolo* u_2 *de U são escolhidos dentre os elementos pertencentes aos subconjuntos* V_{21} *e* V_{22} *sendo* $V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, \dots\}$ *e* $V_{22} = \{v_{22}, \Delta v_{22}, \Delta\Delta v_{22}, \dots\}$. *O código resultante para a fonte V é representado por* $\{0, (1111)^i 1110, (1111)^i 110, (1111)^i 10, (1111)^i 11110\}$.

**Este homofonema está associado ao termo não-periódico, portanto nunca ocorrerá a escolha de um símbolo mudo antes dele.

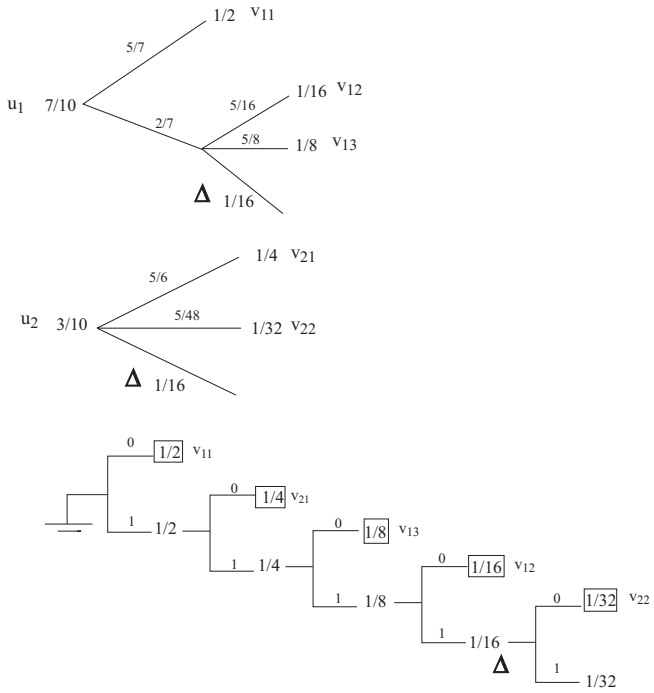


Figura 2.10: Técnica de substituição homofônica símbolo-a-símbolo 2 para a fonte U com distribuição de probabilidade $P_U(u_1) = 7/10$ e $P_U(u_2) = 3/10$.

Assim, o comprimento médio é dado por,

$$E_{SAS2}(W) = \left(\frac{1}{2}\right)\cdot 1 + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{16}\right)\sum_{r=0}^{\infty}(4+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r = 2.$$

Por conseqüência, dado que $H(U) = h(3/10) = 0,8813$, a eficiência de tal técnica é

$$\eta_{SAS2} = \frac{H(U)}{E_{SAS2}(W)} \Rightarrow \eta_{SAS2} = 0,4407.$$

Abordando as técnicas JKM e RM para a mesma fonte.

- *JKM*

  Como,

  $$P_U(u_1) = \frac{7}{10} = \frac{1}{2} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

  $$P_U(u_2) = \frac{3}{10} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Logo, o comprimento médio é dado por $E_{JKM}(W) = \sum_i P_U(u_i)l_i = 2$, *e portanto, a eficiência,* $\eta_{JKM} = \dfrac{H(U)}{E_{JKM}(W)} = \dfrac{0,8813}{2} \Rightarrow \eta_{JKM} = 0,4407.$

- *RM*

  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/16$ *e a fonte* U *com probabilidade* $15/16$, *desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/2, 1/8, 1/32, 1/4, 1/32, 1/16\}$ *(Figura 2.11).*

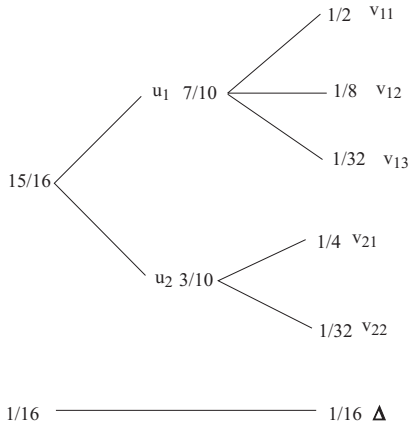


Figura 2.11: Técnica RM para a fonte U *com distribuição de probabilidade* $P_U(u_1) = 7/10$ *e* $P_U(u_2) = 3/10$.

Assim, o comprimento médio é dado por

$$E_{RM}(W) = \left(\frac{1}{2}\right)\cdot 1 + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{16}\right)\cdot 4 = 1,9375,$$

sendo a eficiência dada por $\eta_{RM} = \dfrac{(1 - P(\Delta))H(U)}{E_{RM}(W)} = \dfrac{\left(\frac{15}{16}\right)0,8813}{1,9375} \Rightarrow \eta_{RM} = 0,4264.$

Exemplo 8 *Considere uma fonte discreta binária sem memória com* $K = 3$, *obedecendo à seguinte distribuição de probabilidade* $P_U(u_1) = 1/4$, $P_U(u_2) = 1/3$ *e* $P_U(u_3) = 5/12$.

Nota-se que nesta fonte o primeiro elemento é da forma 2^{-l_i}, *portanto segundo o passo a) da descrição da técnica SH-SAS2 será associado ao homofonema o termo* $1/4$,*i.e.,* $P(v_{11}) = 1/4$ *e o símbolo* Δ *não será necessário para este termo. Caso o símbolo* u_1 *seja emitido pela fonte o homofonema selecionado será* v_{11} *com probabilidade* $P(v_{11}|u_1) = 1$, *o que está ilustrado na Figura 2.12.*

Para os símbolos restantes da fonte U observa-se que $n = 3$*, logo segundo o passo b) da descrição da técnica SH-SAS2,* $n = 3$ *e* $s = 2$*, portanto* $P(\Delta) = P(\Delta|u_i) = 1/4$.

Do Exemplo 2,

$$P_U(u_2) = \frac{1}{3} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

Procedendo a decomposição da probabilidade do terceiro elemento da fonte u_3*,*

$$P_U(u_3) = \frac{5}{12} = \left(\frac{1}{4}\right)\left(\frac{5}{3}\right) = \left(\frac{1}{4}\right)\left[1+\frac{2}{3}\right] = \frac{1}{4} + \left(\frac{1}{4}\right)\left(\frac{2}{3}\right). \tag{2.33}$$

Do Exemplo 2,

$$\frac{2}{3} = \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i. \tag{2.34}$$

Assim,de (2.34) em (2.33),

$$P_U(u_3) = \frac{5}{12} = \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

Como a expansão de $P_U(u_3) = 5/12$ *apresenta um termo não-periódico, novamente o procedimento descrito em 2. de b) da descrição da técnica SH-SAS 2 é seguido.*

Segundo a árvore ilustrada na Figura 2.12 as palavras-código associadas aos homofonemas e ao símbolo mudo são $v_{11} \rightarrow 00$*,* $v_{21} \rightarrow 01$*,* $v_{31} \rightarrow 10$*,* $v_{32} \rightarrow 110$ *e* $\Delta \rightarrow 11$.

Neste exemplo, os homofonemas correspondentes ao símbolo u_2 *da fonte U são escolhidos dentre os elementos pertencentes ao subconjunto* $V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, \dots\}$*, para o símbolo* u_3 *os homofonemas são selecionados dentre os elementos pertencentes aos subconjuntos* $V_{31} = \{v_{31}\}$ *e* $V_{32} = \{v_{32}, \Delta v_{32}, \Delta\Delta v_{32}, \dots\}$*. O código resultante para a fonte V é representado por* $\{00, (11)^i01, 10, (11)^i110\}$.

Desta forma o comprimento médio é dado por,

$$\begin{aligned} E_{SAS2}(W) = \; & \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+2r)\left(\frac{1}{4}\right)^r + \left(\frac{1}{4}\right)\cdot 2 \\ & + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+2r)\left(\frac{1}{4}\right)^r = 2,5. \end{aligned}$$

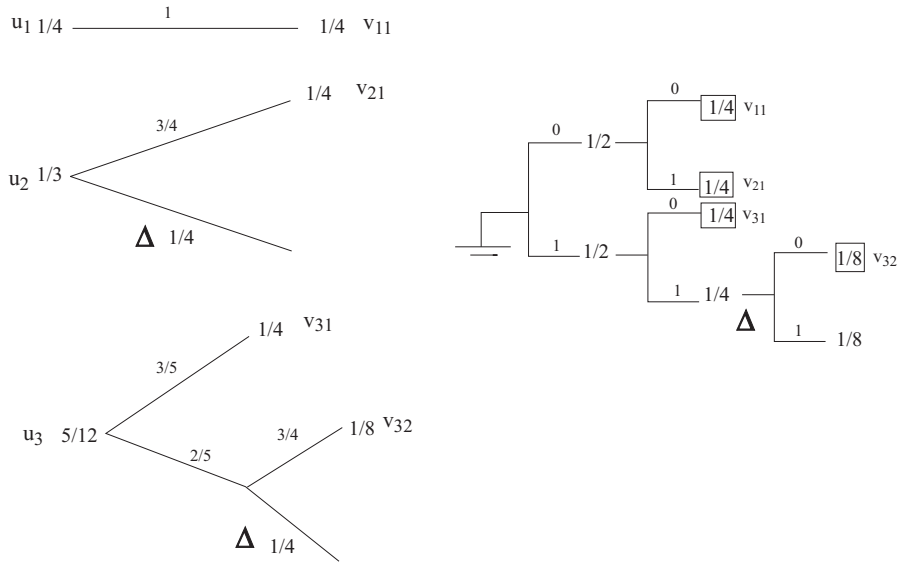


Figura 2.12: Técnica de substituição homofônica símbolo-a-símbolo 2 para a fonte U com distribuição de probabilidade $P_U(u_1) = 1/4$, $P_U(u_2) = 1/3$ e $P_U(u_3) = 5/12$.

Por conseqüência, dado que $H(U) = \left(\frac{1}{4}\right)\log 4 + \left(\frac{1}{3}\right)\log 3 + \left(\frac{5}{12}\right)\log\left(\frac{12}{5}\right) = 1,5546$, *a eficiência de tal técnica é*

$$\eta_{SAS2} = \frac{H(U)}{E_{SAS2}(W)} \Rightarrow \eta_{SAS2} = 0,6218.$$

Abordando agora as técnicas JKM e RM para a mesma fonte.

- *JKM*

  Como,

  $P_U(u_2) = \frac{1}{3} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i$.

  e

  $P_U(u_3) = \frac{5}{12} = \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i$.

  Assim, o comprimento médio é dado por $E_{JKM}(W) = \sum_i P_U(u_i)l_i = 2,5$, *e portanto, a eficiência,* $\eta_{JKM} = \frac{H(U)}{E(W)} = \frac{1,5546}{2,5} \Rightarrow \eta_{JKM} = 0,6218$.

- *RM*

  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/4$ *e a fonte* U *com probabilidade* $3/4$, *desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/8, 1/16, 1/4, 1/4, 1/16, 1/4\}$ *(Figura 2.13).*

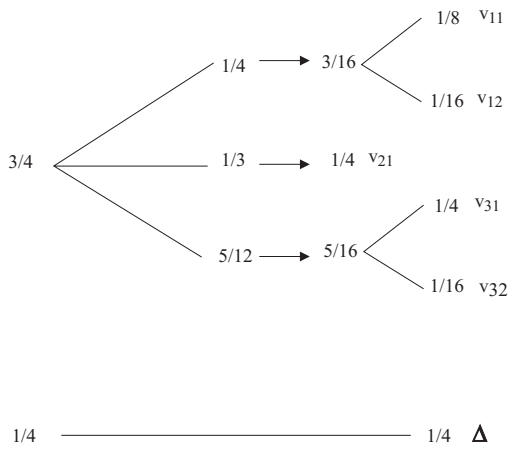


Figura 2.13: Técnica Rocha-Massey para a fonte U com distribuição de probabilidade $P_U(u_1) = 1/4$, $P_U(u_2) = 1/3$ *e* $P_U(u_3) = 5/12$.

Assim, o comprimento médio é dado por

$$E_{RM}(W) = \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{16}\right)\cdot 4 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{16}\right)\cdot 4 + \left(\frac{1}{4}\right)\cdot 2 = 2,375.$$

sendo a eficiência dada por $\eta_{RM} = \dfrac{(1-P(\Delta))H(U)}{E_{RM}(W)} = \dfrac{\left(\frac{3}{4}\right)1,5446}{2,375} \Rightarrow \eta_{RM} = 0,4909.$

Note que a eficiência obtida ao se utilizar a técnica RM é, para a fonte considerada neste exemplo, cerca de 21% *menor que a eficiência alcançada ao se utilizar a técnica JKM ou a técnica SH-SAS 2.*

Exemplo 9 *Considere uma fonte discreta binária sem memória com* $K = 3$ *e obedecendo a seguinte distribuição de probabilidade* $P_U(u_1) = 3/8$, $P_U(u_2) = 1/12$ *e* $P_U(u_3) = 13/24$.

Nota-se que nesta fonte o primeiro elemento tem probabilidade $3/8$, *sendo portanto da forma* $m_i/2^{l_i}$, *podendo ser decomposto em* $1/4+1/8$, *assim dado que o símbolo* u_1 *da fonte U é emitido, o homofonema* v_{11} *é selecionado com probabilidade* $P(v_{11}|u_1) = 2/3$ *tendo portanto probabilidade* $P(v_{11}) = 1/4$, *enquanto que o homofonema* v_{12} *é selecionado com probabilidade* $P(v_{12}|u_1) = 1/3$ *tendo probabilidade* $P(v_{12}) = 1/8$, *o que está ilustrado na Figura 2.14.*

Para os símbolos restantes da fonte U observa-se que $n = 12 = 4 \cdot 3$, *logo segundo o passo b) da descrição da técnica SH-SAS 2,* $n \acute{} = 3$ *e* $s = 2$, *portanto* $P(\Delta) = P(\Delta|u_i) = 1/4$.

Procedendo a expansão das probabilidades dos símbolos u_2 *e* u_3,

$$P_U(u_2) = \frac{1}{12} = \left(\frac{1}{4}\right)\left(\frac{1}{3}\right). \tag{2.35}$$

Do Exemplo 2,

$$\frac{1}{3} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i. \tag{2.36}$$

Assim, de (2.36) em (2.35),

$$P_U(u_2) = \frac{1}{12} = \left(\frac{1}{16}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

$$P_U(u_3) = \frac{13}{24} = \left(\frac{1}{8}\right)\left(\frac{13}{3}\right) = \left(\frac{1}{8}\right)\left[1 + \frac{10}{3}\right] = \frac{1}{8} + \frac{5}{12}. \tag{2.37}$$

Do Exemplo 8,

$$\frac{5}{12} = \left(\frac{1}{4}\right) + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i. \tag{2.38}$$

Assim, de (2.38) em (2.37),

$$P_U(u_3) = \frac{13}{24} = \frac{1}{8} + \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

$P_U(u_3)$ possui dois termos não-periódicos na sua decomposição, e portanto o procedimento descrito no item 2. de b) da descrição da técnica SH-SAS2 é seguido.

Segundo a árvore ilustrada na Figura 2.14 as palavras-código associadas aos homofonemas e ao símbolo mudo são $v_{11} \rightarrow 00$, $v_{12} \rightarrow 100$, $v_{21} \rightarrow 1110$, $v_{31} \rightarrow 01$, $v_{32} \rightarrow 101$, $v_{33} \rightarrow 110$ e $\Delta \rightarrow 10$.

Neste exemplo, os homofonemas correspondentes ao símbolo u_1 são escolhidos entre os conjuntos $V_{11} = \{v_{11}\}$ e $V_{12} = \{v_{12}\}$. Já o símbolo u_2 tem seus homofonemas selecionados dentre os elementos pertencentes ao subconjunto $V_{21} = \{v_{21}, \Delta v_{21}, \Delta\Delta v_{21}, \dots\}$, para o símbolo u_3 os homofonemas são selecionados dentre os elementos pertencentes aos subconjuntos $V_{31} = \{v_{31}\}$, $V_{32} = \{v_{32}\}$ e $V_{33} = \{v_{33}, \Delta v_{33}, \Delta\Delta v_{33}, \dots\}$. O código resultante para a fonte V é representado por $\{00, 100, (10)^i 1110, 01, 101, (10)^i 110\}$.

Assim,

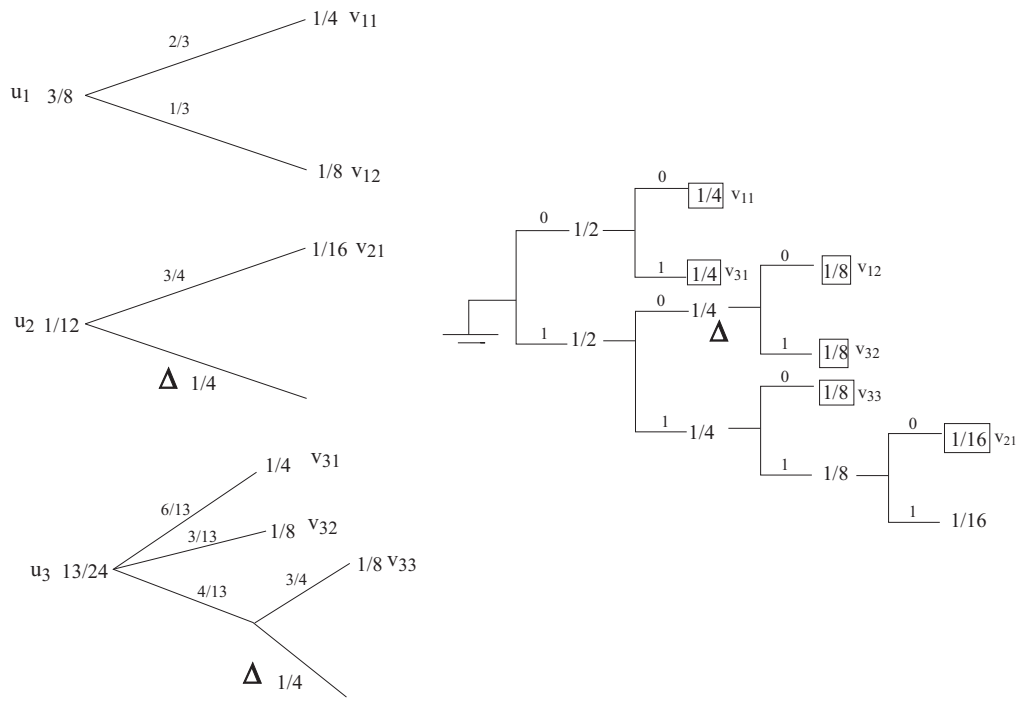


Figura 2.14: Técnica de substituição homofônica símbolo-a-símbolo 2 para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/8$, $P_U(u_2) = 1/12$ e $P_U(u_3) = 13/24$.

$$\begin{aligned} E_{SAS2}(W) = & \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{16}\right)\sum_{r=0}^{\infty}(4+2r)\left(\frac{1}{4}\right)^r + \left(\frac{1}{4}\right)\cdot 2 \\ & + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+2r)\left(\frac{1}{4}\right)^r \\ & = 2,75. \end{aligned}$$

Por conseqüência, dado que $H(U) = \left(\frac{3}{8}\right)\log\left(\frac{8}{3}\right) + \left(\frac{1}{12}\right)\log(12) + \left(\frac{13}{24}\right)\log\left(\frac{24}{13}\right) = 1,3085$*, a eficiência de tal técnica é*

$$\eta_{SAS2} = \frac{H(U)}{E_{SAS2}(W)} \Rightarrow \eta_{SAS2} = 0,4758.$$

Abordando as técnicas JKM e RM para a mesma fonte.

- *JKM*

  Como,

  $P_U(u_1) = \dfrac{3}{8} = \dfrac{1}{4} + \dfrac{1}{8}.$

  $P_U(u_2) = \dfrac{1}{12} = \left(\dfrac{1}{16}\right)\displaystyle\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$

$P_U(u_3) = \dfrac{13}{24} = \dfrac{1}{8} + \dfrac{1}{4} + \left(\dfrac{1}{8}\right)\sum_{i=0}^{\infty}\left(\dfrac{1}{4}\right)^i$.

Assim, o comprimento médio é dado por $E_{JKM}(W) = \sum_i P_U(u_i)l_i = 2,75$ *e, portanto, a eficiência,* $\eta_{JKM} = \dfrac{H(U)}{E_{JKM}(W)} = \dfrac{1,3085}{2,75} \Rightarrow \eta_{JKM} = 0,4758$.

- *RM*

  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/4$ *e a fonte* U *com probabilidade* $3/4$*, desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/4, 1/32, 1/16, 1/4, 1/8, 1/32, 1/4\}$ *(Figura 2.15).*

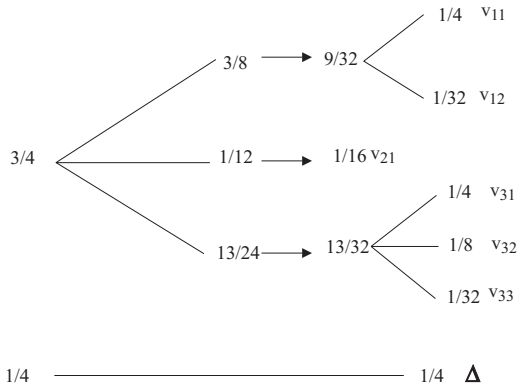


Figura 2.15: Técnica RM para a fonte U *com distribuição de probabilidade* $P_U(u_1) = 3/8$, $P_U(u_2) = 1/12$ *e* $P_U(u_3) = 13/24$.

Assim, o comprimento médio é dado por

$$E_{RM}(W) = \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{16}\right)\cdot 4 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{4}\right)\cdot 2 = 2,4375$$

sendo a eficiência dada por $\eta_{RM} = \dfrac{(1 - P(\Delta))H(U)}{E_{RM}(W)} = \dfrac{\left(\frac{3}{4}\right)1,3085}{2,4375} \Rightarrow \eta_{RM} = 0,4026$.

Mais uma vez a técnica RM mostrou um desempenho inferior se comparado às outras duas técnicas que apresentaram uma eficiência cerca de 15% *superior a eficiência obtida pela técnica RM para esta fonte.*

Exemplo 10 *Considere uma fonte discreta binária sem memória com* $K = 3$ *e obedecendo à seguinte distribuição de probabilidade* $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ *e* $P_U(u_3) = 17/60$.

Segundo o passo b) da descrição da técnica SH-SAS 2, $n = 10 = 2\cdot 5$*, logo,* $n \acute{} = 5$ *e* $s = 4$*, portanto* $P(\Delta) = P(\Delta|u_i) = 1/16$.

Do Exemplo 7,

$$P_U(u_1) = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Do Exemplo 8,

$$P_U(u_2) = \frac{5}{12} = \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

Utilizando a técnica em [14] a fim de decompor $P_U(u_3)$, tem-se

$$P_U(u_3) = \frac{17}{60} = \left(\frac{1}{4}\right)\left(\frac{17}{15}\right) = \left(\frac{1}{4}\right)\left[1 + \frac{2}{15}\right] = \frac{1}{4} + \frac{1}{30}. \tag{2.39}$$

Por outro lado,

$$\left(\frac{1}{30}\right) = \frac{\left(\frac{1}{30}\right)\left(\frac{15}{16}\right)}{\left(\frac{15}{16}\right)} = \frac{\frac{1}{32}}{\frac{15}{16}} = \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i. \tag{2.40}$$

Assim, com (2.40) em (2.39),

$$P_U(u_3) = \frac{17}{60} = \left(\frac{1}{4}\right) + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

Como a expansão de $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$ apresentam termos não-periódicos, o procedimento descrito em 2. de b) da descrição da técnica SH-SAS 2 é seguido.

Observe pela Figura 2.16 que a probabilidade $P_U(u_2)$ foi tratada de forma um pouco distinta daquela do Exemplo 8 uma vez que se optou pela utilização de um único Δ.

Considerando a situação ilustrada na Figura 2.16, nota-se que o símbolo u_1 tem seus homofonemas nos subconjuntos $V_{11} = \{v_{11}, \Delta v_{11}, \Delta\Delta v_{11}, \dots\}$ e $V_{12} = \{v_{12}, \Delta v_{12}, \Delta\Delta v_{12}, \dots\}$, u_2 nos subconjuntos $V_{21} = \{v_{21}\}$, $V_{22} = \{v_{22}, \Delta v_{22}, \Delta\Delta v_{22}, \dots\}$ e $V_{23} = \{v_{23}, \Delta v_{23}, \Delta\Delta v_{23}, \dots\}$, e u_3 nos subconjuntos, $V_{31} = \{v_{31}\}$, $V_{32} = \{v_{32}, \Delta v_{32}, \Delta\Delta v_{32}, \dots\}$ onde $v_{11} \rightarrow 00, v_{12} \rightarrow 11100, v_{21} \rightarrow 01, v_{22} \rightarrow 110, v_{23} \rightarrow 11101, v_{31} \rightarrow 10, v_{32} \rightarrow 11110$ e $\Delta \rightarrow 1111$. Logo, o código resultante para a fonte V é representado por $\{(1111)^i 00, (1111)^i 11100, 01, (1111)^i 110, (1111)^i 11101, 10, (1111)^i 11110\}$ e o comprimento médio,

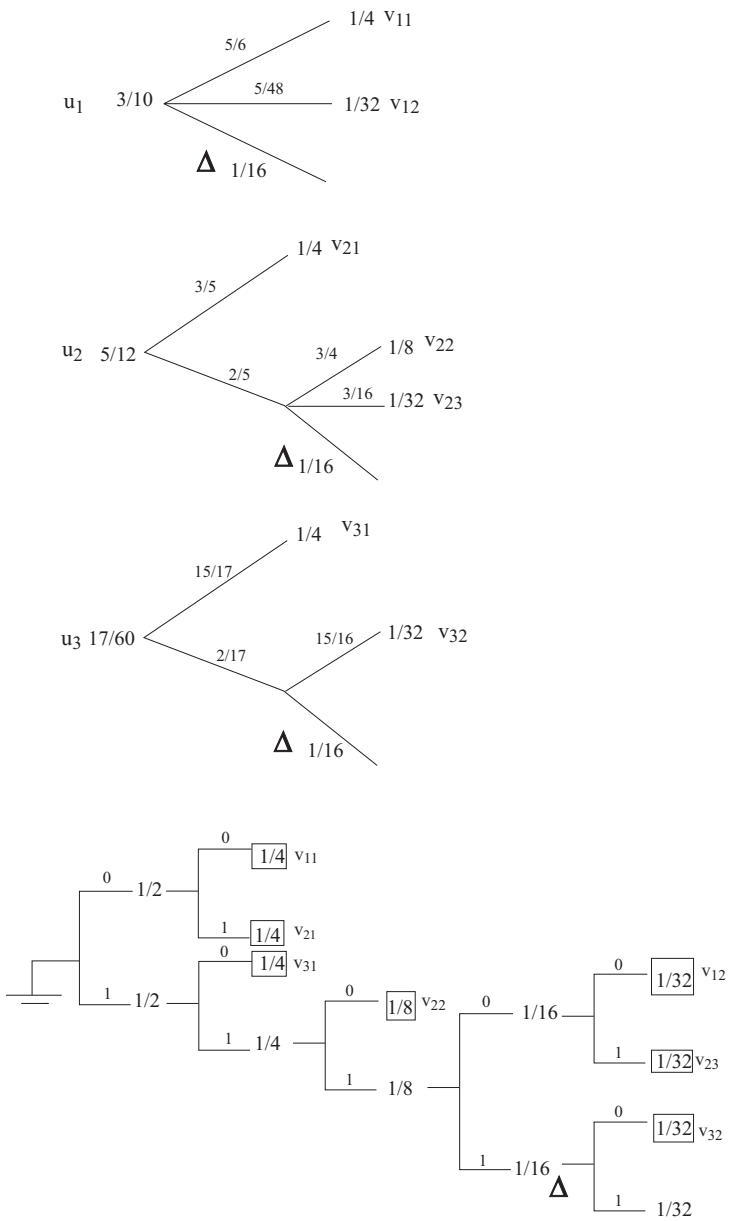


Figura 2.16: Nova técnica de substituição homofônica símbolo-a-símbolo para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$.

$$
\begin{aligned}
E_{SAS2}(W) = \; & \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\
& + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+4r)\left(\frac{1}{16}\right)^r + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\
& + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r = 2,5667.
\end{aligned}
$$

Como, $H(U) = \frac{3}{10}\log\frac{10}{3} + \frac{5}{12}\log\frac{12}{5} + \frac{17}{60}\log\frac{60}{17} = 1,5629$*, então* $\eta_{SAS2} = 0,6089$.

- *JKM*

  Como,

  $$P_U(u_1) = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

  $$P_U(u_2) = \frac{5}{12} = \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i.$$

  $$P_U(u_3) = \frac{17}{60} = \left(\frac{1}{4}\right) + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i.$$

  Assim, o comprimento médio é dado por $E_{JKM}(W) = \sum_i P_U(u_i)l_i = 2,5667$*, e portanto, a eficiência,* $\eta_{JKM} = \frac{H(U)}{E_{JKM}(W)} = \frac{1,5629}{2,5667} \Rightarrow \eta_{JKM} = 0,6089$.

- *RM*

  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/16$ *e a fonte* U *com probabilidade* $15/16$*, desta forma a fonte expandida tem distribuição de probabilidade dada por* $\{1/4, 1/32, 1/4, 1/8, 1/64, 1/4, 1/64, 1/16\}$ *(Figura 2.15).*

  Assim, o comprimento médio é dado por

  $$\begin{aligned} E_{RM}(W) = \; & \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\cdot 3 \\ & + \left(\frac{1}{64}\right)\cdot 6 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{64}\right)\cdot 6 + \left(\frac{1}{16}\right)\cdot 4 = 2,4688, \end{aligned}$$

  sendo a eficiência dada por $\eta_{RM} = \frac{(1 - P(\Delta))H(U)}{E_{RM}(W)} = \frac{\left(\frac{15}{16}\right)1,5629}{2,4688} \Rightarrow \eta_{RM} = 0,5935$.

2.5.2 Análise da técnica

Da Tabela 2.1 é possível perceber que em todos os exemplos a eficiência da técnica SH-SAS 2 foi a mesma obtida pela técnica JKM modificada, em específico naqueles em que as decomposições dos símbolos da fonte apresentaram mesma razão, as probabilidades dos homofonemas e do símbolo mudo coincidiram, e por ambas as técnicas construírem cada palavra-código homofônica como a concatenação de palavras-código mais curtas derivadas a partir das probabilidades da fonte, nestes casos, as técnicas JKM modificada e SH-SAS 2 apresentam mesmo resultado.

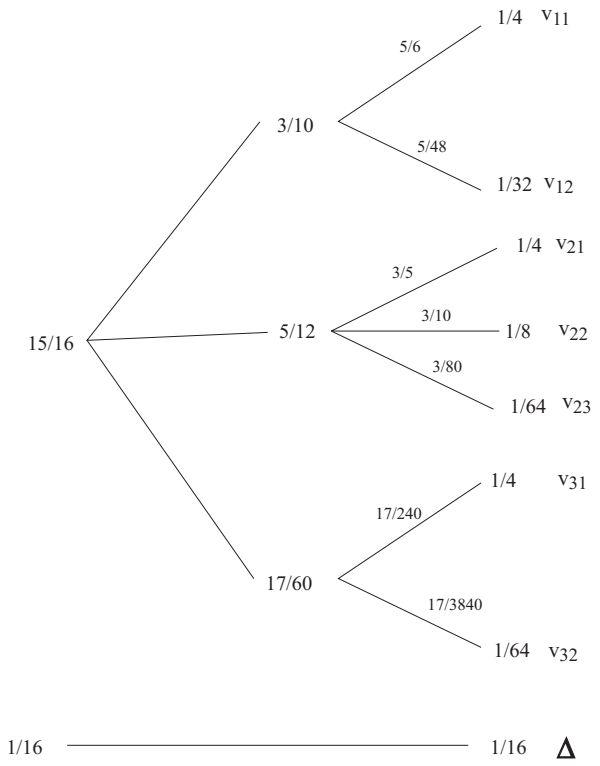


Figura 2.17: Técnica RM para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$.

Tabela 2.1: Comparativo, em termos de eficiência, dos Exemplos da seção 2.5.1 utilizando os valores de η.

Exemplos	JKM	RM	SH-SAS2
Exemplo 5	$\eta_{JKM} = 0,4591$	$\eta_{RM} = 0,4591$	$\eta_{SAS2} = 0,4591$
Exemplo 6	$\eta_{JKM} = 0,36095$	$\eta_{RM} = 0,36095$	$\eta_{SAS2} = 0,36095$
Exemplo 7	$\eta_{JKM} = 0,4407$	$\eta_{RM} = 0,4264$	$\eta_{SAS2} = 0,4407$
Exemplo 8	$\eta_{JKM} = 0,6218$	$\eta_{RM} = 0,4909$	$\eta_{SAS2} = 0,6218$
Exemplo 9	$\eta_{JKM} = 0,4758$	$\eta_{RM} = 0,4026$	$\eta_{SAS2} = 0,4758$
Exemplo 10	$\eta_{JKM} = 0,6089$	$\eta_{RM} = 0,5934$	$\eta_{SAS2} = 0,6089$

Como foi visto na seção 2.4.3, na técnica JKM modificada a probabilidade do símbolo mudo é dada pela razão da decomposição da probabilidade do símbolo da fonte, e, portanto, caso haja razões distintas haverá símbolos mudos distintos. Por exemplo, utilizando a técnica JKM modificada na fonte do Exemplo 2.16, os símbolos u_1 e u_3 utilizariam um Δ_1 com probabilidade $P(\Delta_1) = 1/16$, enquanto que o símbolo u_2 faria uso de um Δ_2 com probabilidade $P(\Delta_2) = 1/4$. Ao utilizar a técnica SH-SAS2 é possível utilizar apenas um símbolo

mudo, tendo, portanto uma única palavra-código a ser detectada e apagada no momento da decodificação. Note que, como ilustrado, no Exemplo 2.16 o comprimento médio, e, portanto a eficiência para as técnicas JKM e SH-SAS2 foram os mesmos.

Ao se comparar com a técnica RM percebe-se pela Tabela 2.1 que nos Exemplos 5 e 6 a eficiência foi a mesma para as três técnicas. Para esses exemplos as decomposições das probabilidades dos símbolos da fonte apresentaram apenas termos periódicos. Nos outros exemplos, a técnica RM apresentou desempenho inferior, considerando como parâmetro a eficiência. Nesses casos as decomposições das probabilidades dos símbolos da fonte apresentam termos não-periódicos.

capítulo 3

Substituição Homofônica com Restrição

3.1 Introdução

Neste capítulo é dada continuidade ao estudo das técnicas de substituição (codificação) homofônica, porém abordando as técnicas de **codificação homofônica com restrição** uma vez que as técnicas de substituição homofônica padrão já foram abordadas no capítulo anterior. Diferentemente das técnicas abordadas no Capitulo 2 nas técnicas de codificação homofônica com restrição os símbolos que constituem as palavras-código dos homofonemas obedecem a uma distribuição de probabilidade arbitrária, i.e., não necessariamente uniforme, como é o caso das técnicas de codificação homofônica padrão.

A seção 3.2 trata de algumas técnicas de codificação homofônica com restrição denominadas MAX-ENT por passo [16] e MIN-ENT por passo [17], na seção seguinte (seção 3.3) é introduzida de uma nova técnica denominada substituição homofônica com restrição símbolo-a-símbolo (SHR-SAS) [18].

Finalizando o capítulo é mostrado como as técnicas de codificação homofônica MAX-ENT por passo [16] e MIN-ENT por passo [17] podem ser usadas na geração de dados honestos com o lançamento de duas ou mais moedas desbalanceadas obtendo desta forma resultados equivalentes ou melhores que as técnicas conhecidas no momento.

3.2 Algumas técnicas de substituição homofônica com restrição

A **codificação (substituição) homofônica com restrição** é uma técnica de codificação na qual os símbolos que constituem as palavras-código dos homofonemas obedecem a uma distribuição de probabilidade arbitrária, i.e., não necessariamente uniforme como no caso da substituição homofônica tradicional mostrada no Capítulo 2, sendo, portanto, uma generalização dela. Tal técnica acha aplicação em casos em que o custo de armazenamento e transmissão de 0's e 1's é distinto.

A codificação homofônica D-ária padrão é caracterizada pelo fato de ser feita em dois passos [6]. No primeiro passo cada probabilidade da fonte é individualmente decomposta como uma soma finita ou infinita de potências negativas de D. Os termos dessa decomposição constituem as probabilidades dos homofonemas. No segundo passo um código livre de prefixo é construído a partir das probabilidades dos homofonemas a fim de produzir um código unicamente decodificável.

Na codificação homofônica D-ária padrão o projetista se beneficia do fato que uma dada probabilidade de um símbolo da fonte $P_U(u_i),\ 0 < P_U(u_i) < 1$, tem essencialmente uma única decomposição na base D. Isto ocorre, pois $P_U(u_i)$ ou tem uma única decomposição como um somatório com infinitas potências negativas de D ou possui uma decomposição com um número finito de potências negativas de D juntamente com uma única decomposição na forma de somatório formado por um número infinito de potências negativas de D, nela a menor potência de D da decomposição com número finito de termos é substituída por uma soma com infinitas potências negativas sucessivas de D. Por exemplo, para $D = 3$, $P_U(u_i) = 4/9$ pode ser decomposto tanto como $P_U(u_i) = 1/3 + 1/9$ como $P_U(u_i) = 1/3 + (1/27)\sum_{i=0}^{\infty}(2/3)^i$.

A codificação homofônica com restrição, infelizmente, não herda a propriedade de única decomposição mencionada há pouco, o que significa que a fim de decompor os símbolos da fonte em homofonemas é necessário trabalhar com todo o conjunto de probabilidades dos símbolos da fonte, em vez de trabalhar apenas com a probabilidade de um símbolo por vez a fim de fazer a decomposição do símbolo em homofonemas. Esta situação foi tratada pelos algoritmos **MAX-ENT por passo** [16] e **MIN-ENT por passo** [17] os quais serão explicados nas seções 3.2.1 e 3.2.2, respectivamente.

No Capítulo 2 a técnica de substituição (codificação) homofônica padrão foi definida como **perfeita** (Definição 1) se os símbolos D-ários que formam qualquer palavra-código de homofonema são variáveis aleatórias estatisticamente independentes, distribuídas de acordo com uma

distribuição de probabilidade uniforme. Desta forma, o conceito de codificação homofônica com restrição perfeita é introduzido na definição a seguir.

Definição 5 *Uma codificação homofônica com restrição é dita perfeita se os símbolos D-ários que formam o homofonema, $X_1, X_2, \ldots, X_W$ são variáveis aleatórias independentes e identicamente distribuídas (i.i.d). Em particular, se além de i.i.d essas variáveis aleatórias são distribuídas de acordo com uma distribuição de probabilidade uniforme então a técnica é simplesmente chamada codificação homofônica perfeita.*

Da mesma forma, levando em consideração o que foi exposto no Capítulo 2 a definição de codificação homofônica **ótima** (Definição 4) é estendida para o caso da codificação homofônica com restrição. Assim,

Definição 6 *Define-se uma codificação homofônica com restrição como ótima, se ela é perfeita e, além disso, sua redundância é a menor possível. Em particular, se essas variáveis aleatórias forem distribuídas de acordo com uma distribuição de probabilidade uniforme, então a técnica é simplesmente denominada codificação homofônica ótima.*

Nas próximas seções (3.2.1 e 3.2.2) duas técnicas de codificação homofônica serão introduzidas. Ambas as técnicas fazem a expansão de um conjunto de símbolos da fonte em um conjunto de homofonemas por meio de passos e a cada passo um novo homofonema é gerado.

3.2.1 MAX-ENT por passo

A técnica de substituição homofônica com restrição abordada nesta seção foi introduzida em 2001 pelos professores Valdemar C. da Rocha Jr. e Cecílio Pimentel em [16]. Nessa técnica os símbolos de cada palavra-código de homofonema são variáveis aleatórias independentes e identicamente distribuídas obedecendo a uma distribuição de probabilidade arbitrária.

A expansão dos símbolos da fonte em homofonemas nessa técnica é feita de modo a maximizar a entropia do conjunto de homofonemas a cada passo por meio da escolha de um elemento que cause maior incremento na entropia, sendo por esta razão denominada MAX-ENT por passo [16].

A descrição detalhada do algoritmo é fornecida no Apêndice C.

3.2.2 MIN-ENT por passo

Esta seção é iniciada com um exemplo que ilustra que em algumas situações é possível obter resultados melhores do que aplicando a técnica MAX-ENT por passo, tendo sido esta a maior motivação para buscar a melhoria do desempenho deste algoritmo [16], o que resultou no algoritmo MIN-ENT por passo [17], o qual é descrito em detalhes no Apêndice D.

Neste algoritmo a expansão dos símbolos do alfabeto em homofonemas é feita de modo a minimizar a entropia do conjunto de homofonemas a cada passo, daí seu nome.

Exemplo 11 *Seja uma fonte discreta binária sem memória com* $P_U(u_1) = 5/9$ *e* $P_U(u_2) = 4/9$. *Considere a substituição homofônica binária perfeita aplicada a* U *quando* $\Pi_2 = \{2/3, 1/3\}$ *para a distribuição de probabilidade dos símbolos das palavras-código dos homofonemas. Aplicando o algoritmo MAX-ENT por passo [16](vide Apêndice C), obtém-se*

$$P_U(u_1) = \frac{4}{9} + \sum_{i=0}^{\infty} \left(\frac{8}{3^{4+2i}} \right)$$

$$P_U(u_2) = \frac{1}{3} + \frac{2}{27} + \sum_{i=0}^{\infty} \left(\frac{8}{3^{5+2i}} \right)$$

que produz um comprimento médio $E_{MAX}(W) = 19/9 = 2,1111$ *para as palavras-código dos homofonemas e uma eficiência* $\eta_{MAX} = H(U)/E_{MAX}(W) = 0,9911/2,1111 = 0,4695$ *bits. Por outro lado, por tentativa e erro obtém-se*

$$P_U(u_1) = \frac{2}{9} + \frac{3}{9}$$

$$P_U(u_2) = \frac{4}{9}$$

que produz comprimento médio $E(W) = 5/3 = 1,6667$ *para as palavras-código dos homofonemas e uma eficiência* $\eta = H(U)/E(W) = 0,9911/1,6667 = 0,5946$ *bits, i.e., uma eficiência cerca de* $26,65\%$ *superior àquela obtida com o algoritmo MAX-ENT por passo.*

□

Existem casos em que ambas as técnicas (MAX-ENT por passo [16] e MIN-ENT por passo [17]) não apresentam limite para o número de lançamentos de moedas para a seleção de homofonema. Foi pensando nisto que se introduziu o uso da técnica de substituição homofônica com restrição Símbolo-a-Símbolo [18] para esses casos em especial, uma vez que com esta técnica sempre é possível limitar o número de lançamentos de moedas.

3.3 Técnica de codificação homofônica com restrição símbolo-a-símbolo

Considere $l_T(x)$ a profundidade da folha x na árvore T e $L_{\max} = \max_x l_T(x)$. Como já foi mencionado anteriormente haverá casos em que tanto o algoritmo MAX-ENT por passo quanto o MIN-ENT por passo produzirão árvores com comprimento infinito, i.e., árvores que não apresentam comprimento máximo, $L_{\max}$, finito.

Introduz-se agora o algoritmo da técnica de **substituição homofônica com restrição símbolo-a-símbolo** [18] na qual é possível se obter um $L_{\max}$ finito nos casos em que não é possível com os algoritmos de MAX-ENT por passo ou MIN-ENT por passo, usando para isto um número finito de palavras curtas que por concatenação produzem as palavras-código dos homofonemas. Tal propriedade será ilustrada na forma de exemplos na seção 3.3.4.

3.3.1 Descrição do algoritmo

Como explicado anteriormente, na codificação homofônica com restrição é necessário se trabalhar com o conjunto de todas as probabilidades dos símbolos da fonte de uma só vez, em vez da probabilidade de apenas um símbolo da fonte por vez a fim de fazer a decomposição em homofonemas de acordo com uma dada distribuição de probabilidade dos símbolos das palavras-código dos homofonemas. Na descrição que se segue deve-se assumir que a probabilidade de um homofonema é selecionada usando qualquer técnica de codificação homofônica com restrição, em particular os algoritmos MAX-ENT por passo ou MIN-ENT por passo podem ser usados para este propósito. Tal técnica é denominada **Substituição homofônica com restrição símbolo-a-símbolo (SHR-SAS)**.

1) **Algoritmo de decomposição do símbolo da fonte**

   Aplique uma técnica de **codificação homofônica com restrição (CHR)** aos símbolos de uma dada fonte K-ária, por um número de passos suficientes para associar pelo menos um ramo a cada símbolo da fonte. Seja S o número de passos empregados. Após S passos pode ocorrer que alguns dos símbolos u_i da fonte estejam completamente representados pelos ramos associados. Tais símbolos associados a u_i são denotados por $\tilde{u}_{ij}, 1 \leq j \leq J_i$, em que J_i é um inteiro positivo. Isto quer dizer que para cada um dos símbolos u_i que foram completamente representados a soma das probabilidades correspondentes aos ramos é igual à probabilidade deste símbolo, i.e., $P_U(u_i) = \sum_{j=1}^{J_i} P_{\tilde{U}}(\tilde{u}_{ij})$. Note, portanto que

$\tilde{u}_{ij}$ denota o j-ésimo homofonema associado ao símbolo u_i da fonte U.

Para cada símbolo u_i da fonte que após S passos não estiverem completamente representados pelos ramos associados, a diferença entre a probabilidade do símbolo, $P_U(u_i)$ e a soma $\sum_{j=1}^{J_i} P_{\tilde{U}}(\tilde{u}_{ij})$ das probabilidades dos ramos correspondentes é chamada probabilidade residual do símbolo e está relacionada ao símbolo mudo, Δ. Denota-se a probabilidade residual do símbolo u_i por $P(u_i, \Delta)$. Segue-se que o símbolo Δ tem probabilidade $P(\Delta)$ dada por

$$P(\Delta) = \sum_{i=1}^{K} P(u_i, \Delta).$$

Note que para os símbolos u_i que por ventura sejam completamente representados após S passos do algoritmo CHR, $P(u_i, \Delta) = 0$.

2) **Saída do canal homofônico**

(a) Dado que a fonte U seleciona um símbolo u_i, um experimento $(J_i + 1)$-ário $T = \{t_1, t_2, \ldots, t_{J_i}, t_{J_i+1}\}$ é feito em que J_i é o número de homofonemas (ramos) associados ao símbolo u_i. Desta forma, feito o experimento T o homofonema mudo é selecionado com probabilidade $P_T(t_{J_i+1}) = 1 - \sum_{i=1}^{K}\sum_{j=1}^{J_i} P_{ij} = 1 - \sum_{i=1}^{K}\sum_{j=1}^{J_i} \frac{P_{\tilde{U}}(\tilde{u}_{ij})}{P_U(u_i)}$ e um dos homofonemas relacionados à u_i é selecionado com probabilidade $P_T(t_j) = P_{ij} = \frac{P_{\tilde{U}}(\tilde{u}_{ij})}{P_U(u_i)}$ em que $1 \leq j \leq J_i$.

(b) A fonte expandida $\tilde{U}$ denota o conjunto de homofonemas mais o homofonema mudo Δ. $\tilde{u}_{ij}$ denota o j-ésimo ramo associado a u_i, i.e., o j-ésimo homofonema associado ao símbolo u_i da fonte U, portanto

$$\tilde{U} = \{\tilde{u}_{11}, \tilde{u}_{12}, \ldots, \tilde{u}_{1J_1}, \tilde{u}_{21}, \tilde{u}_{22}, \ldots, \tilde{u}_{2J_2}, \ldots, \tilde{u}_{K1}, \tilde{u}_{K2}, \ldots, \tilde{u}_{KJ_K}, \Delta\}$$

Cada símbolo na saída V do canal homofônico consiste de uma concatenação de símbolos de $\tilde{U}$ como explicado a seguir.

(c) Suponha que a fonte U selecionou um símbolo u_i para codificar. O experimento T é feito. Se o ramo $\tilde{u}_{ij}$ é selecionado então a saída do canal homofônico é o homofonema $\tilde{u}_{ij}$ e a fonte U é requisitada a selecionar o próximo símbolo a ser codificado. Porém, se Δ é selecionado, o experimento T é repetido quantas vezes forem necessárias até que um ramo $\tilde{u}_{ij}$ seja selecionado. A saída do canal homofônico será, portanto o

homofonema $\Delta\Delta\ldots\Delta\tilde{u}_{ij}$, em que o prefixo de $\tilde{u}_{ij}$ consiste de um número de Δs referente à quantidade de repetições do experimento T até que $\tilde{u}_{ij}$ seja selecionado. A fonte U é então requisitada a selecionar o próximo símbolo a codificar e assim por diante.

3) **Codificação com restrição SAS**

A representação de cada homofonema em V é dada pela concatenação dos representantes dos ramos correspondentes pertencentes à árvore obtida ao se aplicar o algoritmo CHR, e a representação do homofonema mudo é dada pela representação do(s) ramo(s) não usados nesta árvore.

4) **Decodificação com restrição SAS**

O processo de decodificação é imediato, bastando que para isso as palavras-código representando o homofonema mudo Δ sejam apagadas mapeando as palavras-código homofônicas restantes uma a uma aos símbolos da fonte U

Como primeira ilustração dos algoritmos introduzidos nas seções 3.2.1, 3.2.2 e nesta seção, considere o exemplo a seguir.

Exemplo 12 *Seja uma fonte discreta binária sem memória com* $P_U(u_1) = 14/27$ *e* $P_U(u_2) = 13/27$. *Considere a substituição homofônica binária perfeita aplicada a* U *quando* $\Pi_2 = \{3/5, 2/5\}$ *para a distribuição de probabilidade dos símbolos das palavras-código de homofonema.*

Inicialmente é aplicado o algoritmo MAX-ENT por passo [16](vide Apêndice C)

A entropia para esta fonte é $H(U) = 0,999$. *Pela árvore ilustrada na Figura 3.1 e usando o lema do comprimento do caminho (Lema 4, Capítulo A) calcula-se o comprimento médio da palavra-código chegando a* $E_{MAX}(W) = 2,08$. *Segue-se de (2) e (3) que a redundância é* $\rho_{MAX} = 0,5197$ *e a eficiência é* $\eta_{MAX} = 0,4803$, *respectivamente. Os homofonemas para* u_1 *são* $1, 0100, 01010, \ldots$ *e os homofonemas para* u_2 *são* $00, 011, \ldots$.

Usando agora para a mesma fonte e mesma distribuição de probabilidade dos símbolos das palavras de homofonema o algoritmo MIN-ENT por passo [17](vide Apêndice D).

Da árvore da Figura 3.2 calcula-se o comprimento médio, $E_{MIN}(W) = 2$. *Usando* $E_{MIN}(W) = 2$ *e a entropia* $H(U) = 0,999$, *a redundância calculada é dada por* $\rho_{MIN} =$

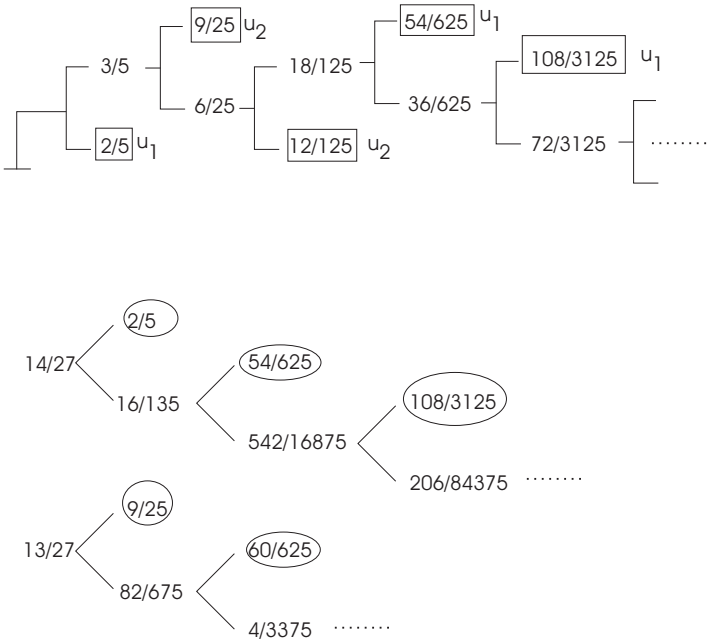


Figura 3.1: Algoritmo MAX-ENT por passo aplicado à fonte binária sem memória com probabilidades dos símbolos $P_U(u_1) = 14/27$ *e* $P_U(u_2) = 13/27$ *quando* $\Pi_2 = \{3/5, 2/5\}$ *é a distribuição de probabilidade dos símbolos das palavras de homofonema.*

$0,5005$ *e a eficiência* $\eta_{MIN} = 0,4995$. *Os homofonemas para* u_1 *são* $00, 010, \ldots$ *e para* u_2 *são* $1, 0110, 01110, \ldots$.

Considere novamente a Figura 3.2 usando alguns dos resultados obtidos ao se utilizar o algoritmo MIN-ENT por passo neste exemplo. Na Figura 3.3, $14/27$ *é expandido em dois homofonemas com probabilidades* $9/25$ *e* $18/125$, *respectivamente, deixando a probabilidade* $49/3375$ *(para expandir depois ou) para ser adicionada à probabilidade do símbolo mudo e termina-se a expansão de* $14/27$. *Similarmente, expande-se* $13/27$ *em um homofonema com probabilidade* $2/5$, *deixando a probabilidade* $11/135$ *(para ser expandida mais tarde ou) ser adicionada à probabilidade do símbolo mudo e termina-se a expansão de* $13/27$. *Segue-se que* $P(\Delta_1) = 49/3375$ *e* $P(\Delta_2) = 11/135$ *então* $P(\Delta) = P_U(u_1)P(\Delta_1) + P_U(u_2)P(\Delta_2) = (14/27)(49/1750) + (13/27)(11/65) = 12/125$. *Na Figura 3.4 é fornecida uma expansão alternativa para as mesmas probabilidades de símbolos da fonte, neste caso* $P(\Delta_1) = 49/3375$ *e* $P(\Delta_2) = 403/16875$ *e portanto,* $P(\Delta) = P_U(u_1)P(\Delta_1) + P_U(u_2)P(\Delta_2) = (14/27)(49/1750) + (13/27)(403/8125) = 24/625$.

Na seção a seguir o canal homofônico é revisto e uma analogia entre o canal K-ário assimétrico com apagamento e a técnica de substituição homofônica com restrição símbolo-a-

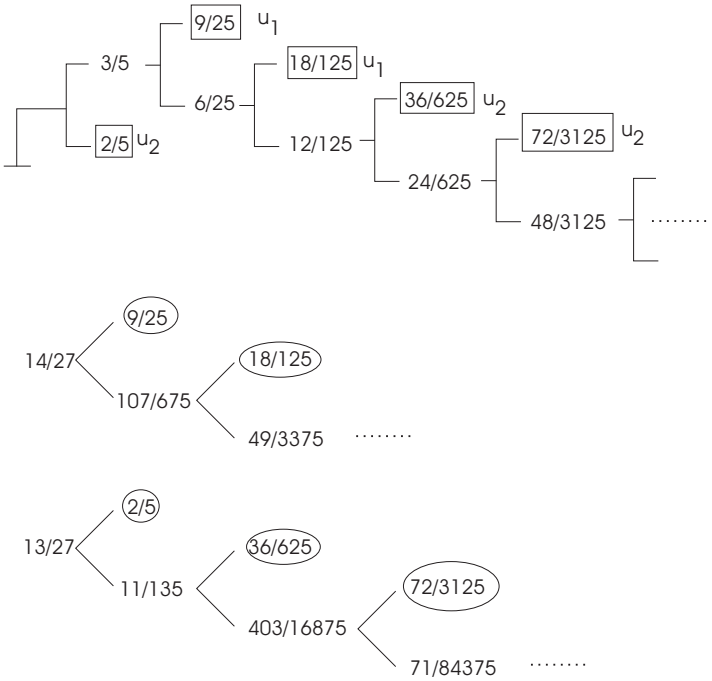


Figura 3.2: Algoritmo MIN-ENT por passo aplicado à fonte binária sem memória com probabilidades dos símbolos $P_U(u_1) = 14/27$ *e* $P_U(u_2) = 13/27$ *quando* $\Pi_2 = \{3/5, 2/5\}$ *é a distribuição de probabilidade dos símbolos das palavras de homofonema.*

símbolo é feita. A seção (seção 3.3.2) fornece mais subsídios para melhor análise dos exemplos envolvendo as técnicas de substituição homofônica com restrição descritas.

3.3.2 O canal homofônico

Como citado na seção 2.2.1 do Capítulo 2 quando o canal homofônico é um canal sem ruído, não-trivial [6], mas a codificação binária é trivialmente livre de prefixo porque todas as palavras-código têm o mesmo comprimento m (i.e., o código é um código de bloco), então se tem substituição homofônica clássica. No caso em que o canal homofônico é sem ruído e a codificação binária é livre de prefixo, então se obtém como resultado uma substituição homofônica com comprimento variável [9]. Uma terceira possibilidade, na qual $H(U|V) \neq 0$ é descrita a seguir em que o canal homofônico é representado por um canal com apagamento.

A seguir uma análise sobre o canal homofônico é feita, assim como uma analogia entre a técnica Rocha-Massey (RM) [7] e o canal K-ário com apagamento. Como resultado concluiu-se que a técnica RM produz informação na maior taxa possível com erro zero e alcança capacidade de um canal K-ário com apagamento quando $H(U) = \log K$ para uma fonte

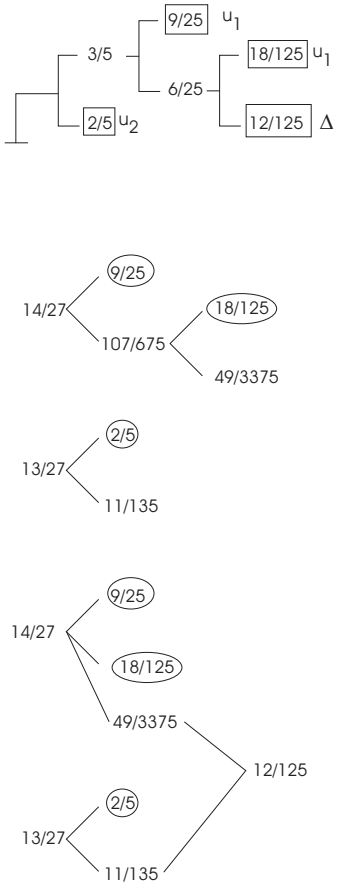


Figura 3.3: Técnica de substituição homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 12/125$

K-ária.

Logo após, na seção 3.3.3, a analogia é estendida considerando o canal K-ário assimétrico e a técnica de codificação homofônica símbolo-a-símbolo com restrição. A fim de simplificar a análise é considerado que apenas um homofonema e um símbolo mudo é associado a cada símbolo da fonte.

Em geral, como visto anteriormente, pode-se ter mais de um homofonema associado a cada símbolo da fonte. Associando mais de um homofonema a cada símbolo da fonte resultará num menor valor para $P(\Delta)$. Conseqüentemente, a eficiência η se aproximará ao valor que é obtido quando um algoritmo CHR para o qual não há limite para o número de lançamentos de moedas desbalanceadas é usado.

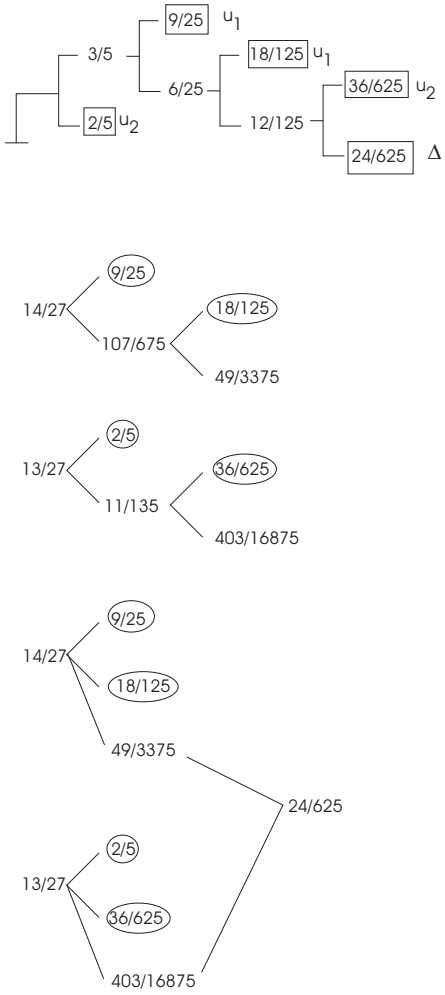


Figura 3.4: Técnica de substituição homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 24/625$

Canal K-ário com apagamento

Um canal binário com apagamento (*BEC - Binary Erasure Channel*) [19, p.92] é um canal discreto sem memória, modelado com uma entrada binária $U = \{u_1, u_2\}$ e uma saída ternária $V = \{v_1, v_2, v_3\}$ tal que $P_{V|U}(v_1|u_1) = P_{V|U}(v_2|u_2) = 1-\epsilon$ e $P_{V|U}(v_3|u_1) = P_{V|U}(v_3|u_2) = \epsilon$, sendo ϵ a probabilidade de ocorrência do símbolo de apagamento. A capacidade do BEC, C_{BEC}, é dada por $C_{BEC} = 1 - \epsilon$ [19, p.93].

Uma generalização imediata do BEC é proporcionada pelo canal K-ário com apagamento (*KEC - K-ary Erasure Channel*), $K \geq 2$. O KEC é um canal discreto sem memória modelado com uma entrada K-ária $U = \{u_1, u_2, \ldots, u_K\}$ e uma saída $(K+1)$-ária $V = \{v_1, v_2, v_3, \ldots, v_{K+1}\}$, em que $P_{V|U}(v_i|u_i) = 1 - \epsilon$ e $P_{V|U}(v_{K+1}|u_i) = \epsilon,\ 1 \leq i \leq K$, sendo ϵ a probabilidade da ocorrência símbolo de apagamento. É mostrado que a capacidade

do KEC, C_{KEC}, é dada por

$$C_{KEC} = [1 - \epsilon] \log K. \tag{3.1}$$

Gallager [19, p.506] propõe um problema no qual um BEC é operado em conjunto com um canal de retorno sem ruído a fim de informar ao remetente qual símbolo foi recebido. Sempre que um símbolo da fonte é transmitido, a codificação consiste em repetir tal símbolo enquanto o símbolo de apagamento é recebido por meio do canal de retorno. No momento em que o remetente recebe o símbolo correto a fonte pode então selecionar o próximo símbolo a ser transmitido. Surpreendentemente, esta estratégia de codificação alcança a capacidade no BEC, i.e., na média a fonte transmite $1 - \epsilon$ bits por uso do canal, ou 1 bit por $1/(1 - \epsilon)$ uso do canal em média. É imediato usar uma estratégia similar no KEC a fim de checar que a operação na capacidade é também alcançada.

O leitor deve ter notado a analogia entre o canal sem ruído usando a estratégia de realimentação para o KEC e o comportamento da técnica RM. É descrita a seguir uma implementação equivalente à técnica RM a fim de deixar tal analogia mais clara.

Descrição alternativa da técnica Rocha-Massey (RM)

Como descrito anteriormente na seção 2.4.2, a implementação da técnica RM consiste em se fazer um experimento binário, o qual produz na saída da fonte expandida, $\tilde{U}$, um símbolo mudo Δ com probabilidade $P_{\tilde{U}}(\Delta)$ ou um símbolo $\tilde{u}_i$ com probabilidade $1 - P_{\tilde{U}}(\Delta)$. Sempre que um símbolo mudo é produzido o experimento é repetido quantas vezes forem necessárias até que um símbolo $\tilde{u}_i$ seja produzido. No entanto, a distribuição de probabilidade da fonte, pode não ser uma distribuição que faz com que a capacidade do canal seja alcançada e tudo que pode ser dito é que a taxa de transmissão de informação, R_{RM}, na técnica RM é $H(U)$ bits por $1/[1 - P_{\tilde{U}}(\Delta)]$ "usos do canal " em média, i.e.,

$$R_{RM} = [1 - P_{\tilde{U}}(\Delta)]H(U). \tag{3.2}$$

Então no canal homofônico RM a informação mútua $I(U;V)_{RM}$ é precisamente $[1 - P_{\tilde{U}}(\Delta)]H(U)$. Conseqüentemente, conclui-se que a técnica RM produz informação na taxa mais alta com erro zero e alcança a capacidade sempre que $H(U) = \log K$ para uma fonte K-ária.

3.3.3 O canal K-ário assimétrico com apagamento

Considere o canal K-ário assimétrico com apagamento (K-AEC - *Asymetric Erasure Channel*), $K \geq 2$. O K-AEC é um modelo de canal discreto sem memória com uma entrada K-ária $U = \{u_1, u_2, \ldots, u_K\}$ e uma saída $(K+1)$-ária $V = \{v_1, v_2, v_3, \ldots, v_{K+1}\}$, em que $P_{V|U}(v_i|u_i) = 1 - \epsilon_i, P_{V|U}(v_{K+1}|u_i) = \epsilon_i$, e $P_V(v_{K+1}) = P(\Delta) = \sum_{i=1}^{K} P_U(u_i)\epsilon_i,\ 1 \leq i \leq K$, em que ϵ_i é a probabilidade de apagamento para o i-ésimo símbolo da fonte.

A analogia entre o K-AEC e a técnica de codificação com restrição SAS deve estar clara. A informação mútua $I(U;V)_{SAS-R}$ entre a entrada U e a saída V de um canal homofônico com restrição SAS, i.e., a taxa máxima de geração de informação em *bits* "por uso do canal" da técnica de substituição homofônica com restrição SAS (para uma dada distribuição de probabilidade de entrada) é dada por

$$\begin{aligned} I(U;V)_{SAS-R} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)(1-\epsilon_i)}\right] \\ &+ P(\Delta)\log\left[\frac{1}{P(\Delta)}\right] - \sum_{i=1}^{K} p_U(u_i)h(\epsilon_i). \end{aligned} \tag{3.3}$$

Em [19, p.506] um canal binário com apagamento (BEC -*binary erasure channel*) é descrito operando com realimentação sem ruído a fim de informar ao remetente que símbolo foi recebido. Quando um símbolo da fonte é transmitido, a codificação consiste na repetição daquele símbolo enquanto um símbolo de apagamento é recebido por intermédio do enlace de realimentação. Quando o receptor recebe o símbolo correto a fonte pode então selecionar o próximo símbolo a ser transmitido. Essa estratégia simples de codificação alcança capacidade no BEC, i.e., na média a fonte transmite $1-\epsilon$ *bits* por uso do canal, ou 1 *bit* por $1/(1-\epsilon)$ uso do canal na média. É portanto imediato utilizar uma estratégia similar no K-AEC e perceber que a capacidade também é alcançada. No caso da técnica de codificação homofônica SAS com restrição, a analogia com o K-AEC resulta na seguinte taxa R_{SAS-R} de transmissão de informação.

$$\begin{aligned} R_{SAS-R} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right] \\ &= H(U) - \sum_{i=1}^{K}\epsilon_i p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right]. \end{aligned} \tag{3.4}$$

Segue-se de (3.3) e (3.4) que

$$I(U;V)_{SAS-R} = R_{SAS-R} + \sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right]. \tag{3.5}$$

Lema 1

$$\sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] \geq 0. \tag{3.6}$$

Demonstração: A prova deste lema é feita a partir da desigualdade fundamental da Teoria da Informação, i.e., aplicando a desigualdade $\ln(1/x) \geq 1-x$ ao lado esquerdo de (3.6). Segue-se que

$$\begin{aligned}\sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] &\geq \frac{1}{\ln 2}\sum_{i=1}^{K} p_U(u_i)\epsilon_i \left[1 - \frac{P(\Delta)}{\epsilon_i}\right] \\ &= \frac{1}{\ln 2}\left[P(\Delta) - P(\Delta)\right] = 0.\end{aligned}$$

■

De (3.5) e (3.6) segue-se que $R_{SAS-R} \leq I(U;V)_{SAS-R}$. Entretanto, a operação com erro zero é garantida nas técnicas com restrição e SAS com restrição.

3.3.4 Alguns exemplos ilustrativos

Exemplo 13 *(cont. 12) Considere o Exemplo 12 e a seção 3.3.2.*

Pela árvore ilustrada na Figura 3.3 observa-se que as palavras-código correspondentes aos homofonemas $\tilde{u}_{11}$ e $\tilde{u}_{12}$, associados ao símbolo u_1 são respectivamente, $00, 010$*, enquanto que para o símbolo u_2 a palavra-código correspodente ao homofonema $\tilde{u}_{21}$ é* 1*. Observe também que o símbolo mudo é representado pela palavra-código* 011*. Desta forma os homofonemas correspondentes ao símbolos u_1 pertencem aos conjuntos $V_{11} = \{\tilde{u}_{11}, \Delta\tilde{u}_{11}, \Delta\Delta\tilde{u}_{11}, \dots\}$ e $V_{12} = \{\tilde{u}_{12}, \Delta\tilde{u}_{12}, \Delta\Delta\tilde{u}_{12}, \dots\}$, enquanto que os homofonemas correspondentes ao símbolo u_2 pertecem ao conjunto $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$, tendo portanto o comprimento médio dado por*

$$\begin{aligned}E_{SAS-R}(W) = &\left(\frac{9}{25}\right)\sum_{i=0}^{\infty}(2+3i)\left(\frac{7}{250}\right)^i + \left(\frac{18}{125}\right)\sum_{i=0}^{\infty}(3+3i)\left(\frac{7}{250}\right)^i \\ &+ \left(\frac{2}{5}\right)\sum_{i=0}^{\infty}(1+3i)\left(\frac{11}{65}\right)^i = 2,0057\end{aligned}$$

*e a taxa (*Equação 3.4*)*

$$R_{SAS-R} = 0,999 - \left[\frac{49}{3375}\log\frac{27}{14} + \frac{11}{135}\log\frac{27}{13}\right] = 0,8993.$$

Deste modo, utilizando o valor de R_{SAS-R} a eficiência e a redundância são dadas respectivamente por

$$\eta_{SAS-R} = \frac{R_{SAS-R}}{E_{SAS-R}(W)} = 0,4483,$$
$$\rho_{SAS-R} = 1 - \eta_{SAS-R} = 0,5516.$$

Com mais um passo na árvore ilustrada na Figura 3.3 chega-se à árvore da Figura 3.4. Para esta árvore os homofonemas correspondentes ao símbolo u_1 pertencem aos conjuntos $V_{11} = \{\tilde{u}_{11}, \Delta\tilde{u}_{11}, \Delta\Delta\tilde{u}_{11}, \dots\}$ e $V_{12} = \{\tilde{u}_{12}, \Delta\tilde{u}_{12}, \Delta\Delta\tilde{u}_{12}, \dots\}$, enquanto que os homofonemas correspondentes ao símbolo u_2 pertecem aos conjuntos $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ e $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$, com as palavras-código correspodentes a $\tilde{u}_{11}, \tilde{u}_{12}, \tilde{u}_{21}, \tilde{u}_{22}$ e Δ, dadas respectivamente por, $00, 010, 1, 0110$ e 0111.

Assim, o comprimento médio é dado por

$$\begin{aligned} E_{SAS-R}(W) = \; & \left(\frac{9}{25}\right)\sum_{i=0}^{\infty}(2+4i)\left(\frac{7}{250}\right)^i + \left(\frac{18}{125}\right)\sum_{i=0}^{\infty}(3+4i)\left(\frac{7}{250}\right)^i \\ & + \left(\frac{2}{5}\right)\sum_{i=0}^{\infty}(1+4i)\left(\frac{31}{625}\right)^i + \left(\frac{36}{625}\right)\sum_{i=0}^{\infty}(4+4i)\left(\frac{31}{625}\right)^i \\ & = 2,0087 \end{aligned}$$

e a taxa

$$R_{SAS-R} = 0,999 - \left[\frac{49}{3375}\log\frac{27}{14} + \frac{403}{16875}\log\frac{27}{13}\right] = 0,9601.$$

Com eficiência e redundância sendo dadas respectivamente por:

$$\eta_{SAS-R} = 0,4779,$$

$$\rho_{SAS-R} = 0,5221.$$

Exemplo 14 *(cont. Exemplo 11) No Exemplo 11 foi mostrado o valor resultante de redundância ρ ao se aplicar os algoritmos de MAX-ENT por passo e MIN-ENT por passo. Neste exemplo, é ilustrado o uso do algoritmo de substituição homofônica SAS com restrição para a mesma fonte.*

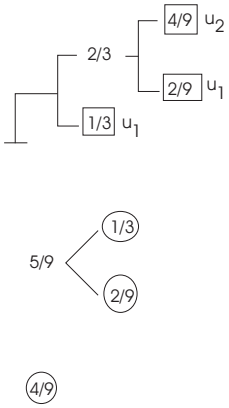


Figura 3.5: Técnica de codificação homofônica com restrição utilizando o algoritmo MIN-ENT por passo para a fonte discreta binária sem memória com $P_U(u_1) = 5/9$ e $P_U(u_2) = 4/9$ e distribuição de probabilidade dos símbolos das palavras de homofonema $\Pi_2 = \{2/3, 1/3\}$.

A árvore ao se utilizar o algoritmo MIN-ENT por passo está ilustrada na Figura 3.5.

Pelo valor de ρ dado no Exemplo 11, tem-se que para o algoritmo MIN-ENT por passo aplicado a esta fonte, eficiência $\eta_{MIN} = 1 - \rho_{MIN} = H(U)/E_{MIN}(W) = \dfrac{0,9911}{1,6667} = 0,5947.$

Já utilizando o algoritmo MAX-ENT por passo [16] a árvore ilustrada na Figura 3.6 é gerada.

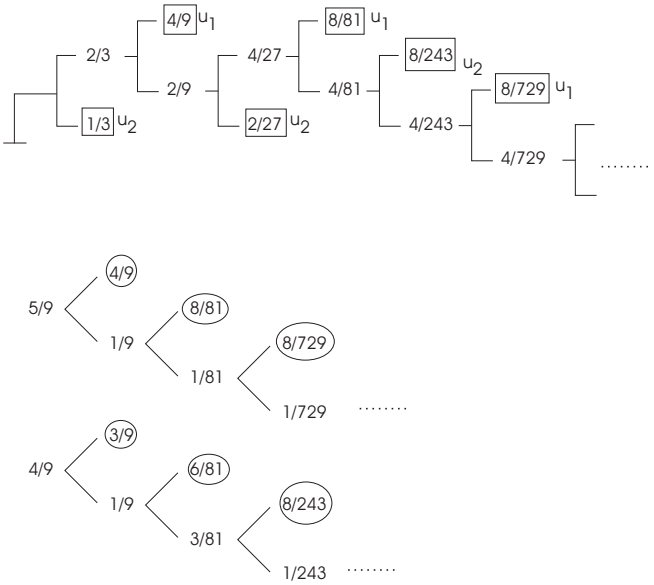


Figura 3.6: Técnica de codificação homofônica com restrição utilizando o algoritmo MAX-ENT por passo para a fonte discreta binária sem memória com $P_U(u_1) = 5/9$ e $P_U(u_2) = 4/9$ e distribuição de probabilidade dos símbolos das palavras de homofonema $\Pi_2 = \{2/3, 1/3\}$.

Com a redundância obtida no exemplo 11 obtém-se eficiência $\eta_{MAX} = 1 - \rho_{MAX} =$

$H(U)/E_{MAX}(W) = \dfrac{0,9911}{2,11} = 0,4695.$

Neste momento é aplicada a técnica de substituição homofônica com restrição símbolo-a-símbolo na árvore obtida (Figura 3.6) utilizando como base o algoritmo MAX-ENT por passo, uma vez que aqui o algoritmo MIN-ENT por passo já resultou numa árvore finita (Figura 3.5).

Neste e em todos os exemplos a seguir, a técnica de codificação homofônica com restrição símbolo-a-símbolo é aplicada inicialmente a partir do ponto em que a cada símbolo da fonte esteja associado a pelo menos um homofonema. A partir daí, a título de comparação, cada uma das outras aplicações da técnica ocorrem à distância de um passo do ponto em que a última aplicação da técnica parou, observando-se a árvore em questão.

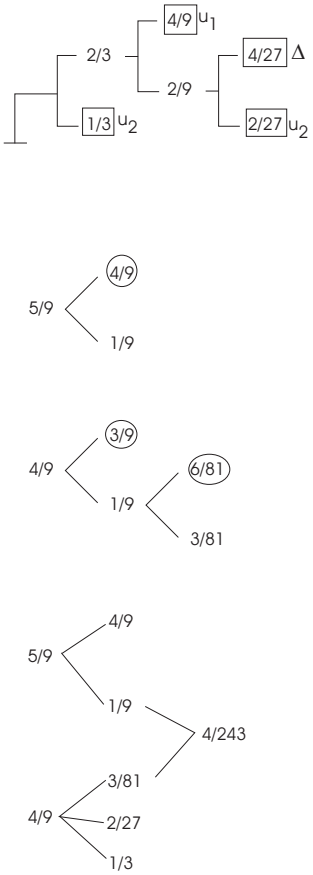


Figura 3.7: Técnica de codificação homofônica com restrição símbolo-a-símbolo tomando como base o algoritmo MAX-ENT por passo

Assim pela árvore obtida (Figura 3.7), o símbolo u_1 *tem seus representantes no conjunto* $V_{11} = \{\tilde{u}_{11}, \Delta\tilde{u}_{11}, \Delta\Delta\tilde{u}_{11}, \dots\}$ *e o símbolo* u_2 *tem seus representantes em* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e* $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$*, com palavras-código para* $\tilde{u}_{11}, \tilde{u}_{21}, \tilde{u}_{22}$

e Δ *dadas, respectivamente, por* $00, 1, 011$ *e* 010.

Neste exemplo, observa-se que o comprimento médio é dado por,

$$\begin{aligned} E_{SAS-R}(W) = & \left(\frac{4}{9}\right)\sum_{i=0}^{\infty}(2+3i)\left(\frac{1}{5}\right)^i + \left(\frac{1}{3}\right)\sum_{i=0}^{\infty}(1+3i)\left(\frac{1}{12}\right)^i \\ & + \left(\frac{2}{27}\right)\sum_{i=0}^{\infty}(3+3i)\left(\frac{1}{12}\right)^i = 2,2551, \end{aligned}$$

tendo conseqüentemente taxa

$$R_{SAS-R} = 0,9911 - \left[\frac{1}{5}\log\frac{9}{5} + \frac{1}{12}\log\frac{9}{4}\right] = 0,724,$$

com eficiência e redundância dadas respectivamente por:

$$\eta_{SAS-R} = R_{SAS-R}/E_{SAS-R}(W) = \frac{0,724}{2,2551} = 0,3211.$$

$$\rho_{SAS-R} = 1 - \eta_{SAS-R} = 1 - R_{SAS-R}/E_{SAS-R}(W) = 1 - 0,3211 = 0,6789.$$

Pela árvore da Figura 3.8, os homofonemas correspondentes a u_1 *pertencem aos conjuntos* $V_{11} = \{\tilde{u}_{11}, \Delta\tilde{u}_{11}, \Delta\Delta\tilde{u}_{11}, \dots\}$ *e* $V_{12} = \{\tilde{u}_{12}, \Delta\tilde{u}_{12}, \Delta\Delta\tilde{u}_{12}, \dots\}$*, enquanto que os homofonemas correspondentes ao símbolo* u_2 *pertecem aos conjuntos* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e* $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$*, com as palavras-códigos correspodentes a* $\tilde{u}_{11}, \tilde{u}_{12}, \tilde{u}_{21}, \tilde{u}_{22}$ *e* Δ*, dadas respectivamente por,* $00, 0100, 1, 011$ *e* 0101.

O comprimento médio obtido é dado, portanto, por

$$\begin{aligned} E_{SAS-R}(W) = & \left(\frac{4}{9}\right)\sum_{i=0}^{\infty}(2+4i)\left(\frac{1}{45}\right)^i + \left(\frac{8}{81}\right)\sum_{i=0}^{\infty}(4+4i)\left(\frac{1}{45}\right)^i \\ & + \left(\frac{1}{3}\right)\sum_{i=0}^{\infty}(1+4i)\left(\frac{1}{12}\right)^i + \left(\frac{2}{27}\right)\sum_{i=0}^{\infty}(3+4i)\left(\frac{1}{12}\right)^i \\ & = 2,1313 \end{aligned}$$

e a taxa

$$R_{SAS-R} = 0,9911 - \left[\frac{1}{81}\log\frac{9}{5} + \frac{3}{81}\log\frac{9}{4}\right] = 0,9373.$$

A eficiência e redundância neste caso são, respectivamente

$$\eta_{SAS-R} = \frac{0,9373}{2,1313} = 0,4398, \tag{3.7}$$

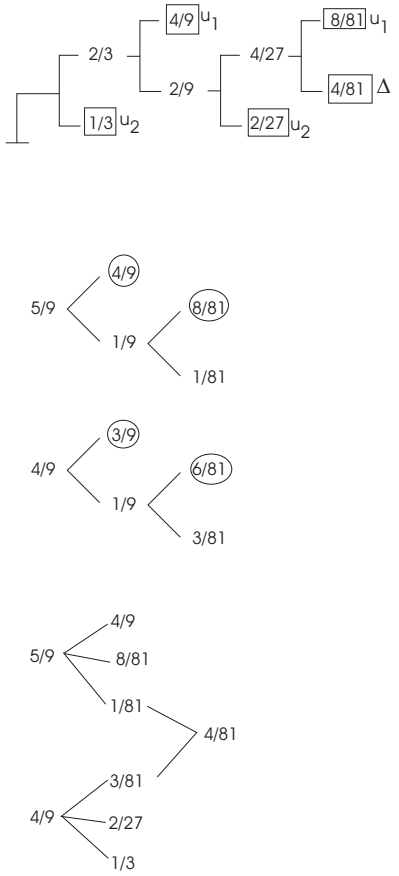


Figura 3.8: Técnica de codificação homofônica com restrição símbolo-a-símbolo tomando como base o algoritmo MAX-ENT por passo

$$\rho_{SAS-R} = 1 - \eta_{SAS-R} = 1 - 0,4398 = 0,5602. \tag{3.8}$$

Já pela árvore ilustrada na Figura 3.9, os homofonemas correspondentes ao símbolo u_1 *pertencem aos conjuntos* $V_{11} = \{\tilde{u}_{11}, \Delta\tilde{u}_{11}, \Delta\Delta\tilde{u}_{11}, \dots\}$ *e* $V_{12} = \{\tilde{u}_{12}, \Delta\tilde{u}_{12}, \Delta\Delta\tilde{u}_{12}, \dots\}$*, e os corespondentes ao símbolo* u_2 *pertecem aos conjuntos* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$*,* $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$ *e* $V_{23} = \{\tilde{u}_{23}, \Delta\tilde{u}_{23}, \Delta\Delta\tilde{u}_{23}, \dots\}$*, com as palavras-códigos correspodentes a* $\tilde{u}_{11}, \tilde{u}_{12}, \tilde{u}_{21}, \tilde{u}_{22}, \tilde{u}_{22}$ *e* Δ*, dadas respectivamente por,* $00, 0100, 1, 011, 01010$ *e* 01011*.*

Assim, o comprimento médio obtido é

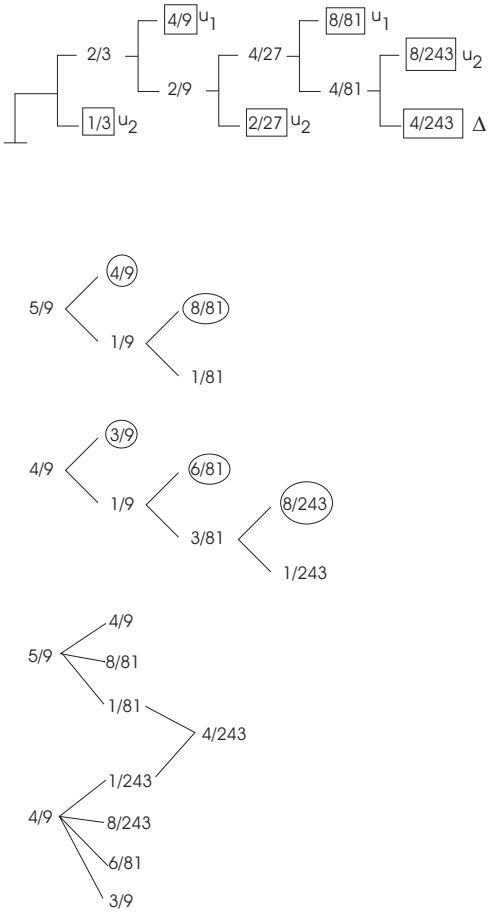


Figura 3.9: Técnica de codificação homofônica com restrição símbolo-a-símbolo tomando como base o algoritmo MAX-ENT por passo

$$\begin{aligned} E_{SAS-R}(W) = \quad & \left(\frac{4}{9}\right)\sum_{i=0}^{\infty}(2+5i)\left(\frac{1}{45}\right)^i + \left(\frac{8}{81}\right)\sum_{i=0}^{\infty}(4+5i)\left(\frac{1}{45}\right)^i \\ & + \left(\frac{1}{3}\right)\sum_{i=0}^{\infty}(1+5i)\left(\frac{1}{108}\right)^i + \left(\frac{2}{27}\right)\sum_{i=0}^{\infty}(3+5i)\left(\frac{1}{108}\right)^i \\ & + \left(\frac{8}{243}\right)\sum_{i=0}^{\infty}(5+5i)\left(\frac{1}{108}\right)^i = 2,1239 \end{aligned}$$

e a taxa é dada por

$$R_{SAS-R} = 0,9911 - \left[\frac{1}{81}\log\frac{9}{5} + \frac{1}{243}\log\frac{9}{4}\right] = 0,9758.$$

A eficiência e redundância são, respectivamente

$$\eta_{SAS-R} = \frac{0,9758}{2,1239} = 0,4594, \tag{3.9}$$

$$\rho_{SAS-R} = 1 - \eta_{SAS-R} = 1 - 0,4594 = 0,5406. \tag{3.10}$$

Exemplo 15 *Seja uma fonte discreta binária sem memória com* $P_U(u_1) = 2/3$, $P_U(u_2) = 1/6$ *e* $P_U(u_3) = 1/6$. *Considere a substituição homofônica binária perfeita aplicada a* U *quando* $\Pi_2 = \{2/3, 1/3\}$ *para a distribuição de probabilidade dos símbolos das palavras-código dos homofonema.*

Entropia da fonte

$$H(U) = \sum_{i=1}^{3} p_U(u_i) \log \frac{1}{p_U(u_i)} = \frac{2}{3} \log \frac{3}{2} + 2 \times \frac{1}{6} \log 6 = 1,2516.$$

Neste exemplo, também é aplicada inicialmente a técnica de codificação homofônica MIN-ENT por passo, estando o resultado ilustrado na Figura 3.10.

O comprimento médio obtido a partir da árvore da Figura 3.10 é

$$\begin{aligned} E_{MIN}(W) &= 1 + \frac{1}{3} + \frac{2}{9} + \frac{2}{27} + \frac{2}{81} + \frac{2}{243} + \frac{2}{729} + \dots \\ &= 1 + \frac{1}{3} + \frac{2}{9} \sum_{i=1}^{\infty} \left(\frac{1}{3}\right)^i \\ &= 1 + \frac{1}{3} + \frac{2}{9} \left(\frac{3}{2}\right) = 1,6667. \end{aligned}$$

A eficiência neste caso é dada por

$$\eta_{MIN} = \frac{H(U)}{E_{MIN}(W)} = 0,751$$

e, portanto, a redundância é dada por

$$\rho_{MIN} = 1 - \eta_{MIN} = 0,249.$$

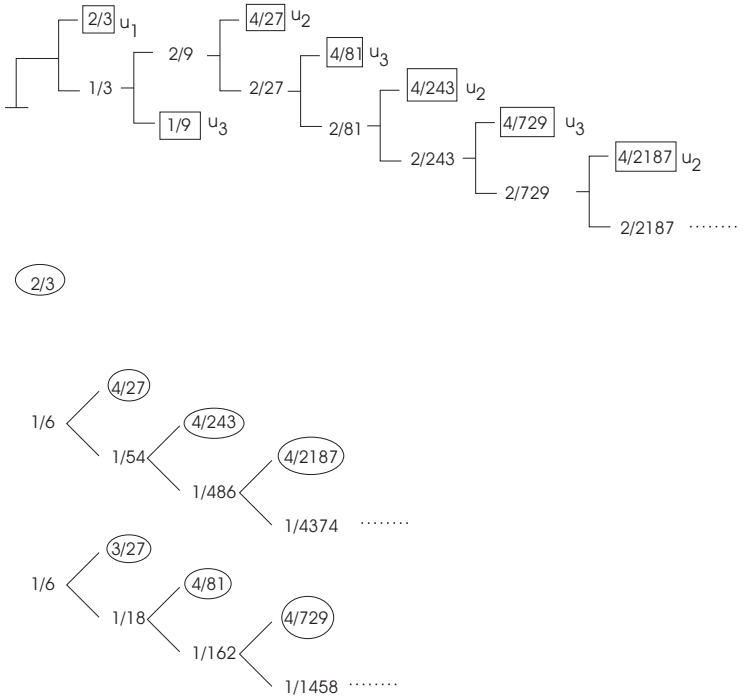


Figura 3.10: Técnica de codificação homofônica com restrição utilizando o algoritmo MIN-ENT por passo para a fonte discreta binária sem memória com $P_U(u_1) = 2/3$, $P_U(u_2) = 1/6$ *e* $P_U(u_2) = 1/6$ *distribuição de probabilidade dos símbolos das palavras de homofonema* $\Pi_2 = \{2/3, 1/3\}$.

Iniciando a aplicação da técnica de codificação homofônica com restrição símbolo-a-símbolo e tomando, novamente, como base o algoritmo MIN-ENT por passo, ao optar por parar inicialmente quando existe um homofonema associado a cada símbolo da fonte é obtida a árvore ilustrada na Figura 3.11.

Observa-se nesse exemplo que o símbolo u_1 *foi completamente representado sem a necessidade do uso do símbolo mudo, desta forma, o símbolo* u_1 *é associado ao homofonema* $\tilde{u}_{11}$ *cuja palavra-código é* 0. *Já os símbolos* u_2 *e* u_3 *necessitam do símbolo mudo e assim os homofonemas associados a* u_2 *pertecem ao conjunto* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e os associados a* u_3 *ao conjunto* $V_{31} = \{\tilde{u}_{31}, \Delta\tilde{u}_{31}, \Delta\Delta\tilde{u}_{31}, \dots\}$, *em que as palavras-código* $100, 11$ *e* 101 *estão associadas a* $\tilde{u}_{21}, \tilde{u}_{31}$ *e* Δ, *respectivamente.*

O comprimento médio é dado por

$$E_{SAS-R}(W) = \left(\frac{2}{3}\right) + \left(\frac{4}{27}\right)\sum_{i=0}^{\infty}(3+3i)\left(\frac{1}{9}\right)^i + \left(\frac{1}{9}\right)\sum_{i=0}^{\infty}(2+3i)\left(\frac{1}{3}\right)^i = 1,8125.$$

A taxa usando (3.4) é, portanto,

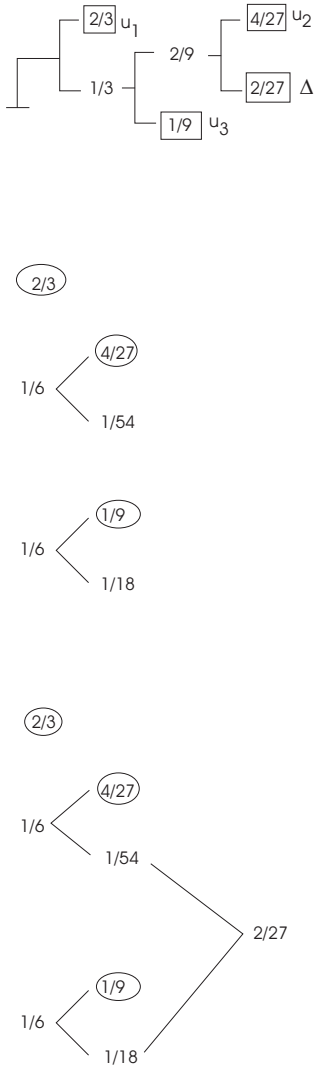


Figura 3.11: Técnica de codificação homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 2/27$.

$$R_{SAS-R} = 1,2516 - \left[\frac{1}{54}\log 6 + \frac{1}{18}\log 6\right] = 1,0601.$$

Logo, a eficiência e a redundância neste caso são dadas respectivamente por

$$\eta_{SAS-R} = 0,5849,$$

$$\rho_{SAS-R} = 0,4151.$$

Continuando a aplicar a técnica de substituição homofônica com restrição símbolo-a-

símbolo, sempre aumentando um passo por vez, são obtidas as árvores ilustradas nas Figuras 3.12, 3.13 e 3.14.

Para as três árvores (Figuras 3.12, 3.13 e 3.14) u_1 *está associado ao homofonema* $\tilde{u}_1$ *cuja palavra-código é* 0.

Para a árvore ilustrada na Figura 3.12 observa-se que o símbolo u_2 *tem seus homofonemas em* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e o símbolo* u_3 *em* $V_{31} = \{\tilde{u}_{31}, \Delta\tilde{u}_{31}, \Delta\Delta\tilde{u}_{31}, \dots\}$ *e* $V_{32} = \{\tilde{u}_{32}, \Delta\tilde{u}_{32}, \Delta\Delta\tilde{u}_{32}, \dots\}$

Para a árvore ilustrada na Figura 3.13 o símbolo u_2 *tem seus homofonemas em* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e* $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$. *Já o símbolo* u_3 *tem seus homofonemas em* $V_{31} = \{\tilde{u}_{31}, \Delta\tilde{u}_{31}, \Delta\Delta\tilde{u}_{31}, \dots\}$ *e* $V_{32} = \{\tilde{u}_{32}, \Delta\tilde{u}_{32}, \Delta\Delta\tilde{u}_{32}, \dots\}$.

Para a árvore ilustrada na Figura 3.14 o símbolo u_2 *tem seus homofonemas em* $V_{21} = \{\tilde{u}_{21}, \Delta\tilde{u}_{21}, \Delta\Delta\tilde{u}_{21}, \dots\}$ *e* $V_{22} = \{\tilde{u}_{22}, \Delta\tilde{u}_{22}, \Delta\Delta\tilde{u}_{22}, \dots\}$. *Já o símbolo* u_3 *tem seus homofonemas em* $V_{31} = \{\tilde{u}_{31}, \Delta\tilde{u}_{31}, \Delta\Delta\tilde{u}_{31}, \dots\}$, $V_{32} = \{\tilde{u}_{32}, \Delta\tilde{u}_{32}, \Delta\Delta\tilde{u}_{32}, \dots\}$ *e* $V_{33} = \{\tilde{u}_{33}, \Delta\tilde{u}_{33}, \Delta\Delta\tilde{u}_{33}, \dots\}$.

Em que $\tilde{u}_{21} \to 100, \tilde{u}_{22} \to 10110, \tilde{u}_{31} \to 11, \tilde{u}_{32} \to 1010, \tilde{u}_{33} \to 101110$. *Observe que para a árvore ilustrada na Figura 3.12,* $\Delta \to 1011$, *para a árvore na Figura 3.13,* $\Delta \to 10111$ *e para a árvore na Figura 3.14,* $\Delta \to 101111$.

Os comprimentos médios, taxas, eficiências e redundâncias, para as árvores ilustradas nas Figuras 3.12, 3.13 e 3.14 são mostrados a seguir.

Pela árvore da Figura 3.12, obtém-se

$$\begin{aligned} E_{SAS-R}(W) = \quad &= \left(\frac{2}{3}\right) + \left(\frac{4}{27}\right)\sum_{i=0}^{\infty}(3+4i)\left(\frac{1}{9}\right)^i + \left(\frac{1}{9}\right)\sum_{i=0}^{\infty}(2+4i)\left(\frac{1}{27}\right)^i \\ &+ \left(\frac{4}{81}\right)\sum_{i=0}^{\infty}(4+4i)\left(\frac{1}{27}\right)^i = 1,7115, \end{aligned}$$

taxa

$$R_{SAS-R} = 1,2516 - \left[\left(\frac{1}{54} + \frac{1}{162}\right)\log 6\right] = 1,1878,$$

eficiência $\eta_{SAS-R} = 0,694$ *e redundância* $\rho_{SAS-R} = 0,306$.

Pela árvore da Figura 3.13, obtém-se

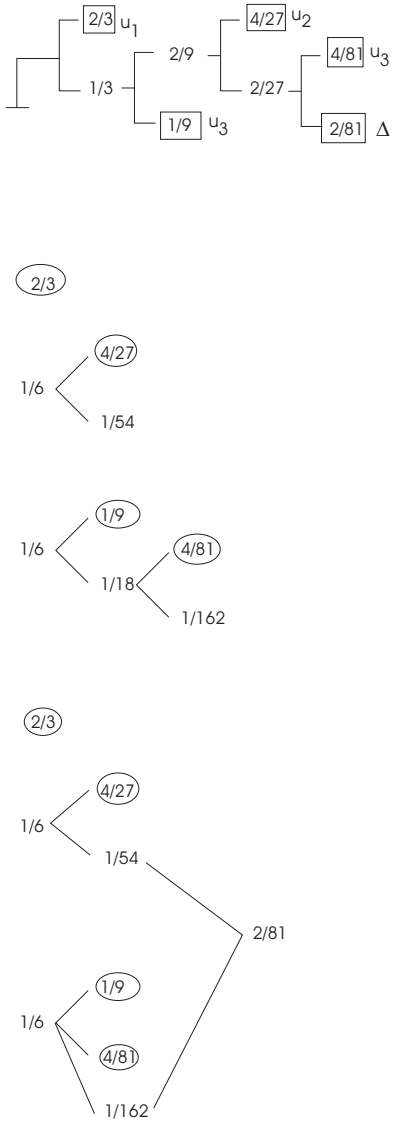


Figura 3.12: Técnica de codificação homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 2/81$.

$$
\begin{aligned}
E_{SAS-R}(W) = \quad & \left(\frac{2}{3}\right) + \left(\frac{4}{27}\right) \sum_{i=0}^{\infty} (3+5i) \left(\frac{1}{81}\right)^i + \left(\frac{4}{243}\right) \sum_{i=0}^{\infty} (5+5i) \left(\frac{1}{81}\right)^i \\
& + \left(\frac{1}{9}\right) \sum_{i=0}^{\infty} (2+5i) \left(\frac{1}{27}\right)^i + \left(\frac{4}{81}\right) \sum_{i=0}^{\infty} (4+5i) \left(\frac{1}{27}\right)^i \\
& = 1,6784,
\end{aligned}
$$

taxa,

$$R_{SAS-R} = 1,2516 - \left[\left(\frac{1}{486} + \frac{1}{162}\right) \log 6\right] = 1,2303,$$

eficiência $\eta_{SAS-R} = 0,733$ *e redundância* $\rho_{SAS-R} = 0,267$.

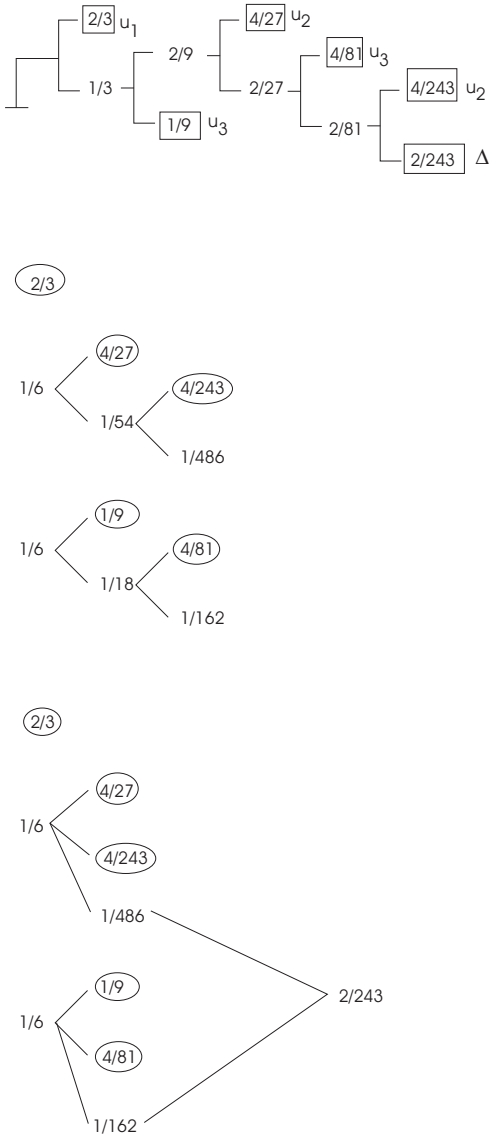


Figura 3.13: Técnica de codificação homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 2/243$.

E finalizando, este exemplo, pela árvore da Figura 3.14 obtém-se,

$$\begin{aligned} E_{SAS-R}(W) = \quad & \left(\frac{2}{3}\right) + \left(\frac{4}{27}\right)\sum_{i=0}^{\infty}(3+6i)\left(\frac{1}{81}\right)^i + \left(\frac{4}{243}\right)\sum_{i=0}^{\infty}(5+6i)\left(\frac{1}{81}\right)^i \\ & + \left(\frac{1}{9}\right)\sum_{i=0}^{\infty}(2+6i)\left(\frac{1}{243}\right)^i + \left(\frac{4}{81}\right)\sum_{i=0}^{\infty}(4+6i)\left(\frac{1}{243}\right)^i \\ & + \left(\frac{4}{729}\right)\sum_{i=0}^{\infty}(6+6i)\left(\frac{1}{243}\right)^i = 1,6712, \end{aligned}$$

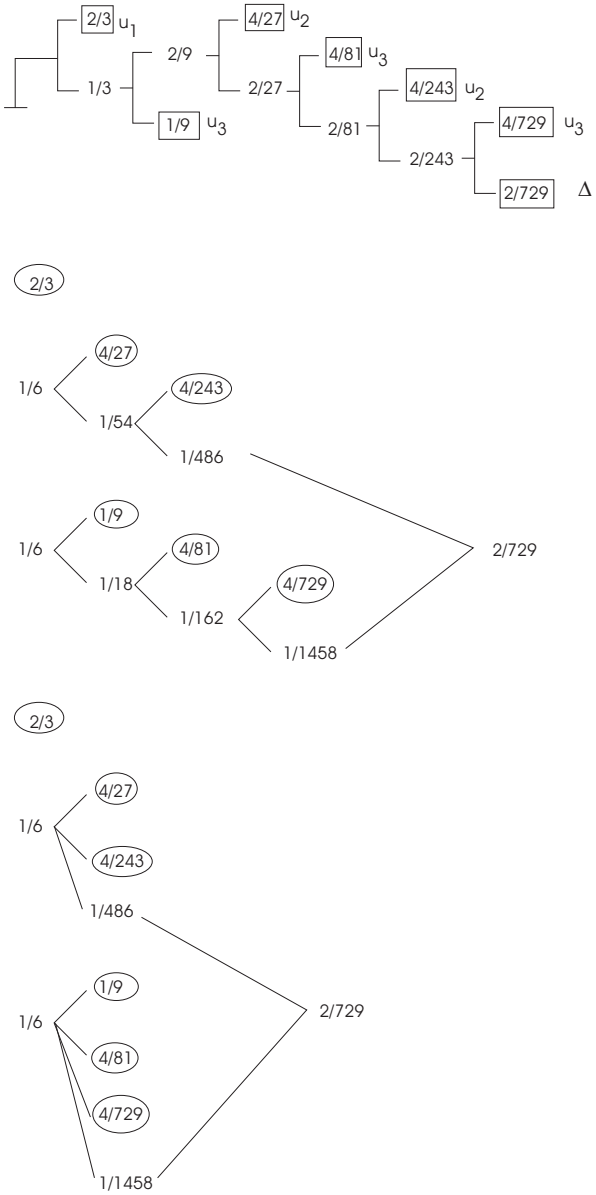


Figura 3.14: Técnica de codificação homofônica com restrição símbolo-a-símbolo baseada no algoritmo MIN-ENT por passo, $P(\Delta) = 2/729$

taxa

$$R_{SAS-R} = 1,2516 - \left[\left(\frac{1}{486} + \frac{1}{1458}\right)\log 6\right] = 1,2445,$$

eficiência $\eta_{SAS-R} = 0,7447$ *e redundância* $\rho_{SAS-R} = 0,2553$.

Comparativo dos exemplos

A fim de facilitar a comparação dos métodos aqui mostrados (MIN-ENT por passo, MAX-ENT por passo e símbolo-a-símbolo com restrição) é mostrada uma tabela com os valores

obtidos de eficiência nos exemplos da seção 3.3.4.

Como o método MAX-ENT nos casos ilustrados demonstrou pior desempenho que o MIN-ENT em alguns dos exemplos não existe resultado na tabela para η_{MAX}.

Tabela 3.1: Tabela com resumo dos valores de η obtidos nos exemplos da seção 3.3.4.

Exemplos	**MAX-ENT**	**MIN-ENT**	**SAS-R**
Exemplos 12 e 13 $P(\Delta) = 12/125$	$\eta_{MAX} = 0,4803$	$\eta_{MIN} = 0,4995$	$\eta_{SAS-R} = 0,4483$
Exemplos 12 e 13 $P(\Delta) = 24/625$	$\eta_{MAX} = 0,4803$	$\eta_{MIN} = 0,4995$	$\eta_{SAS-R} = 0,4779$
Exemplos 11 e 14 $P(\Delta) = 4/27$	$\eta_{MAX} = 0,4695$	$\eta_{MIN} = 0,5947$	$\eta_{SAS-R} = 0,3097$
Exemplos 11 e 14 $P(\Delta) = 4/81$	$\eta_{MAX} = 0,4695$	$\eta_{MIN} = 0,5947$	$\eta_{SAS-R} = 0,4398$
Exemplos 11 e 14 $P(\Delta) = 4/243$	$\eta_{MAX} = 0,4695$	$\eta_{MIN} = 0,5947$	$\eta_{SAS-R} = 0,4594$
Exemplos 15 $P(\Delta) = 2/27$	-	$\eta_{MIN} = 0,7509$	$\eta_{SAS-R} = 0,5849$
Exemplos 15 $P(\Delta) = 2/81$	-	$\eta_{MIN} = 0,7509$	$\eta_{SAS-R} = 0,694$
Exemplos 15 $P(\Delta) = 2/243$	-	$\eta_{MIN} = 0,7509$	$\eta_{SAS-R} = 0,733$
Exemplos 15 $P(\Delta) = 2/729$	-	$\eta_{MIN} = 0,7509$	$\eta_{SAS-R} = 0,7447$

Pela tabela 3.1 nota-se a tendência dos resultados obtidos usando a técnica de codificação Símbolo-a-Símbolo se aproximarem daqueles obtidos aplicando-se a técnica MIN-ENT por passo com a vantagem de limitar o comprimento máximo da árvore.

3.4 Uso das técnicas de substituição homofônica com restrição para a geração de dados honestos por meio do lançamento de duas ou mais moedas desbalanceadas

O problema da geração de uma distribuição de probabilidade discreta usando lançamentos de uma moeda desbalanceada é antigo e importante nas áreas de criptografia e de geração de números aleatórios, sendo usados para testes e simulação de sistemas de comunicações, assim como em muitas outras aplicações computacionais.

Há mais de quarenta anos von Neumann [20] introduziu um algoritmo simples para gerar uma seqüência de *bits* estatisticamente independentes e equiprováveis a partir do lançamento de uma moeda com viés desconhecido. A partir daí, muitos pesquisadores têm considerado o problema e estudado a geração de variáveis aleatórias uniformes sob diferentes pontos de vista [21]-[30].

Basicamente, dois aspectos são levados em conta neste tipo de problema: a geração considerando um **tempo limite curto** (*short bounded time*) ou mais tradicionalmente, conside-

rando um **tempo esperado curto** (*short expected time*). A técnica mostrada nesta seção considera a aproximação por tempo esperado curto. Tal técnica foi apresentada inicialmente em 2004 no XXI Simpósio Brasileiro de Telecomunicações [31] e há pouco foi revisitada, sendo complementada e resultando no artigo [32].

Em [33] muitas questões algorítmicas relacionadas ao problema clássico da simulação de saídas de uma variável aleatória usando um número limitado de moedas desbalanceadas foram consideradas, e um algoritmo foi fornecido a fim de gerar um dado honesto com n faces usando uma moeda honesta e uma desbalanceada. A distribuição de probabilidade de caras e coroas da moeda desbalanceada é dada por

$$\left(2^{\lceil \log r(m) \rceil}/m, 1 - 2^{\lceil \log r(m) \rceil}/m\right), \tag{3.11}$$

Em que m é o maior fator impar de n e $r(m) = m - 2^{\lfloor \log m \rfloor}$.

No pior caso,

$$1 + \lfloor \log n \rfloor + \lceil \log(n - 2^{\lfloor \log n \rfloor}) \rceil + pw(n) \tag{3.12}$$

lançamentos de moedas são necessários, onde $pw(n) = \max\{i : 2^i \text{ divides } n\}$.

As moedas desbalanceadas que são empregadas no algoritmo proposto são arbitrárias, i.e., não dependem de n como é o caso do algoritmo proposto em [33]. Maiores detalhes sobre o algoritmo pode ser obtido em [32] o qual se encontra na integra no Apêndice H.

O exemplo no qual $n = 7$ apresentado em [31] é revisto, uma vez que foi percebido um engano na aplicação do algoritmo e ele apresenta resultado ainda melhor do que o apresentado naquela ocasião.

O algoritmo introduzido em 2004 [31] e revisitado há pouco [32] é basicamente uma generalização para mais de uma moeda desbalanceada do algoritmo MIN-ENT por passo [17] o qual já foi comentado na seção 3.2.2 e que se encontra em detalhes no apêndice D. Foram obtidos resultados equivalentes e em alguns casos ainda melhores daqueles em [33].

Na próxima subseção (subseção 3.4.1) são fornecidos alguns exemplos que mostram valores menores aos obtidos em [33] para o comprimento médio $E[T]$ que é obtido usando o lema do comprimento do caminho (lema 4) para árvore T.

Com o algoritmo de [31, 32], existem casos onde o comprimento máximo $L_{\max}$ não é limitado mas mesmo nesses casos obtém-se $E[T]'$s menores.

3.4.1 Exemplos ilustrativos

Para todas as árvores ilustradas nos exemplos a seguir de cada nó emanam duas ramificações. Em cada nó está indicada a distribuição de probabilidade da moeda usada. Quando não há indicação assume-se que uma moeda honesta é usada, caso haja uma indicação do tipo $(p, 1-p)$ significa que uma moeda desbalanceada com probabilidade de cara dada por p e coroa dada por $1-p$ está sendo usada. Cada ramificação possui uma probabilidade.

A título comparativo, aplica-se o algoritmo sugerido usando as moedas que seriam usadas no algoritmo introduzido em [33] para a geração de uma distribuição de probabilidade uniforme usando duas moedas, uma honesta e outra desbalanceada com distribuição dada em (3.11)

Chama-se atenção mais uma vez para o fato que o algoritmo proposto [32] funciona para qualquer escolha das moedas, enquanto o algoritmo proposto em [33] é específico para uma dada escolha de moedas.

Exemplo 16 *Considere a geração de uma distribuição de probabilidade de um dado honesto, i.e., $n = 6$, usando as moedas $m_1 = (1/2, 1/2)$ e $m_2 = (2/3, 1/3)$. A mesma árvore é obtida (Figura 3.15) tanto para o algoritmo em [33] quanto para o algoritmo proposto em [32]. Calcula-se para estas árvores $E[T] = 2,67$ e $L_{\max} = 3$.*

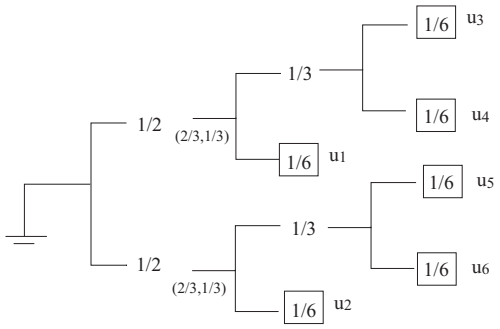


Figura 3.15: Árvore obtida para $n = 6$ tanto pelo algoritmo em [33] quanto para o algoritmo em [32].

O exemplo a seguir foi inicialmente abordado em [31] mostrando como resultado $E[T] = 3,29$ era equivalente ao resultado obtido pelo algoritmo em [33], no entanto ao revisitar o algoritmo observou-se que em um dos passos houve um engano na escolha que deveria ter sido feita seguindo o algoritmo, e seguindo esta escolha, o comprimento médio obtido se mostrou na verdade melhor do que o obtido pelo algoritmo em [33], como é visto a seguir em maiores detalhes.

Exemplo 17 *Considere a geração de uma distribuição de probabilidade uniforme de uma variável aleatória com* $n = 7$ *possíveis valores, usando para isto as moedas* $m_1 = (1/2, 1/2)$ *e* $m_2 = (3/7, 4/7)$. *A árvore obtida (Figura 3.16) com o algoritmo em [33] resulta um* $E[T] = 3,29$ *e* $L_{\max} = 4$.

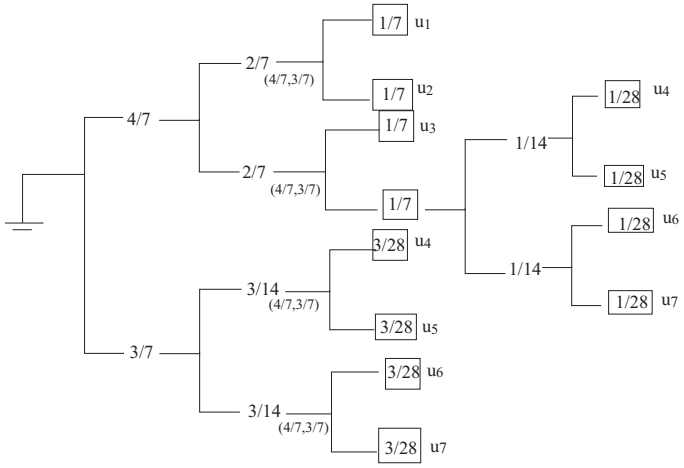


Figura 3.16: Árvore obtida usando o algoritmo em [33] para $n = 7$.

Por outro lado, usando o algoritmo proposto em [32] chega-se à árvore ilustrada na Figura 3.17 cujo comprimento máximo $L_{\max}$ *é ilimitado porém resultando num comprimento médio* $E[T] = 1 + \frac{1}{2} + \frac{1}{2} + \frac{2}{7} + \frac{2}{7} + \frac{3}{14} + \frac{3}{14} + \frac{9}{98} + \frac{9}{196} + \frac{9}{343}\left[1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots\right] = 3,1378 + \sum_{i=0}^{\infty}\left(\frac{1}{2}\right) = 3,1902$ *que é um resultado melhor ao obtido usando o algoritmo em [33].*

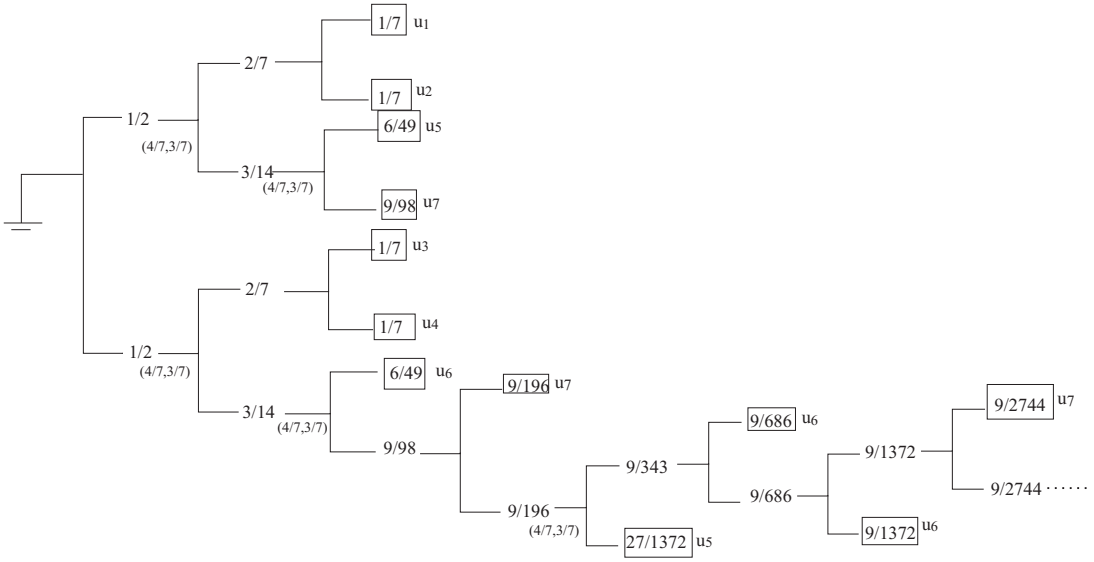


Figura 3.17: Árvore obtida usando o algoritmo em [32] para $n = 7$.

A priori, como pode ser observado pela descrição do algoritmo proposto, o mesmo não depende da escolha das moedas a serem usadas, porém observou-se que em alguns casos o resultado para $E[T]$ pode ser pior que o obtido pelo algoritmo em [33]. Por esta razão ainda se encontra em investigação se existem moedas que proporcionam melhores desempenhos dependendo do n em questão. De qualquer forma, o algoritmo proposto já mostrou que ao usar as moedas propostas em [33] apresenta resultado no mínimo equivalente ao obtido pelo algoritmo em [33].

capítulo 4

Conclusões e sugestões para trabalhos futuros

Esta tese enfocou técnicas de substituição homofônica, embasadas no conceito de Shannon de cripto-sistema fortemente ideal, uma vez que ele provê a motivação para o uso de qualquer tipo de substituição homofônica. Foram revistos alguns conceitos ligados à substituição homofônica, como por exemplo, definição de substituição homofônica de comprimento-variável, assim como a condição necessária e suficiente para tal substituição gerar uma seqüência completamente aleatória. Foi feita a análise de algumas técnicas de substituição homofônica padrão assim como de substituição homofônica com restrição, sendo introduzidas duas novas técnicas de substituição homofônica padrão, que pertencem a uma classe que foi denominada Substituição Homofônica Símbolo-a-Símbolo. A primeira técnica proposta não apresentou o desempenho esperado, porém por meio de sua análise foi possível fazer alterações que resultaram na segunda técnica de substituição homofônica símbolo-a-símbolo, a qual mostrou resultado melhor que a técnica RM e se mostrou semelhante à técnica JKM, considerando como métrica a eficiência. Com relação à técnica JKM modificada, nos casos em que os símbolos da fonte apresentam em sua decomposição razões distintas e, portanto, símbolos mudos distintos, a segunda técnica de substituição homofônica símbolo-a-símbolo apresentou mesmo desempenho com a possibilidade de se utilizar um único símbolo mudo. Uma técnica de substituição homofônica com restrição pertencente à classe das técnicas de substituição homofônica símbolo-a-símbolo foi proposta. Tal técnica apresenta como vantagem sobre as técnicas conhecidas o fato de possibilitar que o comprimento da árvore obtida no processo de codificação

seja limitado, o que não ocorre em alguns casos ao se utilizar uma outra técnica de substituição homofônica com restrição. Para isto, tal técnica utiliza um número finito de palavras curtas que por concatenação produzem as palavras-código dos homofonemas. Observou-se que ao utilizar essa técnica à medida que se aumenta a quantidade de passos na árvore a eficiência da técnica de codificação símbolo-a-símbolo se aproxima da eficiência obtida pela técnica de substituição homofônica com restrição tomada como base, lembrando que a técnica símbolo-a-símbolo apresenta a vantagem de limitar o comprimento máximo da árvore. A partir de técnicas de substituição homofônica com restrição conhecidas foi proposta uma solução alternativa para o problema clássico de geração de uma distribuição de probabilidade discreta uniforme usando duas ou mais moedas desbalanceadas com o uso de técnicas de substituição homofônica com restrição. Uma análise comparativa com um método introduzido recentemente [33] foi feita e observou-se que ao utilizar as mesmas moedas propostas em tal método a técnica aqui introduzida apresentou desempenho equivalente, ou melhor, levando em conta o aspecto do tempo esperado curto. Observa-se, então que as técnicas introduzidas contribuem não só na obtenção de cripto-sistemas simétricos mais resistentes à criptoanálise, como para a geração de números pseudo-aleatórios, podendo ser utilizadas também em testes e simulações de sistemas de comunicações, assim como em muitas outras aplicações computacionais.

4.1 Sugestões para trabalhos futuros

É necessário que seja feita uma análise mais aprofundada das técnicas de substituição homofônica símbolo-a-símbolo a fim de definir cotas superiores. Com relação à técnica de substituição homofônica com restrição é interessante analisar a relação custo benefício, ou um modo de decisão, a fim de definir a quantidade de passos a serem dados a fim de alcançar a eficiência desejada, lembrando que tal eficiência se encontra limitada pela técnica de substituição homofônica utilizada como base do algoritmo. Com relação à solução dada ao problema de geração de uma distribuição de probabilidade discreta uniforme usando duas ou mais moedas desbalanceadas com o uso de técnicas de substituição homofônica com restrição, observou-se que *a priori*, o algoritmo proposto não depende da escolha das moedas a serem usadas, porém o desempenho do algoritmo, medido em termos de tempo esperado curto, varia dependendo do grupo de moedas usadas. Esta observação sugere a existência de um grupo de moedas desbalanceadas que o otimize. Desta forma, sugere-se investigar um possível critério de escolha de moedas a fim de otimizar o algoritmo. Além disso, uma investigação sobre

a possibilidade de implementar tal técnica com árvores finitas em casos que isto não ocorre parece interessante mesmo que o objetivo tenha sido o critério do tempo esperado curto.

Bibliografia

[1] D. Santos, "Brasil é líder em golpe via e-mail", PC World 08/02/2007 - http://www.ipdi.com.br/newsview.php?idNews=37&idCatNews=51, acessado em 15/04/07.

[2] L. A. Gordon, M. P. Loeb, W. Lucyshyn and R. Richardson *2006 CSI/FBI Computer Crime and Security Survey* http://www.gosci.com.

[3] An Introduction to Information Security; A Certicom White Paper; 1997. *http://www.certicom.com*

[4] S. Singh, *The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. Doubleday, 1999.

[5] R. Lidl and H. Niederreiter *Introduction to Finite Fields and their Applications*, Cambridge University Press, 2002.

[6] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An Information-Theoretic Approach to Homophonic Substitution", *Advances in Cryptology-Eurocrypt'89* (Eds. J.-J. Quisquater and J. Vandewalle), LNCS No. 434. Springer, pp. 382-394, 1990.

[7] V. C. da Rocha and J. L. Massey, "Better than "optimum" homophonic substitution", *Proc. IEEE International Symposium on Information Theory*, 25-30 June 2000, Sorrento, Italy, p. 241.

[8] V. C. da Rocha, "Perfect homophonic substitution with finite memory", *Proc. IEEE International Symposium on Information Theory*, 30 June - 05 July 2002, Lausanne, Switzerland, p. 409.

[9] Ch. G. Günther, "A Universal Algorithm for Homophonic Coding", *Advances in Cryptology- Eurocrypt'88*, Lecture Notes in Computer Science, No.330. Heidelberg and New York: Springer, pp. 405-414, 1988.

[10] V. C. da Rocha Jr., C. Pimentel and D. P. B. A. Camara, "Redundancy in homophonic coding and a new homophonic coding technique", *Proceedings of the International Symposium on Information Theory - ISIT 2006*, Seattle, Washington, pp. 1253-1257, 9-14 July 2006.

[11] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Tech. J.*, vol.28, pp. 656-715, Oct. 1949.

[12] N. Abramson, *Information Theory and Coding*. McGraw-Hill, 1963.

[13] V. C. da Rocha and J. L. Massey, "On the entropy bound for optimum homophonic substitution", *Proc. IEEE International Symposium on Information Theory*, 29 June - 4 July 1997, Ulm, Germany, p. 93.

[14] V. C. da Rocha and M.M. Vasconcelos, "Nova geração da representação D-ária de um número racional", *XXII Simpósio Brasileiro de Telecomunicações, 2005, Campinas. Anais do XXII Simpósio Brasileiro de Telecomunicações*, 2005, pp. 573-575.

[15] V. C. da Rocha, "On the minimum redundancy of homophonic coding", *International Telecomunications Symposium - ITS2002*, 30 June - 05 July 2002, Natal-RN, Brasil, pp.310-314.

[16] V. C. da Rocha and C. Pimentel, "Binary-constrained homophonic coding", *VI International Symposium on Communication Theory and Applications*, Ambleside, England,pp. 263-268, 15 - 20 July 2001.

[17] V. C. da Rocha Jr. and C. Pimentel, "Optimum binary-constrained homophonic coding", *VII International Symposium on Communication Theory and Applications*, Ambleside, England,pp. 64-69, 13 - 18 July 2003.

[18] V. C. da Rocha Jr., D. P. B. A. Camara and C. Pimentel, "Binary Constrained Letter-by-Letter Homophonic Coding", *Proceedings of the International Telecommunications Symposium - ITS 2006*,pp. 877-882, 3 - 6 September 2006 Fortaleza - CE, Brasil

[19] R.G. Gallager and D.C. Van Voorhis, "Optimal Source Codes for Geometrically Distributed Integer Alphabets", *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 228-230, Mar. 1975.

[20] J.von Neumann, "Various techniques used in connection with random digits", notes by G. E. Forsythe, *National Bureau of Standards, Applied Math Ser.*, vol. 12, pp. 36-38; reprinted in von Neumann's Collected Works., vol. 5. Oxford, U.K.: Pergamon, 1963, pp. 768-770.

[21] J. Abrahams, "Generation of discrete distributions from biased coins ", *IEEE Trans. on Inform. Theory*, vol. 42, pp. 1541-1546, 1996.

[22] M. Blum, "Independent unbiased coin flips from a correlated biased source-A finite state Markov chain", *Combinatorica*, vol. 6, no. 2, pp. 97-108, 1986.

[23] E. W. Dijkstra, "Making a fair roulette from a possibly biased coin", *Inform. Processing Lett.*, vol. 36, p. 193, 1990.

[24] P.Elias, "The efficient computation of an unbiased random sequence", *Ann. Math. Statist.*, vol. 43, pp. 865-870, 1972.

[25] W. Hoeffding and G. Simons, "Unbiased coin tossing with a biased coin", *Ann. Math. Statist.*, vol. 41, pp. 341-352, 1970.

[26] T. S. Han and M. Hoshi, "Interval algorithm for random number generation", *IEEE Trans. on Inform. Theory*, vol. 43, pp. 599-611, March 1997.

[27] Y. Horibe, "Entropy and optimal random number transformation", *IEEE Trans. on Inform. Theory*, vol. 27,pp.527-529, July 1981.

[28] D.E. Knuth and A. C. Yao, "The complexity of nonuniform random number generation", *in Algorithms and Complexity, New Directions and Results*, J. F. Traub, Ed. New York: Academic, 1976, pp.357-428.

[29] R. Motwani and P. Raghavan, *Randomized Algorithms. Cambridge*, U.K.: Cambridge Univ. Press, 1996.

[30] Q. F. Stout and B. Warren, "Tree algorithms for unbiased coin tossing with a biased coin", *Ann. Probab.*, vol. 12, pp. 212-222, 1984.

[31] D. P. B. de A. Camara, V. C da Rocha Jr. e C. Pimentel, "Geração de uma distribuição discreta usando moedas desbalanceadas ", *Anais do XXI Simpósio Brasileiro de Telecomunicações - SBrT2004*, pp. 1 - 5, Belém, Pará, 06-09 de setembro de 2004.

[32] D. P. B. de A. Camara, V. C da Rocha Jr. e C. Pimentel, "Generation of a Discrete Distribution using Biased Coins", *Proceedings of the International Symposium on Information Theory and its Applications - ISITA2006*, COEX, Seul, Corea, 29 october - 1 november 2006.

[33] L. Gargano and Ugo Vaccaro, " Efficient generation of fair dice with few biased coins ", *IEEE Trans. on Inform. Theory*, vol. 45, pp. 1600-1606, July 1999.

[34] D. Feldman,R. Impagliazzo, M. Naor, N. Nisan, S. Rudich, and A. Shamir, "On dice and coins: Models of computation for random generation", *Inform. Comput.*, vol. 104, pp. 159-174, 1993.

[35] V. C. da Rocha Jr., C. Pimentel e M. M. Vasconcelos, "Substituição homofônica ótima com restrição", XX Simpósio Brasileiro de Telecomunicações, págs. 273 - 277, Rio de Janeiro, Brasil, 05-08 de outubro de 2003.

[36] B. Ryabko and A. Fionov, "Efficient Homophonic Coding", *IEEE Trans. on Info. Theory*, vol.45, no.6, pp.2083-2091, Sept. 1999.

[37] M. Hoshi and T.S. Han, "Interval Algorithm for Homophonic Coding", *IEEE Trans. on Info. Theory*, vol.47, no.3, pp.1021-1031, March 2001.

[38] V. C. da Rocha Jr. and C. Pimentel, "Optimum binary-constrained homophonic coding", *VII International Symposium on Communication Theory and Applications*, 13 - 18 July 2003, Ambleside, England, pp. 64-69.

[39] A. Sahai, "Evaluating channels for control: capacity reconsidered", *Proceedings of the American Control Conference*, Chicago, Illinois, USA, pp.2358-2362, June 2000.

[40] V. C. da Rocha, "Binary source coding of certain sources with a dyadic probability distributuion", *International Symposium on Information Theory and its Applications*, Parma,Italy, 10-13 October 2004.

APÊNDICE A

Alguns conceitos de teoria da informação

A.1 Introdução

Em 1948 Shannon tratou a comunicação com o uso de fontes, codificadores de fonte, codificadores de canal, assim como os decodificadores de fonte e de canal. Embora tal formalização pareça óbvia nos tempos atuais, não era assim há quase sessenta anos. Além disso, Shannon viu que canais e fontes poderiam e deveriam ser descritos usando as noções de entropia e entropia condicional. Ele foi eloqüente sobre o uso de tais noções tanto pela sua caracterização por meio de axiomas intuitivos quanto pela apresentação de teoremas de codificação precisos. Além disso, ele indicou o quanto conceitos tão explícitos, operacionalmente significativos como o conteúdo de informação de uma fonte ou a capacidade de informação de um canal, podem ser identificados usando entropia e a maximização de funções envolvendo a entropia [1]. Sem dúvida alguma, o impacto provocado pelo trabalho de Shannon [1] nas telecomunicações tem sido imenso sem contar na relação que a Teoria da Informação tem com várias outras áreas, como por exemplo: Física, Economia, Teoria da Comunicação, Estatística, Probabilidade e Ciência da Computação. Este apêndice trata de alguns dos conceitos de Teoria da Informação introduzidos por Shannon em [2], conceitos esses necessários para a compreensão das técnicas abordadas no texto. Um tratamento mais abrangente da Teoria da Informação encontra-se, por exemplo, nas referências [3] - [7]*.

*Boa parte do material apresentado neste capítulo foi baseada nas notas de aula utilizadas pelo Prof. Dr. James L. Massey no período de 1980 a 1998 no ETH Zurich.

A.2 A medida de informação de Hartley

Mesmo antes do importante trabalho de Shannon [2], Hartley [8] já havia reconhecido alguns aspectos relacionados à informação. Talvez o mais importante tenha sido o fato de perceber que a recepção de um símbolo apenas proporciona informação se existir outras possibilidades de valores para ele além daquele que foi recebido, em outras palavras, um símbolo fornece informação, apenas se for o valor de uma **variável aleatória** [9,pp. 72-73]. A partir daí, Hartley propôs uma medida quantitativa baseada no seguinte raciocínio: Considere um símbolo com D possíveis valores. A informação fornecida por n desses símbolos é dada por n vezes a quantidade de informação fornecida por um desses símbolos, uma vez que existem D^n possíveis valores para os n símbolos, $\log(D^n) = n\log(D)$ seria a medida apropriada de informação, na qual a base selecionada para o logaritmo define a unidade de informação. Deste modo, pode-se expressar a medida da quantidade de informação de Hartley, proporcionada pela observação de uma variável aleatória discreta X, como

$$I(X) = \log_b L, \tag{A.1}$$

na qual L é o número de possíveis valores de X.

Quando $b = 2$ em (A.1), a unidade de informação de Hartley é denominada "*bit*" (tal nomenclatura, sugerida por John Tukey, passou a ser usada a partir do trabalho de Shannon [2]). Assim, quando $L = 2^n$, $I(X) = n$ *bits* de informação.

A medida de informação de Hartley proporciona resposta correta para muitos problemas técnicos, porém observa-se que a medida de informação proposta por Hartley considera os eventos equiprováveis, deixando assim uma lacuna que impede seu uso geral e que foi preenchida anos mais tarde por Shannon [2].

A.3 A medida de informação de Shannon

Em 1948, vinte anos após o trabalho de Hartley [8], Shannon apresentou seu revolucionário trabalho [2] no qual introduzia toda uma nova teoria, incluindo uma nova medida de informação. Shannon, evidentemente, encontrou algo que Hartley não havia percebido e que era essencial para a aplicação geral da teoria. Ele percebeu que diferentes valores da variável aleatória X têm diferentes probabilidades, fornecendo, portanto, mais ou menos informação. A medida de informação proposta por Shannon pode ser vista como uma média ponderada

da medida de informação proposta por Hartley. Tal medida de informação foi denominada Entropia e é definida formalmente a seguir.

Sendo P_X a distribuição de probabilidade de uma variável aleatória discreta X, então a *entropia (ou incerteza)* de X é definida como:

Definição 7 *(**Entropia**): A entropia (ou incerteza) de uma variável aleatória discreta X é a quantidade*

$$H(X) = -\sum_{x \in supp(P_X)} P_X(x) \log_b P_X(x), \tag{A.2}$$

na qual $supp(P_X)$ é o conjunto dos valores não nulos de P_X.

No caso de valores nulos, pode-se considerar o fato que,

$$\lim_{p \to 0_+} p \log p = 0. \tag{A.3}$$

□

Neste capítulo, **log** é considerado como logaritmo na base dois. A seguir, o conceito de entropia será ilustrado por meio de alguns exemplos.

Exemplo 18 *Suponha que a variável aleatória discreta X possui dois valores, x_1 e x_2, com $P_X(x_1) = 0,5$ e $P_X(x_2) = 0,5$. Deste modo a partir de (A.2) chega-se que a entropia é $H(X) = -(0,5)(-1) - (0,5)(-1) = 1$.*

□

Exemplo 19 *Considere uma variável aleatória discreta X cujos valores x_1 e x_2 tenham probabilidades $P_X(x_1) = 0,9688$ e $P_X(x_2) = 0,0313$, respectivamente, a entropia, neste caso, é $H(X) = -(0,96875)(-0,0444) - (0,03125)(-4,9977) \approx 0,20$.*

□

Exemplo 20 *Seja a variável aleatória discreta X com dois possíveis valores x_1 e x_2 tais que $P_X(x_1) = 1$ e $P_X(x_2) = 0$. Usando a convenção $0 \log(0) = 0$, a entropia é 0.*

□

O *Exemplo 1*, no qual x_1 e x_2 são resultados equiprováveis, indicam grande incerteza. Já o *Exemplo 2*, no qual x_1 é 30 vezes mais provável de ocorrer que x_2, observa-se uma pequena incerteza. Finalmente, no *Exemplo 3* o resultado é totalmente previsível, uma vez que x_1 ocorre com probabilidade 1.

Considerando um vetor aleatório dado por $X = [Y, Z]$, define-se a entropia de um vetor aleatório como indicado a seguir.

Definição 8 ***(Entropia de vetores aleatórios)***

$$H(XY) = -\sum_{(x,y)\in supp(P_{XY})} P_{XY}(x,y)\log P_{XY}(x,y), \tag{A.4}$$

□

Exemplo 21 *Considere que X possui apenas dois valores, x_1 e x_2, e que $P_X(x_1) = p$ e $P_X(x_2) = 1 - p$. Então a incerteza de X em bits, tal que $0 < p < 1$, é dada por*

$$h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{(1-p)}. \tag{A.5}$$

A expressão (A.5) ocorre com tamanha freqüência em Teoria da Informação que recebe uma nomenclatura especial: ***entropia binária****, sendo denotada por $h(p)$. O gráfico de $h(p)$ é mostrado na Figura A.1.*

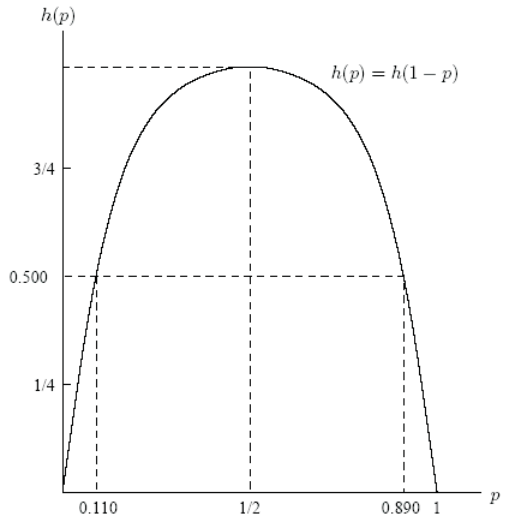


Figura A.1: Gráfico da entropia binária [7].

Observe que, se X representar a saída de uma fonte binária, quando $p = 0$ ou $p = 1$, esta fonte não gera informação. A quantidade média máxima de informação proporcionada

por cada símbolo de uma fonte binária é $\log 2$*, ou* 1 *bit, o que ocorre, se e só se,* 0 *e* 1 *forem equiprováveis.*

□

A.4 Algumas propriedades da entropia

A desigualdade (A.6), a seguir, é tão utilizada em Teoria da Informação (TI) que é denominada *desigualdade TI.*

Desigualdade da Teoria da Informação: Para um número real positivo r,

$$\log r \leq (r-1)\log e \tag{A.6}$$

com igualdade, se e só se, $r = 1$.

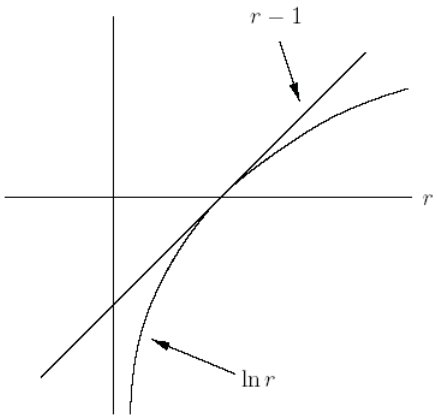


Figura A.2: Representação gráfica de $\ln(r)$ *e de* $r-1$ *[7]*

Lema 2 *Se* $p_1, p_2, ..., p_N$ *e* $q_1, q_2, ..., q_N$ *são números não negativos que satisfazem as condições* $\sum_{i=1}^{N} p_n = 1$ *e* $\sum_{i=1}^{N} q_n = 1$*, então*

$$-\sum_{i=1}^{N} p_i \log(p_i) \leq -\sum_{i=1}^{N} p_i \log(q_i), \tag{A.7}$$

com igualdade, se e só se, $p_i = q_i, \forall i$.

Demonstração:

Fazendo $r = q_i/p_i$ em (A.6), chega-se a

$$\log(q_i/p_i) \leq [(q_i/p_i) - 1]\log e, \tag{A.8}$$

com igualdade, se e só se, $q_i = p_i$. Tal fato é verdade para todo $i = 1, 2, ..., N$. Assim, multiplicando ambos os lados de (A.8) por p_i e somando sobre i, tem-se

$$\sum_{i=1}^{N} p_i \log(q_i/p_i) \leq \sum_{i=1}^{N} (q_i - p_i) \log e = \left[\sum_{i=1}^{N} q_i - \sum_{i=1}^{N} p_i \right] \log e = (1-1) \log e = 0,$$

com igualdade, se e só se, $p_i = q_i, \forall i$. Então

$$\sum_{i=1}^{N} p_i \log(q_i) - \sum_{i=1}^{N} p_i \log(p_i) \leq 0$$
$$- \sum_{i=1}^{N} p_i \log(p_i) \leq - \sum_{i=1}^{N} p_i \log(q_i)$$

que é o resultado esperado. ■

Como dito anteriormente, a unidade na qual a entropia é medida depende da base do logaritmo usado para calculá-la. Se o logaritmo na base 2 é usado, a unidade é o *bit*, se for usada a base natural (base e) a unidade é a unidade *natural*, às vezes denotada por *nat*.

Fazer a conversão para uma unidade diferente é simples, basta aplicar a relação $\log_b x = \log_a x \log_b a$. A aplicação da regra de mudança de base do logaritmo na função entropia dá origem ao seguinte lema, no qual $H_s(X)$ denota entropia na base s.

Lema 3

$$H_b(X) = (\log_b a) H_a(X).$$

Teorema 1 *Se uma variável aleatória discreta X tem L possíveis valores, então*

$$0 \leq H(X) \leq \log L, \tag{A.9}$$

com igualdade à esquerda, se e só se, $P_X(x) = 1$ para algum valor de x, e com igualdade à direita, se e só se, $P_X(x) = 1/L, \forall x$.

Demonstração:

Parte 1: $0 \leq H(X)$

Se $x \in supp(P_X)$, i.e., se $P_X(x) > 0$, então

$$-P_X(x) \log P_X(x) \begin{cases} = 0 & se \quad P_X(x) = 1 \\ > 0 & se \quad 0 < P_X(x) < 1 \end{cases}$$

Assim, vê-se imediatamente de (A.2) que $H(X) = 0$, se e só se, $P_X(x) = 1\ \forall x \in supp(P_X)$, mas é claro que existe apenas um x neste caso.

Parte 2: $H(X) \leq \log L$

Considere a quantidade

$$\begin{aligned} H(X) - logL &= \left[- \sum_{x \in supp(P_X)} P_X(x) \log P_X(x) \right] - \log L \\ &= \sum_{x \in supp(P_X)} P_X(x) \left[\log \frac{1}{P_X(x)} - \log L \right] \\ &= \sum_{x \in supp(P_X)} P_X(x) \left[\log \frac{1}{L \cdot P_X(x)} \right]. \end{aligned}$$

Aplicando a desigualdade TI (A.6), obtém-se

$$\begin{aligned} H(X) - \log L &\leq \sum_{x \in supp(P_X)} P_X(x) \left[\frac{1}{L \cdot P_X(x)} - 1 \right] \log e \\ &= \left[\sum_{x \in supp(P_X)} \frac{1}{L} - \sum_{x \in supp(P_X)} P_X(x) \right] \log e \\ &\leq (1 - 1) \log e = 0, \end{aligned}$$

na qual, pela condição de igualdade na expressão (A.6), tem-se que a igualdade ocorre, se e só se, $L \cdot P_X(x) = 1, \forall x \in supp(P_X)$, o que é verdade, se e só se, $P_X(x) = 1/L$ para todos os L valores de X, i.e., quando todos os valores de X forem equiprováveis.

■

Definição 9 *A incerteza condicional (ou entropia condicional) de uma variável aleatória discreta X, dado a ocorrência de um evento $Y = y$, é a quantidade*

$$H(X|Y = y) = - \sum_{x \in supp(P_{X|Y}(.|y))} P_{X|Y}(x|y) \log P_{X|Y}(x|y). \tag{A.10}$$

□

Das similaridades matemáticas entre as definições (A.2) e (A.10) de $H(X)$ e $H(X|Y = y)$, respectivamente, pode-se deduzir imediatamente o seguinte resultado.

Corolário 3 *Se uma variável aleatória discreta X tem L possíveis valores, então*

$$0 \leq H(X|Y = y) \leq \log L, \tag{A.11}$$

com igualdade à esquerda, se e só se, $P_{X|Y}(x|y) = 1$ para algum valor de x, e com igualdade à direita, se e só se, $P_{X|Y}(x|y) = 1/L, \forall x$ (Note que y é um valor fixo neste corolário).

□

Quando se fala de "incerteza de X dado Y" se quer dizer a incerteza condicional de X dado um evento $Y = y$, calculada a média sobre todos os valores y de Y. Assim, resulta a seguinte expressão.

Definição 10 *A incerteza condicional (ou entropia condicional) da variável aleatória discreta X, dada a variável aleatória discreta Y, é dada por*

$$H(X|Y) = -\sum_{y \in supp(P_Y)} P_Y(y) H(X|Y = y). \tag{A.12}$$

□

O resultado a seguir é uma conseqüência direta de (A.12).

Corolário 4 *Se uma variável aleatória discreta X tem L possíveis valores, então*

$$0 \leq H(X|Y) \leq \log L, \tag{A.13}$$

com igualdade à esquerda, se e só se, para todo $y \in supp(P_Y), P_{XY}(x|y) = 1$ para algum valor de x, e com igualdade à direita, se e só se, para todo $y \in supp(P_Y), P_{X|Y}(x|y) = 1/L, \forall x$.

□

Com (A.10) em (A.12) chega-se a

$$H(X|Y) = -\sum_{(x,y) \in supp_{(P_{XY})}} P_{XY}(x, y) \log P_{X|Y}(x|y). \tag{A.14}$$

A seguir, a última das definições de incerteza para variáveis aleatórias discretas é introduzida.

Definição 11 *A incerteza condicional (ou entropia condicional) de uma variável aleatória discreta X dada a variável aleatória discreta Y e dado que o evento Z=z ocorre, é a quantidade*

$$H(X|Y, Z = z) = -\sum_{(x,y) \in supp_{(P_{XY|Z}(.,.|z))}} P_{XY|Z}(x, y|z) \log P_{X|YZ}(x|y, z). \tag{A.15}$$

De modo análogo a (A.14) segue-se

$$H(X|Y,Z) = -\sum_{z \in supp_{(P_Z)}} P_Z(z) H(X|Y, Z=z). \tag{A.16}$$

As equações (A.15) e (A.16) proporcionam, com freqüência, o modo mais conveniente de se calcular $H(X|Y,Z)$.

Teorema 2 *Para quaisquer duas variáveis aleatórias discretas X e Y,*

$$H(X|Y) \leq H(X)$$

com igualdade, se e só se, X e Y são variáveis aleatórias discretas independentes.

□

Demonstração: Vide [7, p.15]

■

Observa-se que (A.14) e (A.15) diferem apenas no fato que as distribuições de probabilidade na última são condicionadas também ao evento $Z = z$. Desta forma, devido a essa similaridade matemática chega-se ao seguinte corolário.

Corolário 5 *Para quaisquer três variáveis aleatórias discretas X, Y e Z*

$$H(X|Y, Z=z) \leq H(X|Z=z), \tag{A.17}$$

com igualdade, se e só se, $P_{XY|Z}(x,y|z) = P_{X|Z}(x|z)P_{Y|Z}(y|z), \forall x, y$ (Note que z é um valor fixo de Z neste corolário.)

□

Multiplicando ambos os lados da desigualdade (A.17) por $P_Z(z)$ e somando sobre todos os $z \in supp(P_Z)$, obtém-se a próxima desigualdade, que relaciona várias incertezas e que mais uma vez mostra que condicionar nunca aumenta a incerteza.

Corolário 6 *Para quaisquer três variáveis aleatórias discretas X, Y e Z*

$$H(X|YZ) \leq H(X|Z), \tag{A.18}$$

com igualdade, se e só se, $\forall z \in supp(P_Z)$, a relação

$$P_{XY|Z}(x,y|z) = P_{X|Z}(x|z)P_{Y|Z}(y|z),$$

for verdadeira $\forall x, y$ *(ou equivalentemente, se e só se,* X *e* Y *são estatisticamente independentes quando condicionadas ao conhecimento de Z).*

□

Das desigualdades (A.17) e (A.18) pode-se concluir que condicionar variáveis aleatórias nunca pode aumentar a incerteza.[†]

A regra da cadeia para incerteza

Seja $[X_1, X_2, \ldots, X_N]$ um vetor aleatório discreto cujos N componentes são variáveis aleatórias discretas.

Utilizando a regra de multiplicação para distribuições de probabilidade como

$$\begin{aligned} H(X_1X_2\ldots X_N) = \quad & E[-\log P_{X_1}(X_1)P_{X_2|X_1}(X_2|X_1)\ldots \\ & P_{X_N|X_1\ldots X_{N-1}}(X_N|X_1\ldots X_{N-1})].^{\ddagger} \end{aligned} \tag{A.19}$$

A identidade (A.19) pode ser escrita de forma mais compacta como

$$\begin{aligned} H(X_1X_2\ldots X_N) &= E\left[-\log \prod_{n=1}^{N} P_{X_n|X_1\ldots X_{n-1}}(X_n|X_1,\ldots,X_{n-1})\right] \\ &= \sum_{n=1}^{N} E\left[-\log P_{X_n|X_1\ldots X_{n-1}}(X_n|X_1,\ldots,X_{n-1})\right] \\ &= \sum_{n=1}^{N} H\left(X_n|X_1\ldots X_{n-1}\right). \end{aligned} \tag{A.20}$$

Numa maneira menos compacta, porém mais fácil de ler, a expansão (A.20) pode ser reescrita como

$$H(X_1X_2\ldots X_N) = H(X_1) + H(X_2|X_1) + \cdots + H(X_N|X_1\ldots X_{N-1}). \tag{A.21}$$

A identidade (A.21) é denominada algumas vezes **regra da cadeia para a incerteza**. Do modo como se chegou a (A.21) fica claro que a ordem das variáveis aleatórias em $H(X_1X_2\ldots X_N)$ é arbitrária. Assim, por exemplo, $H(XYZ)$ pode ser expandido de seis diferentes formas:

[†]Note, porém, que condicionar a um evento pode aumentar a incerteza, i.e., $H(X|Y=y)$ pode ser maior que $H(X)$. Vide, por exemplo, [7,p.16].

$$\begin{aligned} H(XYZ) &= H(X) + H(Y|X) + H(Z|XY) \\ &= H(X) + H(Z|X) + H(Y|XZ) \\ &= H(Y) + H(X|Y) + H(Z|XY) \\ &= H(Y) + H(Z|Y) + H(X|YZ) \\ &= H(Z) + H(X|Z) + H(Y|XZ) \\ &= H(Z) + H(Y|Z) + H(X|YZ). \end{aligned}$$

De forma análoga a (A.21), obtém-se

$$\begin{aligned} H(X_1X_2\ldots X_N|Y=y) &= H(X_1|Y=y) + H(X_2|X_1, Y=y) \\ &\quad + \cdots + H(X_N|X_1\ldots X_{N-1}, Y=y). \end{aligned}$$

$$\begin{aligned} H(X_1X_2\ldots X_N|Y) &= H(X_1|Y) + H(X_2|X_1Y) \\ &\quad + \cdots + H(X_N|X_1\ldots X_{N-1}Y). \end{aligned}$$

e, finalmente,

$$\begin{aligned} H(X_1X_2\ldots X_N|Y, Z=z) &= H(X_1|Z=z) + H(X_2|X_1Y, Z=z) \\ &\quad + \cdots + H(X_N|X_1\ldots X_{N-1}Y, Z=z). \end{aligned}$$

Mais uma vez chama-se atenção para o fato que a ordem das variáveis aleatórias componentes $X_1, X_2, \ldots, X_N$ nas expansões mostradas é inteiramente arbitrária. Cada uma dessas incertezas condicionais pode ser expandida de $N!$ maneiras correspondentes aos $N!$ diferentes ordenamentos dessas variáveis aleatórias.

A.5 Codificação eficiente da informação

Nas seções A.3 e A.4 foram introduzidas, respectivamente, a medida de informação de Shannon e algumas propriedades interessantes dela. Usando tais informações mostra-se que respostas para problemas relacionados à transmissão e armazenamento de informação podem ser expressos, de fato, em termos da medida de informação de Shannon, em particular, abordada-se o problema da codificação digital da fonte de informação em uma seqüência de símbolos de um dado alfabeto. Além disso, alguns métodos eficientes de codificação são revistos.

A Figura A.3 ilustra o processo de codificação de fonte. Note que o canal é considerado sem ruído. Na presença de ruído também é necessário o uso de códigos de canal [10], os quais não são abordados aqui.

Figura A.3: Sistema de codificação sem ruído.

A.5.1 Codificação de uma única variável aleatória

Considere a situação conceitual ilustrada na Figura A.4 na qual uma única variável aleatória U é codificada em dígitos D-ários.

Figura A.4: Técnica de codificação de comprimento variável.

Mais precisamente, para as quantidades mostradas na Figura A.4:

1. U é uma variável aleatória com valores no alfabeto $\{u_1, u_2, \ldots, u_K\}$.
2. Cada X_i recebe valores do alfabeto D-ário, representado geralmente por $\{0, 1, 2, \ldots, D-1\}$.
3. W é uma variável aleatória, i.e., os valores da variável aleatória $z_i = [X_{i1}X_{i2}\ldots X_{iW}]$ são seqüências D- árias com comprimento variável.

Definição 12 ***(Códigos)*** *Seja U a fonte cujo alfabeto é dado por $U = \{u_1, u_2, \ldots, u_K\}$. Então um código é definido como o mapeamento de todas as possíveis seqüências dos símbolos de U em seqüências de um outro alfabeto $X = \{0, 1, \ldots, D-1\}$. Assim, U é chamado alfabeto da fonte e X alfabeto do código.*

A partir da definição geral dada (Definição 12) algumas propriedades adicionais dos códigos serão consideradas resultando nas classes de códigos introduzidas a seguir.

Um código de fonte pode ser classificado como:

- um **código não-singular** se todas as palavras-código são distintas, i.e.,

$$u_i \neq u_j \Rightarrow z_i \neq z_j.$$

- um **código de bloco** de comprimento n se todas as palavras-código têm comprimento fixo n.

Exemplo 22 *Considere o alfabeto de fonte* $U = \{u_1, u_2, u_3, u_4\}$ *e o código binário* $X = \{0, 1\}$. *A Tabela A.1 mostra dois possíveis códigos de fonte.*

Tabela A.1: Exemplos de códigos binários.

Símbolos	Código A	Código B
u_1	00	0
u_2	01	11
u_3	10	00
u_4	11	010

O código A é um exemplo de código de bloco com $n = 2$ *e o B de um código não-singular.*

□

Do exemplo anterior nota-se que para fins práticos poderia haver problema na decodificação de uma seqüência codificada usando o código B, pois apesar de todas as suas palavras-código serem distintas numa seqüência em que ocorre, por exemplo, 00 a mesma poderia ser decodificada tanto como 'u_1u_1' quanto como 'u_3'. Nota-se assim que o código B é não-singular, porém considerando seqüências de palavras-código ele se torna singular. Desta forma, uma condição ainda mais restritiva que a não-singularidade deve ser definida a fim de se evitar dubiedades no processo de decodificação.

Definição 13 ***(n-ésima extensão de um código)*** *A n-ésima extensão de um código de bloco que mapeia os símbolos* u_i *em palavras-código* z_i *é o código de bloco que mapeia as seqüências de símbolos da fonte* $(u_{i1}, u_{i2}, \ldots, u_{in})$ *em seqüências de palavras-código* $(z_{i1}, z_{i2}, \ldots, z_{in})$.

□

Definição 14 ***(Códigos unicamente decodificáveis)*** *Um código é dito unicamente decodificável, se e só se, sua n-ésima extensão é não-singular para qualquer valor finito de n.*

□

Exemplo 23 *Considere o alfabeto de fonte* $U = \{u_1, u_2, u_3, u_4\}$ *e o código binário* $X = \{0, 1\}$. *A Tabela A.2 mostra três possíveis códigos de fonte.*

Nota-se que:

Tabela A.2: Exemplos de códigos binários.

Símbolos	Código A	Código B	Código C
u_1	0	0	00
u_2	11	11	01
u_3	00	00	10
u_4	11	010	11

- *O código A é singular, uma vez que $z_2 = z_4 = 11$*
- *O código B é não-singular, mas NÃO é unicamente decodificável, já que* 00 *pode ser decodificado tanto como u_3 ou u_1u_1, i.e., $z_3 = z_1z_1 = 00$ na qual $z_1z_1 = 00$ é a segunda extensão do código.*
- *O código C é um código de bloco não-singular de comprimento 2 e é, portanto, unicamente decodificável.*

□

Definição 15 ***(Códigos instantâneos)*** *Um código unicamente decodificável é dito instantâneo se é possível decodificar cada mensagem formada por uma seqüência de símbolos codificados da fonte, de tal modo que cada palavra-código é decodificada sem que seja necessário observar palavras-código posteriores.*

□

Observa-se, assim, que um código para ser prático deve ser pelo menos unicamente decodificável, a fim que se evitem dubiedades no processo de decodificação. Os códigos instantâneos formam uma subclasse dos unicamente decodificáveis e possuem propriedades úteis. Um código instantâneo permite uma decodificação imediata, uma vez que não é necessário para isto o armazenamento no receptor dos símbolos anteriores e correntes a fim de se fazer a decodificação corretamente.

Exemplo 24 *Considere a seguir três códigos binários para a fonte $U = \{u_1, u_2, u_3, u_4\}$:*

Observa-se que os códigos A, B e C são unicamente decodificáveis. Mas eles são também instantâneos?

Considere a seqüência de símbolos codificada usando o código A.

Tabela A.3: Exemplos de códigos binários.

Fonte	Código A	Código B	Código C
u_1	0	0	0
u_2	10	01	01
u_3	110	011	011
u_4	1110	0111	111

$$\overline{0}\underline{10}\overline{1110}\underline{110}\overline{0}\underline{10}\overline{0}\underline{0}\overline{10} \Rightarrow u_1u_2u_4u_3u_1u_2u_1u_1u_2$$

As barras sobre ou sob as seqüências de $0s$ *e* $1s$ *indicam palavras-código do código* A*. Nota-se que o "*0*" funciona como indicador de que uma palavra-código acabou de ser recebida, desta forma o código* A *é um código instantâneo.*

Agora considere uma seqüência codificada pelo código B*.*

$$\overline{011}\underline{01}\overline{0111}\underline{0}\overline{0} \Rightarrow u_3u_2u_4u_1u_1$$

Neste código o símbolo "0*" também funciona como um separador, porém diferentemente do código* A*, o "*0*" indica o início de uma nova palavra-código, desta forma é necessário esperar o início da próxima palavra a fim de proceder à decodificação, assim o código* B*, não é instantâneo.*

Por fim, analisando uma seqüência codificada usando o código C*:*

$$011111...$$

Ainda não é possível decodificar esta seqüência. De fato antes que se receba um 0 *ou EOF (end-of-file) a seqüência não pode ser decodificada, pois não é possível saber se a primeira palavra-código é* $0, 01$ *ou* 011*. Além disso, assim que for possível iniciar o processo de decodificação da seqüência, tal decodificação não é de modo algum tão direta quanto nos casos dos códigos* A *e* B*. Não obstante, este código é unicamente decodificável uma vez que o "*0*" age ainda como separador.*

□

Do Exemplo 24 percebe-se porque códigos como o código A são chamados instantâneos, claramente porque decodificar é um processo rápido e fácil (i.e., instantâneo!). Entretanto, a

praticidade desses códigos encontra-se na **condição de prefixo** que permite que tais códigos sejam analisados e projetados eficientemente.

Definição 16 ***(Prefixo de um código)*** *Seja $z_i = x_{i1}x_{i2}\ldots x_{in}$ uma palavra-código de comprimento n. Diz-se que $z_i^{'}$ é um prefixo de z_i se $z_i^{'} = x_{i1}x_{i2}...x_{im}$, na qual $m < n$*[§]*.*

□

Definição 17 ***(Condição de prefixo)*** *Uma condição suficiente e necessária para um código ser instantâneo é que nenhuma palavra-código do código seja prefixo de uma outra palavra-código deste código.*

□

Exemplo 25 *Considere novamente os códigos do Exemplo 24. Agora é possível usando a condição 17 dizer se tais códigos são ou não instantâneos.*

Código A *é instantâneo pois nenhuma palavra-código deste código é prefixo de uma outra palavra-código mais longa deste mesmo código.*

Código B *não é instantâneo pois $z_1 = 0$ é prefixo de $z_2 = 01$, $z_2 = 01$ é prefixo de $z_3 = 011$, etc. Porém este código é unicamente decodificável uma vez que "0" age como separador.*

Código C *não é instantâneo pois, assim como no código B, $z_1 = 0$ é prefixo de $z_2 = 01$, $z_2 = 01$ é prefixo de $z_3 = 011$, porém tal código é unicamente decodificável.*

□

A Figura A.5 mostra como cada uma das classes de códigos abordada aqui se relaciona.

Propriedades dos códigos instantâneos

Propriedade 1 Facilidade em provar se um código é instantâneo por meio da verificação da condição de prefixo.

Propriedade 2 O código livre de prefixo permite um projeto sistemático de códigos instantâneos baseado na especificação dos comprimentos das palavras-código.

Propriedade 3 A decodificação baseada em árvore é rápida e não requer memória de armazenamento.

[§]Note que uma palavra-código é prefixo de si mesma.

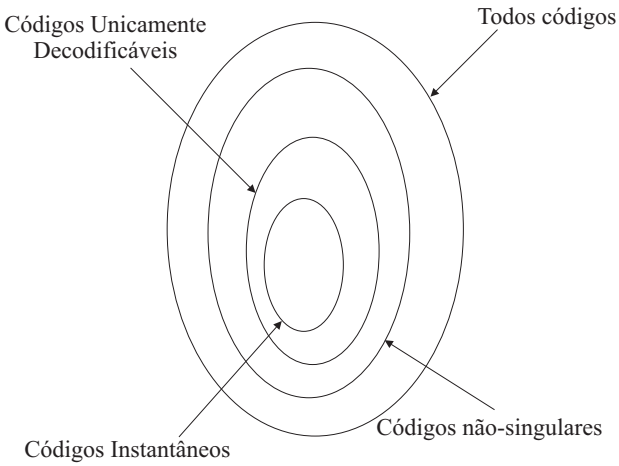


Figura A.5: Classes de códigos.

Tabela A.4: Código A livre de prefixo e código B não instantâneo.

Símbolos	Código A
u_1	0
u_2	10
u_3	11

Símbolos	Código B
u_1	1
u_2	00
u_3	11

Propriedade 4 Códigos instantâneos são unicamente decodificáveis e como o comprimento de uma palavra-código é a principal consideração no projeto e seleção de códigos, não há vantagem em considerar a classe geral dos códigos unicamente decodificáveis que não são instantâneos[¶].

A.5.2 Representação de códigos usando árvores enraizadas

Exemplo 26 *Considere os códigos mostrados na Tabela A.4 e observe na Figura A.6 as árvores binárias correspondentes.*

□

Note que as palavras-código (representadas pelos círculos negros na ponta dos ramos) no caso dos códigos livre de prefixo, correspondem a todas a folhas, i.e., todos os círculos negros que representam as palavras-código se encontram em vértices finais das quais não saem outros ramos, diferentemente dos códigos que não são livres de prefixo, como é o caso do código B

[¶]Vide Teorema de McMillan (Proposição 8).

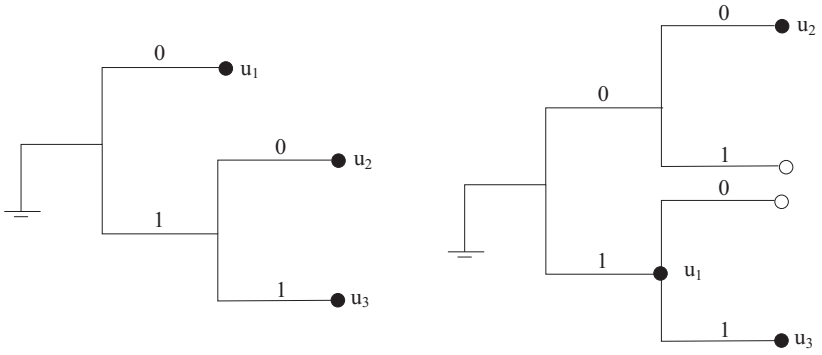


Figura A.6: Árvores binárias referentes aos códigos A e B do Tabela A.4.

da Tabela A.4. Neste tipo, existem palavras-código representadas nos nós intermediários da árvore.

A fim de fazer futuras considerações mais precisas, algumas definições são introduzidas.

Definição 18 *Uma árvore D-ária é definida com uma árvore enraizada finita (ou semi-finita) tal que D ramos saem de cada nó, inclusive do nó raiz.*

Cada um dos D ramos que saem de cada um dos nós deve receber um marcador diferente correspondendo aos símbolos D-ários do código, i.e., $0, 1, \ldots, D-1$.

Definição 19 *A árvore completa D-ária de comprimento N é a árvore D-ária com D^N folhas, cada uma delas distando N ramos do nó raiz.*

A Figura A.7 ilustra árvores D-árias mostrando uma árvore binária e uma árvore ternária.

Nota-se, portanto, que todo código D-ário livre de prefixo pode ser identificado por um conjunto de folhas em uma árvore D-ária, por outro lado, qualquer conjunto de folhas numa árvore D-ária define um código D-ário livre de prefixo.

Exemplo 27 *O código livre de prefixo $z_1 = [011]$, $z_2 = [10]$, $z_3 = [11]$ e $z_4 = [00]$ tem como árvore correspondente àquela ilustrada na Figura A.8.*

□

O resultado a seguir diz exatamente quando um dado conjunto de comprimentos de palavras-código pode formar um código D-ário livre de prefixo.

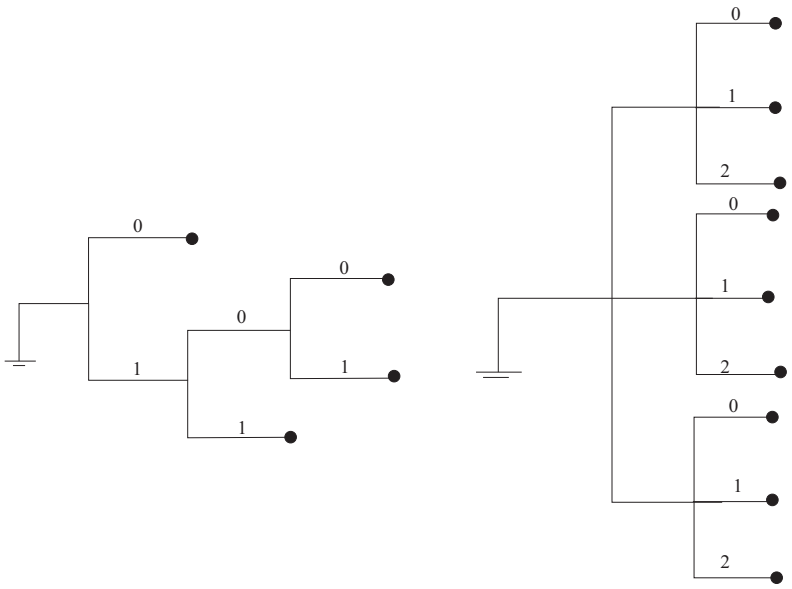


Figura A.7: Exemplo de uma árvore binária e uma árvore completa ternária de comprimento 2.

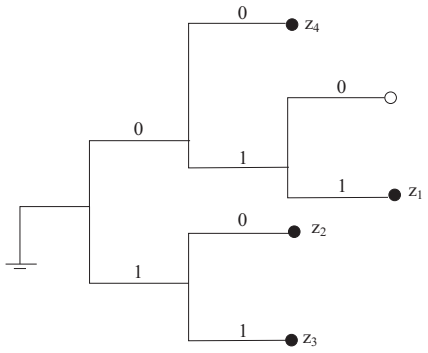


Figura A.8: Árvore D-ária para o código livre de prefixo $z_1 = [011]$, $z_2 = [10]$, $z_3 = [11]$ *e* $z_4 = [00]$.

Proposição 7 ***(Desigualdade de Kraft)*** *Existe um código D-ário livre de prefixo cujos comprimentos das palavras-código são inteiros positivos,* $l_1, l_2, l_3, ..., l_K$*, se e só se,*

$$\sum_{i=1}^{K} D^{-l_i} \leq 1. \tag{A.22}$$

Quando (A.22) é satisfeita com igualdade, o código livre de prefixo correspondente não possui folhas livres em sua árvore D-ária.

□

A desigualdade de Kraft proporciona uma condição necessária e suficiente para a existência de códigos livre de prefixo obedecendo a certo grupo de comprimentos de palavras-código, sendo precursora do teorema de McMillan (Proposição 8).

A prova da Proposição 8 pode ser vista em [12, p.57-59]. Tal prova consiste na verdade de um algoritmo para construção de um código D-ário livre de prefixo com palavras-código cujos comprimentos são $l_1, l_2, l_3, ..., l_K$, caso tal código exista. O algoritmo em questão é equivalente a construir a árvore partindo da raiz, associando a qualquer folha distante l_i ramos dela a palavra-código z_i, observando que as palavras-código mais curtas são selecionadas primeiro.

Pela condição de suficiência na Proposição 7 e como os códigos instantâneos são uma subclasse dos códigos unicamente decodificáveis, isto indica que um código unicamente decodificável pode ser construído com palavras-código de comprimentos $l_1, l_2, l_3, ..., l_K$ obedecendo (A.22). Porém, a prova da condição de necessidade não se aplica aos códigos unicamente decodificáveis. Na verdade, a parte "necessária" da desigualdade de Kraft sugere uma investigação das restrições sobre os comprimentos de palavras-código de códigos unicamente decodificáveis. Pelo Teorema de McMillan (Proposição 8), dado que os comprimentos das palavras-código obedecem a Desigualdade de Kraft (A.22) então é possível construir um código unicamente decodificável, podendo este ser livre de prefixo ou não.

Proposição 8 ***(Teorema de McMillan)*** *Os comprimentos das palavras-código de qualquer código unicamente decodificável devem obedecer a Desigualdade de Kraft.*

$$\sum_{i=1}^{K} D^{-l_i} \leq 1. \tag{A.23}$$

Inversamente, dado um conjunto de comprimentos de palavras-código que satisfazem esta desigualdade, então existe um código unicamente decodificável com tais comprimentos.

□

Exemplo 28 *Construa um código binário livre de prefixo com comprimentos* $l_1 = 2, l_2 = 2, l_3 = 2, l_4 = 3, l_5 = 4$.

Como $\sum_{i=1}^{5} 2^{-l_i} = 1/4+1/4+1/4+1/8+1/16 = 15/16 < 1$, *sabe-se devido à Desigualdade de Kraft que um código livre de prefixo binário com palavras-código com tais comprimentos existe. A solução deste problema é indicada pela árvore da Figura A.9 e pelo código sugerido na Tabela A.5.*

□

Exemplo 29 *Construa um código binário livre de prefixo com comprimentos* $l_1 = 1, l_2 = 2, l_3 = 2, l_4 = 3, l_5 = 4$.

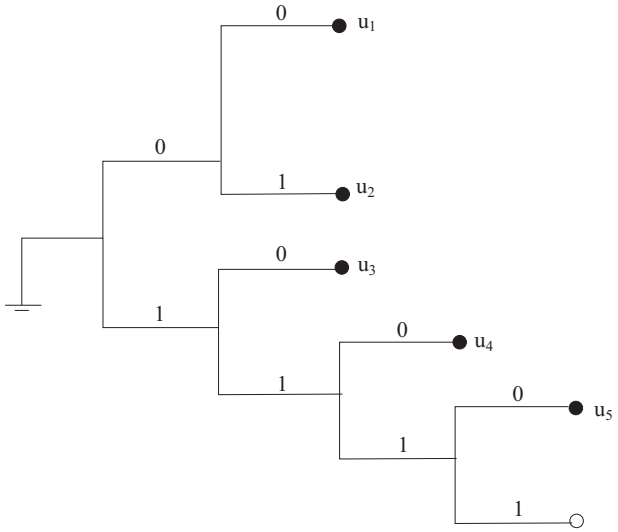


Figura A.9: Árvore binária para o código com comprimentos de palavras-código $l_1 = 2, l_2 = 2, l_3 = 2, l_4 = 3, l_5 = 4$.

Tabela A.5: Código associado ao exemplo 28.

Símbolos	Código
u_1	00
u_2	01
u_3	10
u_4	110
u_5	1110

Como $\sum_{i=1}^{5} 2^{-l_i} = 1/2+1/4+1/4+1/8+1/16 = 19/16 > 1$, *sabe-se devido à Desigualdade de Kraft que um código binário livre de prefixo binário, com tais comprimentos de palavras-código, não existe.*

□

Árvores enraizadas com probabilidades

Por uma árvore enraizada com probabilidades entende-se uma árvore enraizada com números não negativos (probabilidades) associados a cada vértice da árvore de modo que

1. à raiz é associado probabilidade 1, e

2. a probabilidade de um dado nó da árvore (incluindo a raiz) é dada pela soma das

probabilidades dos nós e/ou folhas de profundidade 1 pertencentes à sub-árvore que parte do nó em questão.

Note que aqui não há exigência que a árvore seja D-ária, i.e., que tenha o mesmo número de ramos partindo de cada nó.

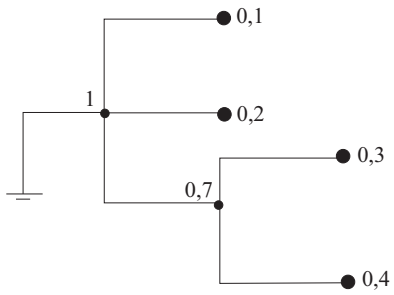


Figura A.10: Exemplo de uma árvore enraizada.

Note que numa árvore enraizada com probabilidades, a soma das probabilidades das folhas deve ser um.

Lema 4 ***(Lema do comprimento do caminho)*** *Numa árvore enraizada com probabilidades, a distância média das folhas ao nó raiz é igual à soma das probabilidades dos nós, incluindo o nó raiz.*

A probabilidade em cada um dos vértices da árvore enraizada pode ser vista como a **probabilidade de se alcançar o vértice por meio de um passeio aleatório em um único sentido** na árvore, começando na raiz e indo até alguma das folhas. Dado que se está num nó específico, a probabilidade condicional de se escolher o próximo ramo para se continuar o passeio aleatório é simplesmente a probabilidade do nó ou folha no fim do ramo, dividida pela probabilidade do nó no início do ramo. Observe que na árvore da Figura A.10 a probabilidade de se chegar às folhas com probabilidade 0,3 e 0,4, dado que se está no nó de probabilidade 0,7 é respectivamente, 3/7 e 4/7.

Suponha agora que a árvore enraizada tenha T folhas cujas probabilidades são dadas por $p_1, p_2, \ldots, p_T$. Define-se a entropia das folhas da árvore enraizada como

$$H_{folhas} = -\sum_{i:p_i \neq 0} p_i \log p_i. \tag{A.24}$$

Note que H_{folhas} pode ser considerada a entropia $H(U)$ de uma variável aleatória U cujos valores especificam a folha alcançada no passeio aleatório descrito anteriormente.

Suponha agora que tal árvore possui N nós e que as probabilidades deles sejam dadas por $P_1, P_2, \ldots, P_N$. Pelo lema do comprimento do caminho (Lema 4), o comprimento médio é dado por $P_1 + P_2 + \cdots + P_N$. A fim de definir a entropia de ramificação em cada um desses nós, considere que $q_{i1}, q_{i2}, \ldots, q_{iL_i}$ são as probabilidades dos nós e folhas no final dos L_i ramos partindo de um nó cuja probabilidade é P_i. Assim, a entropia de ramificação, H_i, nesse nó é dada por

$$H_i = -\sum_{j:q_{ij}\neq 0} \frac{q_{ij}}{P_i} \log \frac{q_{ij}}{P_i}, \tag{A.25}$$

na qual $\frac{q_{ij}}{Pi}$ é a probabilidade condicional de escolher o j-ésimo desses ramos como o próximo passo do passeio aleatório dado que se está no i-ésimo nó.

Exemplo 30 *Pela Figura A.10, $T = 4$ folhas e $N = 2$ nós, tendo como probabilidades das folhas $p_1 = 0,1; p_2 = 0,2; p_3 = 0,3$ e $p_4 = 0,4$ e probabilidade dos nós, $P_1 = 1$ e $P_2 = 0,7$.*

Assim,

$$H_{folhas} = -\sum_{i=1}^{4} p_i \log p_i = 1,846 \ bits.$$

Nota-se que $L_1 = 3; q_{11} = 0,1; q_{12} = 0,2; q_{13} = 0,7; P_1 = 1$. Assim,

$$H_1 = -0,1 \log 0,1 - 0,2 \log 0,2 - 0,7 \log 0,7 = 1,157 \ bits.$$

Para $L_2 = 2; q_{21} = 0,3; q_{22} = 0,4; P_2 = 0,7$,

$$H_2 = -\frac{3}{7} \log \frac{3}{7} - \frac{4}{7} \log \frac{4}{7} = h\left(\frac{3}{7}\right) = 0,985 \ bits.$$

□

Devido ao item (2.) da definição de árvore enraizada com probabilidades, nota-se que

$$P_i = \sum_{j=1}^{L_i} q_{ij}. \tag{A.26}$$

Usando o resultado em (A.26) juntamente com $\log(q_{ij}/P_i) = \log q_{ij} - \log P_i$ em (A.25), obtém-se o produto

$$P_i H_i = -\sum_{j:q_{ij}\neq 0} q_{ij} \log q_{ij} + P_i \log P_i, \tag{A.27}$$

o qual é usado para provar o seguinte resultado [7,p.31].

Teorema 3 ***(Teorema da entropia das folhas)*** *A entropia das folhas de uma árvore enraizada com probabilidades é dada pela soma (A.28) feita sobre todos os nós, incluindo o nó raiz, i.e.,*

$$H_{folhas} = \sum_{i=1}^{N} P_i H_i. \tag{A.28}$$

Exemplo 31 *(continuação Exemplo 30) Calculando H_{folhas} a partir de (A.28)*

$$H_{folhas} = (1) \cdot H_1 + (0,7) \cdot H_2 = 1,157 + (0,7) \cdot (0,985) = 1,846 \; bits$$

o que concorda com o resultado anteriormente obtido no Exemplo 30.

□

Cota inferior de E(W) para códigos livres de prefixo

Usando os resultados mostrados nesta seção chega-se a uma cota inferior fundamental de E(W), comprimento médio das palavras-código (A.35), para códigos D-ários livres de prefixo, para uma variável aleatória K-ária U.

Nesta seção também foi visto que códigos D-ários livre de prefixo definem árvores D-árias enraizadas em que cada palavra-código corresponde a uma folha da árvore. A distribuição de probabilidade P_U associa probabilidades às palavras-código e portanto, às folhas. Por convenção se associa probabilidade 0 a qualquer folha que não corresponde a uma palavra-código. Além disso, associa-se a todos os nós uma probabilidade igual à soma das probabilidades dos nós de profundidade 1 que pertencem à sub-árvore que partem de tal nó. Desta forma é criada uma árvore enraizada D-ária com probabilidades.

Exemplo 32 *Considere a distribuição de probabilidade da fonte binária discreta U, $P_U(u_1) = 0,1; P_U(u_2) = P_U(u_3) = P_U(u_4) = 0,3$ cujo código foi representado no Exemplo 27, resultando na árvore ilustrada a seguir.*

□

Para a árvore binária enraizada com probabilidade criada pela construção descrita há pouco, nota-se que

$$H_{folhas} = H(U), \tag{A.29}$$

i.e., a entropia das folhas é igual à incerteza da variável aleatória codificada. Além disso, como D ramos saem de cada nó, segue-se do Corolário 3 do Teorema 1 que a entropia dos ramos em cada um dos nós satisfaz

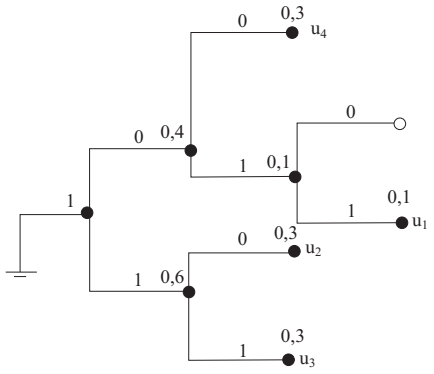


Figura A.11: Árvore enraizada binária representando o código livre de prefixo do Exemplo 27.

$$H_i \leq \log D, \tag{A.30}$$

com igualdade, se e só se, o próximo dígito do código toma quaisquer das D possibilidades com mesma probabilidade, dado que os dígitos anteriores são aqueles no caminho até o nó i. Usando (A.29) e (A.30) em (A.28) obtém-se,

$$H(U) \leq \log D \sum_{i=1}^{N} P_i. \tag{A.31}$$

Porém, pelo Lema do comprimento do caminho (Lema 4), o somatório à direta de (A.31) é a distância média das folhas, i.e., o comprimento médio das palavras-código, E(W). Desta forma está provada a seguinte cota.

Teorema 4 *O comprimento médio das palavras-código, $E(W)$, de um código D-ário livre de prefixo para uma variável aleatória K-ária U satisfaz*

$$E(W) \geq \frac{H(U)}{\log D}, \tag{A.32}$$

com igualdade, se e só se, o código é ótimo[‖] e a probabilidade de cada valor de U é uma potência negativa de D.

Considerando a cota inferior para $E(W)$ introduzida no Teorema 4, define-se a eficiência de um código.

Definição 20 ***(Eficiência do código)*** *A eficiência do código é dada por*

$$\eta = \frac{H(U)}{E(W)}, \tag{A.33}$$

[‖]no sentido de possuir o menor comprimento médio possível, i.e., um código compacto (Definição 22).

na qual se $H(U) = E(W)$ o código é 100% eficiente.

□

Como conseqüência da Definição 20, a redundância do código é definida como

Definição 21 ***(Redundância do código)*** *A redundância do código é dada por*

$$\rho = 1 - \frac{H(U)}{E(W)}. \tag{A.34}$$

A.5.3 Comprimento médio e códigos compactos

O comprimento médio da palavra-código, $E(W)$, é geralmente, usado como parâmetro de eficiência de um código de modo que quanto menor $E(W)$ melhor o código. Se $z_i = [x_{i1}, x_{i2}, \ldots, x_{il_i}]$ é uma palavra-código para u_i e, l_i é o comprimento desta palavra-código, então o comprimento médio das palavras-código é dado por

$$E(W) = \sum_{i=1}^{K} P_U(u_i) \cdot l_i. \tag{A.35}$$

□

Considerando um conjunto de possíveis códigos D-ários para a mesma fonte, é necessário que se faça uma escolha por meio da comparação do desempenho de tais possíveis códigos. Para propósitos de armazenamento e comunicação o principal critério usado é o **comprimento médio** (A.35) de um código, em que códigos com menor comprimento médio são preferidos.

Definição 22 ***(Códigos compactos)*** *Considere um código unicamente decodificável que mapeia os símbolos de uma fonte U em palavras-código de um alfabeto D-ário. O código é dito um código compacto se seu comprimento médio $E(W)$ for menor ou igual ao comprimento médio de todos os outros códigos unicamente decodificáveis para a mesma fonte e alfabeto de código.*

□

Exemplo 33 *Considere os códigos binários ilustrados na tabela abaixo. Qual deles é melhor usando o critério de comprimento médio?*

$E_A(W) = 2$ *bits/ símbolo e* $E_B(W) = (0,5) \cdot 1 + (0,1) \cdot 3 + (0,2) \cdot 3 + (0,2) \cdot 2 = 1,8$ *bits/ símbolo.*

Símbolos	$P_U(u_i)$	Código A	Código B
u_1	0,5	00	1
u_2	0,1	01	000
u_3	0,2	10	001
u_4	0,2	11	01

$E_B(W) < E_A(W)$, então o código B é melhor que o código A considerando o critério do menor comprimento médio, mas existe um outro código C para o qual $E_C(W) < E_B(W)$? Ou o código B é o código compacto para esta fonte? O quão pequeno pode ser o comprimento médio?

□

Códigos livre de prefixo Shannon-Fano

Nesta seção é revisto o primeiro teorema de Shannon para **fontes sem memória** ** e uma cota superior para $E(W)$ é reapresentada.

Pelo Teorema 4 nota-se que um código compacto é obtido quando $E(W) = \dfrac{H(U)}{\log D}$ o que ocorre quando todos os símbolos da fonte têm probabilidade da forma $P_U(u_i) = D^{-l_i}$, concluindo assim que neste caso, $l_i = \log_D \dfrac{1}{P_U(u_i)}$.

Considere agora o caso em que as probabilidades dos símbolos da fonte não são necessariamente da forma $P_U(u_i) = D^{-l_i}$. Como, $\log_D \dfrac{1}{P_U(u_i)}$ não é inteiro parece razoável escolher o menor inteiro maior que este valor para l_i a fim de se obter um código compacto, i.e.,

$$l_i = \left\lceil \log_D \frac{1}{P_U(u_i)} \right\rceil, \tag{A.36}$$

na qual x é um inteiro, tal que $x \leq \lceil x \rceil < x + 1$.

Então,

$$\log_D \frac{1}{P_U(u_i)} \leq l_i < \log_D \frac{1}{P_U(u_i)} + 1. \tag{A.37}$$

Inicialmente é verificado se os comprimentos das palavras-código escolhidos desta forma obedecem a Desigualdade de Kraft (A.22).

**Uma fonte D-ária discreta sem memória é uma fonte na qual os sucessivos símbolos por ela emitidos são estatisticamente independentes. Tal fonte é completamente descrita por seu alfabeto, $\{u_1, u_2, \ldots, u_K\}$, e por sua distribuição de probabilidade, $\{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

Tomando a exponencial na desigualdade à esquerda em (A.37),

$$\frac{1}{P_U(u_i)} \leq D^{l_i}$$

ou

$$P_U(u_i) \geq D^{-l_i}. \tag{A.38}$$

Somando (A.38) sobre todos os i,

$$1 \geq \sum_{i}^{K} D^{-l_i}. \tag{A.39}$$

Assim, de (A.39) percebe-se que escolhendo os comprimentos das palavras-código conforme (A.37) a Desigualdade de Kraft é obedecida e, portanto, tais comprimentos podem ser usados na construção de um código instantâneo.

Multiplicando ambos os lados de (A.37) e somando em i, chega-se a

$$H_D(U) \leq E(W) \leq H_D(U) + 1. \tag{A.40}$$

É importante notar que a equação (A.32) mostra uma cota inferior para $E(W)$ independente da técnica de codificação considerada, requerendo apenas que o código seja instantâneo. Já a expressão (A.40) foi obtida considerando a técnica de codificação definida em (A.37). Tal método de codificação é denominado código Shannon-Fano uma vez que foi introduzido implicitamente no trabalho de 1948 de Shannon [2], mas só mostrado explicitamente por Fano. Como (A.40) é válida para fontes sem memória então aplicando tal expressão para a **n-ésima extensão da fonte**[††],

$$H_D(U^n) \leq E_n(W) < H_D(U^n) + 1, \tag{A.41}$$

onde $E_n(W)$ representa o comprimento médio das palavras-código para a n-ésima extensão da fonte, desta forma

$$E_n(W) = \sum_{i=1}^{K^n} P(\upsilon_i)\lambda_i, \tag{A.42}$$

[††]Dada uma fonte D-ária discreta sem memória, U, a sua n-ésima extensão, U^n, é uma fonte D-ária discreta sem memória com K^n símbolos $\{\upsilon_1, \upsilon_2, \ldots, \upsilon_{K^n}\}$ na qual cada um desses símbolos corresponde a uma seqüência de comprimento n de símbolos u_i. A probabilidade de um símbolo de U^n é dada pelo produto das probabilidades dos símbolos u_i que formam υ_i.

na qual λ_i é o comprimento da palavra-código correspondente ao símbolo $\upsilon_i = (u_{i1}, u_{i2}, \ldots, u_{in})$ e $P(\upsilon_i)$ é a probabilidade de υ_i.

Assim, $E_n(W)$ é portanto o número médio de símbolos do código usados por um único símbolo da fonte U. Aplicando (A.2) na n-ésima extensão da fonte,

$$\begin{aligned} H_D(U^n) &= \sum_{i=1}^{K^n} P(\upsilon_i) \log \frac{1}{P(\upsilon_i)} \\ &= \sum_{i=1}^{K^n} P(\upsilon_i) \log \frac{1}{P_U(u_{i_1}) P_U(u_{i_2}) \ldots P_U(u_{i_n})} \\ &= \sum_{i=1}^{K^n} P(\upsilon_i) \log \frac{1}{P_U(u_{i_1})} + \sum_{i=1}^{K^n} P(\upsilon_i) \log \frac{1}{P_U(u_{i_2})} \\ &+ \cdots + \sum_{i=1}^{K^n} P(\upsilon_i) \log \frac{1}{P_U(u_{i_n})}. \end{aligned}$$

Logo,

$$H_D(U^n) = nH_D(U). \tag{A.43}$$

Assim, de (A.43) e (A.41) resulta

$$H_D(U) \leq \frac{E_n(W)}{n} < H_D(U) + \frac{1}{n}. \tag{A.44}$$

Percebe-se a partir de (A.44) que é possível fazer $\dfrac{E_n(W)}{n}$ tão próximo quanto se queira de $H_D(U)$ por meio da codificação de n-ésima extensão da fonte U em vez da codificação de U. Desta forma,

$$\lim_{n \to \infty} \frac{E_n(W)}{n} = H_D(U). \tag{A.45}$$

A expressão (A.44) é conhecida como o **primeiro teorema de Shannon** ou **teorema da codificação sem ruído**.

Exemplo 34 *Gerar um código instantâneo usando a técnica de codificação introduzida nesta seção e descrita por (A.37) para a fonte especificada na Tabela A.6.*

$$\begin{aligned} 0,58 &\leq l_1 < 0,58 + 1 = 1,58 \Rightarrow l_1 = 1 \\ 2,17 &\leq l_2 < 2,17 + 1 = 3,17 \Rightarrow l_2 = 3 \\ 3,17 &\leq l_3 < 3,17 + 1 = 4,17 \Rightarrow l_3 = 4. \end{aligned}$$

Tabela A.6: Fonte binária U discreta sem memória.

Símbolos	$P_U(u_i)$	$\log(1/P_U(u_i))$
u_1	2/3	0,58
u_2	2/9	2,17
u_3	1/9	3,17

Tabela A.7: Código Shannon-Fano para a fonte binária discreta sem memória U com distribuição de probabilidade $P_U(u_1) = 2/3, P_U(u_2) = 2/9$ e $P_U(u_3) = 1/9$.

Símbolos	Código A
u_1	0
u_2	100
u_3	1010

Assim, um código livre de prefixo com palavras-código cujos comprimentos são dados por $l_1 = 1, l_2 = 3$ e $l_3 = 4$ é dado na Tabela A.7.

Para o código A, o comprimento médio é dado por

$$E_A(W) = \frac{2}{3} \times 1 + \frac{2}{9} \times 3 + \frac{1}{9} \times 4 = 1,78.$$

Porém, nota-se que facilmente um outro código livre de prefixo é obtido para esta fonte (Tabela A.8) e que o comprimento médio das palavras-código deste código é dado por

$$E_B(W) = \frac{2}{3} \times 1 + \frac{2}{9} \times 2 + \frac{1}{9} \times 2 = 1,33$$

que é menor que o comprimento médio obtido pelo código A.

Tabela A.8: Código livre de prefixo para a fonte binária discreta sem memória U com distribuição de probabilidade $P_U(u_1) = 2/3, P_U(u_2) = 2/9$ e $P_U(u_3) = 1/9$.

Fonte	Código B
u_1	0
u_2	10
u_3	11

Desta forma, apesar do código A obedecer (A.37) claramente ele não é um código compacto.

A.5.4 Codificação de Huffman

Nesta seção é descrita uma importante classe de códigos instantâneos, chamados códigos de Huffman, atribuídos ao trabalho pioneiro de Huffman [11].

Os códigos de Huffman utilizam um algoritmo que usa os símbolos u_i da fonte e suas probabilidades $p_i = P_U(u_i)$, procurando atribuir a cada símbolo uma palavra-código de comprimento proporcional à quantidade de informação fornecida por tal símbolo. Os códigos de Huffman são importantes porque são códigos compactos. Isto é, o algoritmo de Huffman produz um código com comprimento médio, $E(W)$, que é o menor possível para um dado número de símbolos da fonte, alfabeto do código e distribuição de probabilidade da fonte.

Definição 23 ***(Fonte reduzida)*** *Considere uma fonte U com K símbolos $\{u_i : i = 1, 2, ...K\}$ e as probabilidades associadas a estes símbolos $\{P_U(u_i) : i = 1, 2, ...K\}$. Sejam os símbolos reordenados tais que $P_U(u_1) \geq P_U(u_2) \geq ... \geq P_U(u_K)$. Combinando os D últimos símbolos de U, $\{u_{K-D+1}, u_{K-D+2}, ..., u_K\}$ num símbolo $u*_{K-D+1}$ com probabilidade $P(u*_{K-D+1}) = \sum_{i=1}^{D} P(u_{K-D+i})$, obtém-se uma nova fonte denominada fonte reduzida de U contendo $K - D + 1$ símbolos, $\{u_1, u_2, ...u*_{K-D+1}\}$. Esta fonte é chamada fonte reduzida U_1. Fontes reduzidas sucessivas $U_2, U_3, ...$ pode ser obtidas aplicando um processo similar de reordenação e combinação dos símbolos até que a fonte tenha apenas D símbolos.*

□

Note que só será possível reduzir uma fonte a exatamente D símbolos se a fonte original tiver $K = D + \alpha \cdot (D - 1)$ símbolos em que α é um inteiro não negativo. Para uma fonte binária isto ocorre para qualquer valor de $K \geq 2$. Para códigos não binários se $\alpha = \frac{K-D}{(D-1)}$ não é um número inteiro é necessário inserir símbolos mudos com probabilidade zero a fim de criar uma fonte com $K = D + \lceil\alpha\rceil(D - 1)$ símbolos, em que $\lceil\alpha\rceil$ é o menor inteiro maior ou igual a α.

Um código compacto D-ário trivial para uma fonte reduzida com D símbolos é então usado para projetar o código para a fonte reduzida anterior como descrito a seguir.

Descrição 1

Considere que há um código compacto para a fonte reduzida U_j. Designando os últimos D símbolos de U_j, $\{u_{K-D+1}, u_{K-D+2}, ..., u_K\}$ como os símbolos que foram combinados para

formar o símbolo $u*_{K-D+1}$ *de* U_j*. Atribui-se a cada símbolo de* U_{j-1}*, exceto aos últimos* D *símbolos, a palavra-código usada pelo símbolo correspondente de* U_j*. As palavras-código para os últimos* D *símbolos de* U_{j-1} *são formados adicionando* $\{0, 1, ..., D\}$ *à palavra-código de* $u*_{K-D+1}$ *a fim de formar* D *novas palavras-código.*

O algoritmo de Huffman então opera seguindo a seqüência da ultima fonte reduzida à fonte original, projetando códigos compactos para cada uma delas, até que o código compacto para a fonte original seja formado.

Algoritmo para gerar códigos de Huffman binários

1. Reordene os símbolos da fonte em ordem decrescente de probabilidade de cada símbolo.
2. Sucessivamente reduza a fonte U para U_1, então para U_2, e assim por diante, seguindo o procedimento descrito na Definição 23 para $D = 2$.
3. Atribua um código compacto para a fonte reduzida final. Para uma fonte com dois símbolos um código trivial é $\{0, 1\}$.
4. Siga o caminho a partir da última fonte reduzida à fonte original atribuindo um código compacto com o método mostrado na **Descrição 1**. O código compacto obtido para U é o código de Huffman.

O exemplo a seguir ilustra o algoritmo de Huffman para o caso binário.

Exemplo 35 *Considere uma fonte binária com 5 símbolos, os quais possuem probabilidades.*

$$P_U(u_1) = 0,2; P_U(u_2) = 0,4; P_U(u_3) = 0,1; P_U(u_4) = 0,1; P_U(u_5) = 0,2$$

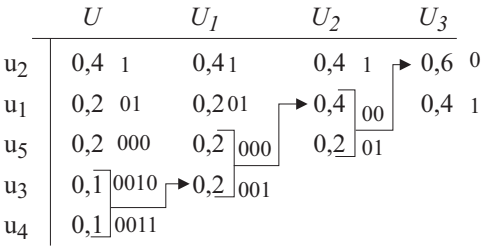


Figura A.12: Código binário de Huffman.

O comprimento médio do código obtido é $E(W) = 2,2$ *bits/ símbolo e a eficiência é* $\eta = 96,5\%$*. Como o código de Huffman é compacto qualquer outro código binário projetado para está fonte terá comprimento* $E(W_O) \geq E(W)$

□

Códigos de Huffman D-ários

Para o projeto de códigos de Huffman D-ários é utilizado o seguinte algoritmo.

1. Calcule $\alpha = \frac{K-D}{(D-1)}$. Se α não é inteiro então adicione símbolos mudos com probabilidade zero à fonte, tal que ela passe a ter $K = D + \lceil\alpha\rceil(D-1)$ símbolos.
2. Reordene os símbolos da fonte em ordem decrescente de probabilidade do símbolo
3. Sucessivamente reduza a fonte U para U_1, então para U_2, e assim por diante, seguindo o procedimento descrito na Definição 23.
4. Atribua um código compacto para a fonte reduzida final. Para uma fonte com dois símbolos um código trivial é $\{0, 1, ..., D-1\}$.
5. Siga o caminho a partir da última fonte reduzida à fonte original atribuindo um código compacto com o método mostrado na **Descrição 1**. O código compacto obtido para U descartando as palavras-código associadas aos símbolos mudos é o código de Huffman D-ário.

Exemplo 36 *Considere uma fonte quaternária ($D = 4$) com 11 símbolos, que possuem probabilidades* $P_U(u_1) = 0,16; P_U(u_2) = 0,14; P_U(u_3) = 0,13; P_U(u_4) = 0,12; P_U(u_5) = 0,10; P_U(u_6) = 0,10; P_U(u_7) = P_U(u_8) = 0,06; P_U(u_9) = 0,05; P_U(u_{10}) = P_U(u_{11}) = 0,04$. *Pede-se projetar um código compacto quaternário para esta fonte. Calculando α, observa-se que ele não é inteiro ($\alpha = 2,33$), desta forma torna-se necessária a adição de símbolos mudos à fonte de modo a ter $K = 13$ símbolos. Assim, pela Figura A.13 observa-se que o código obtido tem comprimento médio $E(W) = 1,78$ unidades quaternárias/ símbolo e eficiência $\eta = 93\%$.*

□

A.6 Canais e informação mútua

Nas seções anteriores o interesse maior estava relacionado às propriedades das fontes de informação e com a transformação de seqüências de símbolos da fonte em seqüências de palavras-código.

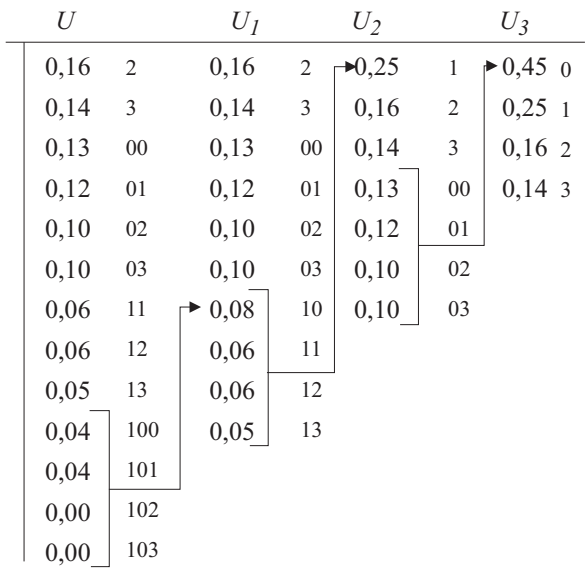


Figura A.13: Código de Huffman D-ário.

Foi possível relacionar a medida de informação às propriedades das fontes de informação. Em particular, foi mostrado que a entropia (expressa em unidades apropriadas) define uma cota inferior para o número médio de símbolos necessários para codificar cada símbolo da fonte. Tal cota foi usada para definir redundância (Definição 21) e eficiência (Definição 20) de um código. Na verdade, nota-se que grande parte do que foi visto até o momento serviu para proporcionar alicerce para as definições de redundância e eficiência, e para a construção de códigos com a menor redundância possível.

Na prática, nem sempre é interessante usar códigos de canal com pouca ou nenhuma redundância uma vez que na presença de ruído se torna inviável a recuperação pelo receptor da mensagem originalmente transmitida. Nesta seção o interesse passa da fonte de informação para o canal de informação, i.e., da geração da informação para sua transmissão.

Para iniciar, considere que as seguintes suposições se aplicam ao modelo de um canal de informação considerado.

Estacionário As propriedades estatísticas do ruído não mudam com o tempo.

Sem memória O comportamento do canal e o efeito do ruído no momento t não depende do comportamento do canal ou do efeito do ruído em qualquer momento passado.

Definição 24 ***(Canal de informação discreto)*** *Um canal de informação discreto é uma tripla X, Y, P, na qual X é o alfabeto de entrada, Y é o alfabeto de saída e P é a distribuição de probabilidades de transição $P_{Y|X}(y|x)$ do canal. $X = \{x_i : i = 1, 2, ...r\}$ é um conjunto*

discreto de $r = |X|$ *símbolos (no qual* $|X|$ *é a cardinalidade do alfabeto de entrada), e* $Y = \{y_j : i = 1, 2, ...s\}$ *é um conjunto discreto com cardinalidade* $s = |Y|$ *símbolos. O comportamento da transmissão do canal é descrito pelas probabilidades em* $P = \{P_{Y|X}(y_j|x_i) : i = 1, 2, ...r; j = 1, 2, ..., s\}$*, em que* $P_{Y|X}(y_j|x_i)$ *é a probabilidade que o símbolo de saída* y_j *seja recebido dado que o símbolo de entrada* x_i *foi transmitido.*

□

As probabilidades condicionais que descrevem um canal de informação discreto podem ser representadas convenientemente usando a seguinte matriz

$$\mathbf{P} = \begin{bmatrix} P(y_1|x_1) & P(y_2|x_1) & \dots & P(y_s|x_1) \\ P(y_1|x_2) & P(y_2|x_2) & \dots & P(y_s|x_2) \\ \vdots\vdots\ddots\vdots & & & \\ P(y_1|x_r) & P(y_2|x_r) & \dots & P(y_s|x_r) \end{bmatrix}, \tag{A.46}$$

na qual $\mathbf{P}$ é a matriz canal que, por conveniência, pode ser descrita também da seguinte forma

$$\mathbf{P} = \begin{bmatrix} P_{11} & P_{12} & \dots & P_{1s} \\ P_{21} & P_{22} & \dots & P_{2s} \\ \vdots\vdots\ddots\vdots & & & \\ P_{r1} & P_{r2} & \dots & P_{rs} \end{bmatrix}, \tag{A.47}$$

na qual $P_{ij} = P(y_j|x_i)$.

Uma representação gráfica de um canal de informação discreto é dada na Figura A.14.

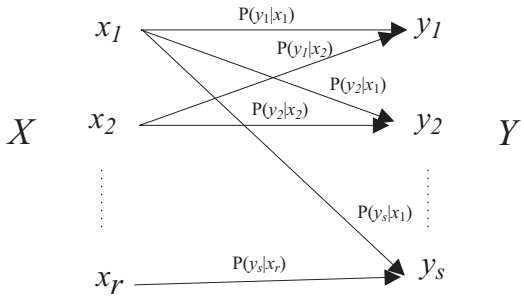


Figura A.14: Representação gráfica de um canal de informação discreto

A matriz canal apresenta as seguintes propriedades e estrutura:

- Cada linha de $\mathbf{P}$ contém as probabilidades de todas as possíveis saídas da mesma entrada do canal.

- Cada coluna de **P** contém as probabilidades de todas as possíveis entradas para uma saída particular do canal.
- Se o símbolo x_i for transmitido deve-se receber um símbolo de saída com probabilidade 1, que é:

$$\sum_{j=1}^{s} P(y_j|x_i) = 1, i = 1, 2, ..., r, \tag{A.48}$$

i.e., as probabilidades em cada linha devem somar 1.

Exemplo 37 *Considere um canal binário, com alfabeto de entrada* $\{0, 1\}$ *e alfabeto de saída* $\{0, 1\}$.

a) **Exemplo de canal sem ruído:** *Se o canal binário é sem ruído não há erro na transmissão, a matriz canal é dada por* $\boldsymbol{P} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ *e o canal é representado graficamente da seguinte forma*

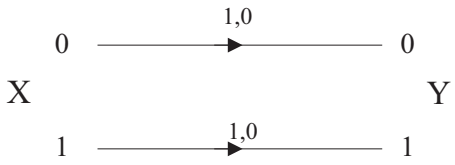


Figura A.15: Canal sem ruído.

b) **Exemplo de canal ruidoso:** *Se o canal binário é ruidoso e introduz uma inversão de bit em 1% do tempo, então a matriz canal é dada por* $\boldsymbol{P} = \begin{bmatrix} 0.99 & 0.01 \\ 0.01 & 0.99 \end{bmatrix}$ *e o canal é representado graficamente da seguinte forma*

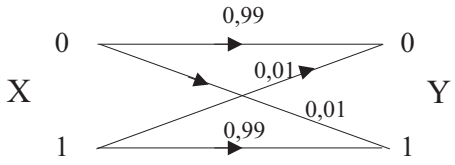


Figura A.16: Canal ruidoso.

□

A.6.1 Informação mútua

A fim de especificar completamente o comportamento de um canal é necessário especificar características da entrada assim como a matriz canal, **P**. As características da entrada são dadas pelas probabilidades dos símbolos de entrada, $P(X) = \{P(x_1), P(x_2), ..., P(x_r)\}$.

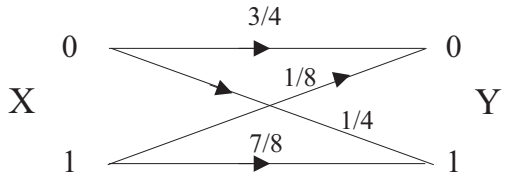
Sendo o canal totalmente especificado, as probabilidades de saída, $P(Y) = \{P(y_1), P(y_2), \ldots, P(y_s)\}$, podem ser calculadas usando:

$$P(y_j) = \sum_{i=1}^{r} P(y_j|x_i)P(x_i). \tag{A.49}$$

Exemplo 38 *Considere um canal binário completamente especificado por:*

$$P = \begin{bmatrix} 3/4 & 1/4 \\ 1/8 & 7/8 \end{bmatrix} \quad e \quad \begin{array}{l} P(x=0) = 2/3 \\ P(x=1) = 1/3 \end{array}$$

o qual é representado graficamente por



As probabilidades de saída são calculadas da seguinte forma:
$P(y=0) = P(y=0|x=0)P(x=0) + P(y=0|x=1)P(x=1) = \frac{3}{4} \times \frac{2}{3} + \frac{1}{8} \times \frac{1}{3} = \frac{13}{24}$
$P(y=1) = 1 - P(y=0) = \frac{11}{24}$.

□

Conceitualmente caracterizam-se as probabilidades de canal como:

- *a priori* se são atribuídos às probabilidades *antes* do canal ser usado (sem nenhum conhecimento).
- *a posteriori* se são atribuídos às probabilidades *depois* do canal ser usado (havendo conhecimento da resposta do canal).

Especificamente:

$P(y_j)$ denota uma probabilidade *a priori* do símbolo de saída y_j.

$P(y_j|x_i)$ denota uma probabilidade *a posteriori* do símbolo de saída y_j se se sabe que o símbolo x_i foi enviado.

$P(x_i)$ denota uma probabilidade *a priori* do símbolo de entrada x_i.

$P(x_i|y_j)$ denota uma probabilidade *a posteriori* do símbolo de entrada x_i se se sabe que o símbolo y_j de saída foi recebido.

Similarmente, pode-se referir à entropia *a priori* de X:

$$H(X) = \sum_{x \in X} P(x) \log \frac{1}{P(x)}, \tag{A.50}$$

como a incerteza média que se tem sobre a entrada antes da saída do canal ser observada e a entropia a posteriori de X dado y_j:

$$H(X|y_j) = \sum_{x \in X} P(x|y_j) \log \frac{1}{P(x|y_j)}, \tag{A.51}$$

como a incerteza média que se tem sobre a entrada depois da saída do canal, y_j, ser observada.

$H(X)$ incerteza média da entrada do canal antes de ser observada a saída;

$H(X|Y)$ incerteza média (ou equivocação) da entrada do canal depois de observar-se a saída;

$H(X) - H(X|Y)$ redução na incerteza média da entrada do canal em função da observação das saídas Y.

A seguir é introduzida a definição de informação mútua, que é uma medida da redução da incerteza de uma variável aleatória devido ao conhecimento sobre uma outra variável aleatória.

Definição 25 ***(Informação mútua)*** *Para um alfabeto de entrada X e um alfabeto de saída Y a expressão*

$$I(X;Y) = H(X) - H(X|Y) \tag{A.52}$$

é definida como a informação mútua entre X e Y.

□

O leitor poderia questionar porque se usa o termo "informação mútua" em vez de "informação proporcionada por Y sobre X" para $I(X;Y)$. Para perceber o porquê, nota-se inicialmente que $H(XY)$ pode ser expandido de duas formas,

$$H(XY) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

chegando, consequentemente a

$$H(X) - H(X|Y) = H(Y) - H(Y|X)$$

ou, equivalentemente,

$$I(X;Y) = I(Y;X). \tag{A.53}$$

Assim, vê-se que X fornece a mesma quantidade de informação sobre Y assim como Y fornece sobre X. A relação é completamente simétrica. Logo, o fornecimento de informação é de fato mútuo.

Uma expressão alternativa para a equação (A.52) da informação mútua pode ser derivada da seguinte forma:

$$\begin{aligned} I(X;Y) = \quad & H(X) - H(X|Y) \\ & = \sum_{x\in X} P(x) \log \frac{1}{P(x)} - \sum_{x\in X}\sum_{y\in Y} P(x,y) \log \frac{1}{P(x|y)} \\ & = \sum_{x\in X}\sum_{y\in Y} P(x,y) \log \frac{1}{P(x)} - \sum_{x\in X}\sum_{y\in Y} P(x,y) \log \frac{1}{P(x|y)} \\ & = \sum_{x\in X}\sum_{y\in Y} P(x,y) \log \frac{P(x|y)}{P(x)}. \end{aligned}$$

Usando

$$P(x|y) = \frac{P(x,y)}{P(y)} = \frac{P(y|x)P(x)}{P(y)} = \frac{P(y|x)P(x)}{\sum_{x\in X} P(y|x)P(x)}. \tag{A.54}$$

Proposição 9 ***(Expressão alternativa para a informação mútua)***

$$\begin{aligned} I(X;Y) \quad & = \sum_{x\in X}\sum_{y\in Y} P(x,y) \log \frac{P(x,y)}{P(x)P(y)} \\ & = \sum_{x\in X}\sum_{y\in Y} P(x)P(y|x) \log \frac{P(y|x)}{P(y)}. \end{aligned} \tag{A.55}$$

□

Propriedades de informação mútua

Proposição 10 *A informação mútua é uma quantidade não negativa:*

$$I(X;Y) \geq 0, \tag{A.56}$$

com $I(X;Y) = 0$, se e só se, $P(x,y) = P(x)P(y), \forall x, y$, i.e., os alfabetos de entrada e saída forem estatisticamente independentes.

Demonstração:

Da desigualdade (A.7), chega-se a

$$\sum_{i=1}^{N} p_i \log \frac{q_i}{p_i} \leq 0 \tag{A.57}$$

para duas fontes de cardinalidade N com probabilidades dos símbolos, p_i e q_i, e igualdade, se e só se, $p_i = q_i$ para $i = 1, 2, 3, ..., N$.

Faça $p_i \equiv P(x,y)$, $q_i \equiv P(x)P(y)$ e $N \equiv |X \times Y|$. Então, das equações (A.55) e (A.57), obtém-se:

$$-I(X;Y) = \sum_{x \in X} \sum_{y \in Y} P(x,y) \log \frac{P(x)P(y)}{P(x,y)} \equiv \sum_{x \in X} \sum_{y \in Y} p_i \log \frac{q_i}{p_i} \leq 0.$$

Então

$$I(X;Y) \geq 0. \tag{A.58}$$

■

É interessante notar que em 1948, Shannon não usou o termo "informação mútua" nem um símbolo especial para denotá-la, mas simplesmente usou diferenças de incertezas. A terminologia "informação mútua" (ou "informação mútua média" como é com freqüência chamada) e o símbolo $I(X;Y)$ foram introduzidos mais tarde por Fano. Acha-se conveniente seguir Fano, porém nunca se deve perder de vista a idéia de Shannon que a informação é nada mais que uma mudança na incerteza.

Proposição 11 ***(Informação mútua e entropia)***

$$I(X;Y) = H(X) - H(X|Y), \tag{A.59}$$

$$I(X;Y) = H(Y) - H(Y|X), \tag{A.60}$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y), \tag{A.61}$$

$$I(X;Y) = I(Y;X), \tag{A.62}$$

$$I(X;X) = H(X), \tag{A.63}$$

□

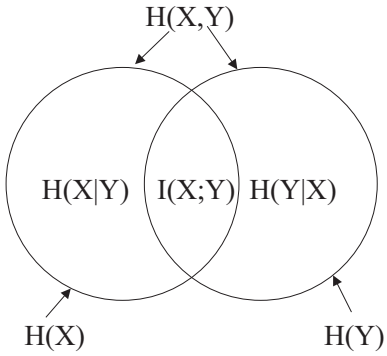


Figura A.17: Relação entre entropia e informação mútua.

As relações entre as diversas entropias estão expressas no diagrama de Venn ilustrado na Figura A.17.

As duas definições a seguir devem parecer naturais neste ponto.

Definição 26 *A informação mútua condicional entre as variáveis aleatórias discretas X e Y, dado que o evento $Z = z$ ocorre, é a quantidade*

$$I(X;Y|Z=z) = H(X|Z=z) - H(X|Y,Z=z). \tag{A.64}$$

Definição 27 *A informação mútua condicional entre as variáveis aleatórias discretas X e Y, dada a variável aleatória Z é a quantidade*

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z). \tag{A.65}$$

De (A.12) e (A.16), segue-se que

$$I(X;Y|Z) = \sum_{z \in supp(P_Z)} P_Z(z) I(X;Y|Z=z). \tag{A.66}$$

Do fato que $H(XY|Z=z)$ e $H(XY|Z)$ podem ser expandidas de duas formas:

$$\begin{aligned} H(XY|Z=z) &= H(X|Z=z) + H(Y|X,Z=z) \\ &= H(Y|Z=z) + H(X|Y,Z=z) \end{aligned}$$

e

$$\begin{aligned} H(XY|Z) &= H(X|Z) + H(Y|X,Z) \\ &= H(Y|Z) + H(X|Y,Z) \end{aligned}$$

segue-se das Definições 26 e 27 que

$$I(X;Y|Z=z) = I(Y;X|Z=z) \tag{A.67}$$

e que

$$I(X;Y|Z) = I(Y;X|Z). \tag{A.68}$$

Considera-se a seguir as desigualdades fundamentais satisfeitas pela informação mútua. A Definição 25, por causa de (A.13) e (A.62), imediatamente implica no seguinte resultado.

Teorema 5 *Para quaisquer duas variáveis aleatórias X e Y,*

$$0 \leq I(X;Y) \leq min[H(X), H(Y)], \tag{A.69}$$

com igualdade à esquerda, se e só se, X e Y são variáveis aleatórias independentes, e com igualdade à direita, se e só se ou Y determina essencialmente X, ou X essencialmente determina Y, ou ambos.

De modo similar, as Definições 26 e 27 levam às desigualdades

$$0 \leq I(X;Y|Z=z) \leq min[H(X|Z=z), H(Y|Z=z)] \tag{A.70}$$

e

$$0 \leq I(X;Y|Z) \leq min[H(X|Z), H(Y|Z)], \tag{A.71}$$

respectivamente.

Essa seção é encerrada chamando-se atenção para um fato. Como condicionar pode reduzir incerteza, pode-se sentir tentado a achar que a seguinte desigualdade é verdadeira.

$$I(X;Y|Z) \leq I(X;Y).$$

Porém, nem sempre a situação acima é verdade. Usando a intuição é possível ver o porquê. Suponha que num cripto-sistema X é o texto-claro, Y é o texto-cifrado e Z é a chave, observa-se neste caso que tanto $I(X;Y|Z) < I(X;Y)$ quanto $I(X;Y|Z) > I(X;Y)$ é possível.

A.6.2 Canal sem ruído e canal determinístico

Nesta seção são definidos formalmente **canais sem ruído** e também é definida uma outra classe de canais chamados **canais determinísticos**.

Canal sem ruído

Definição 28 ***(Canal sem ruído)*** *Um canal para o qual existem pelo menos tantos símbolos de saída quanto símbolos de entrada, mas no qual cada símbolo de saída pode ser produzido pela ocorrência de apenas um dos símbolos de entrada é chamado um* ***canal sem ruído****. A matriz canal de um canal deste tipo tem a propriedade de possuir um e apenas um elemento não nulo em cada coluna.*

□

Exemplo 39 *O canal ilustrado na Figura A.18 com seis saídas e três entradas é do tipo sem ruído porque se sabe com certeza, qual símbolo de entrada,*$\{a_1, a_2, a_3\}$*, foi transmitida dado o conhecimento sobre a saída do canal,*$\{b_1, b_2, b_3, b_4, b_5, b_6\}$*.*

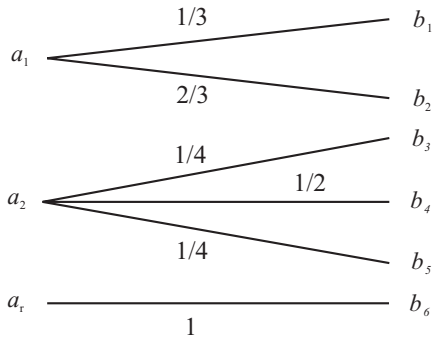


Figura A.18: Exemplo de um canal sem ruído.

A matriz canal correspondente é dada por

$$\boldsymbol{P} = \begin{bmatrix} 1/3 & 2/3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/4 & 1/2 & 1/4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

□

Sendo y_j o símbolo de saída recebido, então pela definição de canal sem ruído, sabe-se com certeza qual símbolo de entrada foi transmitido, diga-se x_i^*, i.e., $P(x_i^*|y_j) = 1$ para x_i^* e portanto $P(x_i|y_j) = 0$ para qualquer outro símbolo de entrada x_i, $x_i \neq x_i^*$. Desta forma a equivocação $H(X|Y)$ dada por

$$\begin{aligned} H(X|Y) &= \sum_{x\in X}\sum_{y\in Y} P(x,y)\log\frac{1}{P(x|y)} \\ &= \sum_{y\in Y} P(y)\sum_{x\in X} P(x|y)\log\frac{1}{P(x|y)} \end{aligned}$$

é igual a zero.

Proposição 12 ***(Informação mútua para canais sem ruído)*** *A informação mútua para canais sem ruído é dada por*

$$I(X;Y) = H(X), \tag{A.72}$$

isto é, a quantidade de informação é igual à entropia da variável de entrada do canal.

□

Canal determinístico

Definição 29 ***(Canal Determinístico)*** *Um canal no qual existem pelo menos tantos símbolos de entrada quanto de saída, mas no qual cada símbolo de entrada é capaz de produzir apenas um símbolo de saída é chamado canal determinístico. A matriz canal nesse caso tem a propriedade de existir um e apenas um elemento não nulo em cada linha, e como os elementos de cada linha devem somar 1, este elemento não nulo será 1.*

□

Exemplo 40 *O canal ilustrado na Figura A.19 com três saídas e seis entradas é determinístico porque se sabe com certeza, qual símbolo de saída do canal,*$\{b_1, b_2, b_3\}$ *é recebido dado que o símbolo de entrada transmitido,*$\{a_1, a_2, a_3, a_4, a_5, a_6\}$*, é conhecido.*

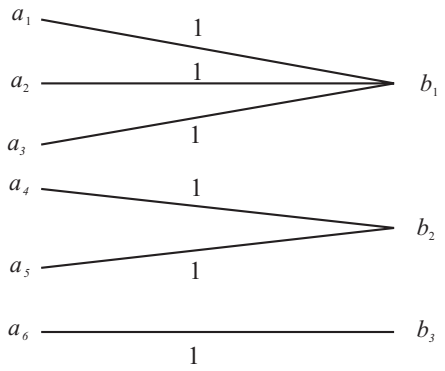


Figura A.19: Exemplo de um canal determinístico.

A matriz canal correspondente é dada por:

$$\boldsymbol{P} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

□

Referências

[1] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communcation*, University of Illinois Press, Urbana and Chicago, 1963.

[2] C. E. Shannon, "A mathematical theory of communication (parts I and II)". *Bell System Technical Journal*, XXVII:379-423.

[3] N. Abramson, *Information Theory and Coding.* McGraw-Hill, 1963.

[4] R.G. Gallager and D.C. Van Voorhis, "Optimal Source Codes for Geometrically Distributed Integer Alphabets", *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 228-230, Mar. 1975.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* New York: Wiley, 1991.

[6] R. Togneri and C. J. S. deSilva, *Fundamentals of Information Theory and Coding Design*, Chapman & Hall/CRC, 2002.

[7] J. L. Massey, "Applied Digital Information Theory I", *Class notes at the ETH Zurich*, http://www.isi.ee.ethz.ch/education/public/pdfs/aditI.pdf, 1980-1998.

[8] R.V.L. Hartley "Transmission of Information", *Bell Syst. Tech. J.*, Vol. 3, July 1928, pp. 535 - 564.

[9] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastics Processes*, Fourth Edition, McGraw-Hill, 2002.

[10] S. Lin and D. J. Costello, *Error Control Coding*, 2nd Edition, Prentice Hall, 2004.

[11] - D.A. Huffman, “A method for the construction of minimun redundancy codes”, *Proc. IRE*, 40, 1098-1101, 1952.

APÊNDICE B

Conceitos básicos de criptografia

Inicialmente, a criptografia era usada apenas para fins militares e diplomáticos. Porém, devido ao grande desenvolvimento nos meios de comunicação, o que era um privilégio de militares e diplomatas passou a se disseminar para outras áreas.

Durante a Segunda Guerra Mundial houve um grande desenvolvimento na área, novas técnicas foram criadas e máquinas foram usadas no processo de cifragem e decifragem [1].

Atualmente, um cidadão comum tem a possibilidade de utilizar tais técnicas para se comunicar e armazenar seus dados de forma segura. Com o surgimento da Internet, projetada desde o início com o intuito de proporcionar comunicação ininterrupta e irrestrita [2,pp.47-50], a necessidade de proteger os dados, seja para mantê-los secretos, seja para mantê-los íntegros ou até mesmo para ter certeza de sua origem, tem mostrado cada vez mais a importância do uso de técnicas de segurança e em particular da criptografia.

Neste apêndice são revistos alguns aspectos básicos sobre criptografia, objetivando dar subsídios para o entendimento desta tese. Para mais conceitos e informações nessa área, deve-se consultar livros textos especializados, como por exemplo: [3]-[7].

B.1 Introdução à criptografia

A técnica que se propõe a manter mensagens seguras é a **criptografia**, a qual é praticada por **criptógrafos**. A **criptoanálise**, arte e ciência de recuperar a mensagem sem a necessi-

dade do conhecimento da chave*, é praticada pelos **criptoanalistas**. O ramo da matemática que engloba tanto a criptografia quanto a criptoanálise é chamado **criptologia** e é praticado por **criptologistas** [3].

A criptografia é uma das ferramentas utilizadas para a proteção de dados, proporcionando privacidade e integridade, evitando que as informações sejam reveladas, alteradas ou substituídas por pessoas não autorizadas. Diferentemente de outras ferramentas utilizadas para a segurança de dados, os cripto-sistemas são aqueles que se mostram mais completos até o momento, proporcionando alto nível de segurança com mais flexibilidade [8], sem esquecer todavia, que a criptografia constitui apenas uma parte de um sistema de segurança. Os cripto-sistemas usam transformações a fim de detectar a alteração dos dados (**integridade**) assim como para tornar os dados não inteligíveis (**privacidade**) para pessoas não autorizadas.

A criptografia é conhecida classicamente como uma arte muito antiga que utiliza alguns procedimentos visando tornar certas informações não legíveis para pessoas não autorizadas, caso tais informações sejam interceptadas. Por isso, para muitos a criptografia é apenas uma ferramenta para manter informações secretas, mas como será visto no decorrer deste apêndice, ela é mais que isso. A maioria das aplicações de álgebra e teoria dos números na área veio à tona a partir de 1976 com o surgimento da criptografia de chave pública [9], antes disso, provavelmente, o resultado matemático mais sofisticado foi dado por Shannon [10] no seu trabalho de 1949 onde uma fundamentação teórica para criptografia foi fornecida baseada em conceitos de teoria da informação introduzidos por ele no trabalho de 1948 [11]. Nesse trabalho [10] a medida de sigilo baseada na incerteza sobre o texto claro dado o texto cifrado interceptado dizia que, se nada pudesse ser dito sobre o texto claro independentemente da quantidade de texto cifrado interceptado a cifra alcançaria sigilo perfeito. A única maneira de obter-se sigilo perfeito seria através do uso de um cripto-sistema de bloco descartável, do inglês, *one-time pad*.

A palavra criptografia é de origem grega significando "Escrita Escondida" (*Kriptos* (escondido) + *graphos*(escrita)). Seu primeiro registro é de 400 A.C. na utilização pelos espartanos de um mecanismo conhecido como Cítala Espartana [12]. Neste cripto-sistema o processo de **cifragem**† consistia em enrolar uma tira de couro ou papiro num cilindro e escrever a mensagem (**texto claro**) no sentido do comprimento do cilindro; ao se desenrolar a tira,

*A definição de chave é apresentada no decorrer deste apêndice.

†Processo pelo qual com alguma informação secreta transforma-se o **texto claro** (dados originais, legíveis) em **texto cifrado** (dados não inteligíveis, sem sentido).

a mensagem parecia não ter nenhum sentido. Para se obter a mensagem original, ou seja **decifrar**[‡] a mensagem cifrada (**texto cifrado**) recebida, bastava enrolar novamente a tira de couro ou papiro num cilindro com as mesmas dimensões do cilindro usado no processo de cifragem. Neste caso, observa-se que a informação secreta compartilhada entre o remetente e receptor, que possibilita a troca de mensagens, dificultando o acesso a estas mensagens por uma pessoa não autorizada, corresponde às dimensões do cilindro, o que pode se chamar de **chave secreta** do cripto-sistema.

Outro cripto-sistema clássico muito conhecido é a cifra de César. Este cripto-sistema foi criado e utilizado pelo imperador romano Júlio César em suas conquistas. O processo de cifragem neste cripto-sistema consistia num deslocamento cíclico de três letras do alfabeto, i. e., a letra **a** era substituída pela letra **d**, a letra **b** era substituída pela letra **e** e assim por diante. Conhecido o deslocamento usado no processo de cifragem, a decifragem era feita facilmente, realizando as substituições de forma invertida, i. e., substituindo-se **d** por **a**, **e** por **b** e assim por diante.

A criptografia clássica é subdividida em **cifras de transposição** e **cifras de substituição**. A cítala Espartana é um exemplo de cifra de transposição. Neste tipo de cifra as letras do texto claro são permutadas de alguma forma dando origem assim ao texto cifrado. Já a cifra de César é um exemplo de **cifra de substituição simples** ou **monoalfabética**. Neste tipo de cifra ocorre a substituição de uma letra do alfabeto original por uma letra de um alfabeto com as letras em uma outra ordem.

Cifras de substituição simples foram usadas por vários séculos até serem quebradas definitivamente pelos árabes utilizando um método de criptoanálise baseado na análise de freqüência das letras do alfabeto. Na verdade o surgimento da criptoanálise só foi possível a partir do momento que a humanidade obteve um nível suficiente de aprendizado em várias disciplinas, incluindo matemática, estatística e lingüística [13,p.15], e naquela época a civilização árabe vivia num ambiente bastante favorável a isso.

Além das cifras de substituição simples ou monoalfabéticas, outros tipos de cifras de substituição são as **cifras polialfabéticas** e as cifras baseadas em **substituição homofônica**. A cifra de Vigenère é um exemplo de cifra polialfabética, na qual vários alfabetos eram utilizados no processo de cifragem. As cifras baseadas em substituição homofônica consistem em associar a cada letra do alfabeto original um grupo de possíveis substitutos de forma que o

[‡]Processo reverso ao processo de cifragem que permite a obtenção do texto claro a partir do texto cifrado [7,p.1].

número de substitutos seja proporcional à freqüência da letra. Observa-se que tais tipos de cifras de substituição surgiram basicamente com o intuito de dificultar a criptoanálise baseada em análise de freqüência.

Para aqueles interessados em saber um pouco mais sobre a criptografia clássica e, principalmente, aspectos históricos da criptografia o livro de Simon Singh [13] é uma excelente fonte.

De um modo geral, a mensagem ou texto claro, denotada por M, pode ser, por exemplo, uma seqüência de *bits*, um arquivo de texto, uma figura, voz digitalizada, etc.. . Considerando um meio digital, M pode ser simplesmente uma seqüência binária a ser armazenada ou transmitida. Em qualquer caso, M representa uma mensagem a ser cifrada. O texto cifrado ou criptograma, denotado por C, por sua vez também pode ser uma seqüência binária.

A função de cifragem E (*encryption*) é aplicada a M e à chave K produzindo o criptograma C, i.e.,

$$E_K(M) = C. \tag{B.1}$$

No processo reverso, a função de decifragem D opera sobre a chave K e sobre o criptograma C para recuperar a mensagem M, i.e.,

$$D_K(C) = M. \tag{B.2}$$

Como o objetivo de cifrar e decifrar a mensagem é proteger a mensagem possibilitando sua recuperação, então a seguinte identidade deve ser verdadeira:

$$D_K(E_K(M)) = M. \tag{B.3}$$

B.1.1 Autenticidade, integridade e não-repudiação

A criptografia atual é mais que "escrita secreta", mais que cifragem e decifragem. A autenticação, por exemplo é uma parte fundamental do dia-a-dia dos indivíduos assim como a privacidade. Usa-se autenticação, por exemplo, quando um documento é assinado. No mundo atual onde decisões são comunicadas eletronicamente é necessário que tais procedimentos sejam replicados para os meios eletrônicos.

Além de proporcionar confidencialidade, a criptografia também é usada muitas vezes para proporcionar:

Autenticação do usuário: Assegura que as partes envolvidas numa comunicação são quem elas realmente dizem ser. Desta forma, o receptor é capaz de ter certeza da origem da mensagem, de forma que nenhum impostor pode se passar pelo remetente legítimo.

Autenticação da origem dos dados: Assegura a fonte dos dados.

Integridade dos dados: O receptor pode verificar se a mensagem recebida não foi alterada; um intruso não pode substituir uma mensagem legítima por uma falsa ou mesmo alterá-la.

Não repudiação: Torna possível a não repudiação de uma transação, i. e., aquele que receber a assinatura poderá usá-la para provar para uma terceira parte neutra que a assinatura foi de fato gerada pelo assinante, o qual não pode repudiar a assinatura.

B.1.2 Algoritmos e chaves

Um **algoritmo criptográfico**, ou **cifra**, é uma função matemática usada para cifragem e decifragem. Geralmente existem duas funções relacionadas, uma para cifragem e outra para decifragem.

Um princípio básico da criptografia é o **princípio de Kerckhoff** que diz que a segurança de um cripto-sistema não deve repousar no fato de que o criptoanalista inimigo desconhece os processos de cifragem e de decifragem. O princípio de Kerckhoff assume que o criptoanalista possui completo conhecimento sobre o algoritmo criptográfico e sua implementação. Portanto, de acordo com Kerckhoff, a segurança do cripto-sistema deve depender apenas do segredo da chave, e não do segredo dos processos de cifragem e de decifragem. A observação de tal princípio proporciona um modo de controle de qualidade e de padronização dos cripto-sistemas.

A chave, K, deve ser grande o bastante para o nível de segurança desejado. Dependendo do tipo de cripto-sistema usado a mesma chave é usada para os processos de cifragem e de decifragem, ou chaves diferentes são usadas em cada um destes processos. Cripto-sistemas que utilizam a mesma chave para cifrar e para decifrar podem ser descritos da seguinte forma:

$$E_K(M) = C. \tag{B.4}$$

$$D_K(C) = M. \tag{B.5}$$

Tais funções têm a propriedade ilustrada na Figura B.1

$$D_K(E_K(M)) = M. \tag{B.6}$$

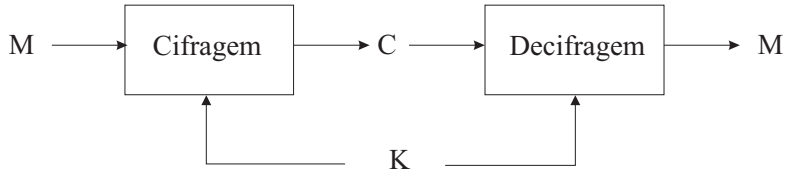


Figura B.1: Cifragem e decifragem com uma chave.

Algumas cifras, utilizam chaves diferentes para os processos de cifragem e de decifragem. Considere, portanto que na cifragem é utilizada a chave K_1 e na decifragem a chave K_2.

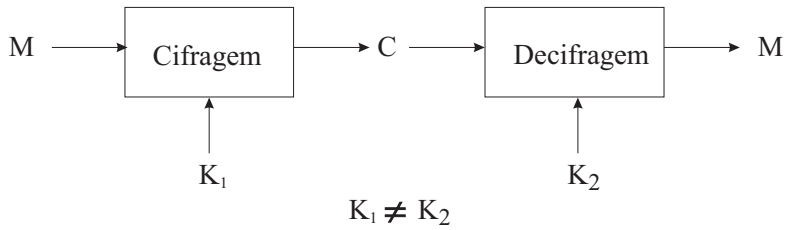


Figura B.2: Cifragem e decifragem com duas chaves distintas.

Assim,

$$E_{K_1}(M) = C. \tag{B.7}$$

$$D_{K_2}(C) = M. \tag{B.8}$$

Tais funções têm a propriedade ilustrada na Figura B.2:

$$D_{K_2}(E_{K_1}(M)) = M. \tag{B.9}$$

Na próxima seção serão abordados os diferentes tipos de cripto-sistemas.

B.2 Tipos de cripto-sistemas

Existem basicamente dois tipos de cripto-sistemas, o clássico, que surgiu desde a origem da escrita conhecido como **criptografia de chave secreta** ou **criptografia simétrica**, assim

chamada por ter apenas uma chave compartilhada pelos usuários que desejam se comunicar de forma segura, e a **criptografia de chave pública** ou **assimétrica**, assim chamada devido a existência de duas chaves, surgida na década de 70 e revolucionando a área.

B.2.1 Criptografia de chave pública

Até o momento foram abordados os cripto-sistemas clássicos, neles viu-se que os indivíduos interessados em trocar uma mensagem de forma segura compartilhavam apenas uma informação (chave) que tornava possível tanto a cifragem quanto a decifragem e que esta informação deveria ser mantida secreta uma vez que a segurança do cripto-sistema dependia dela. Essa informação compartilhada entre o remetente e o receptor do texto cifrado (ou criptograma) é a chave secreta, K, e como já visto, segundo o Princípio de Kerckhoff é nela que deve residir toda a segurança do cripto-sistema [3]. Como exposto no início da seção, este tipo de cripto-sistema também é conhecido como cripto-sistema simétrico (Figura B.1).

As cifras de chave secreta mais modernas são geralmente mistas usando operações de substituição e transposição (permutação) a fim de aumentar a segurança do cripto-sistema por meio da **confusão**[§] e **difusão**[¶][3,p.237].

Uma desvantagem dos cripto-sistemas simétricos está relacionada ao gerenciamento de chaves. Como em tal cripto-sistema a chave deve permanecer secreta, a distribuição de chaves deve ser feita de modo seguro, o que pode provocar um alto custo. Além disso, seu armazenamento e distribuição torna-se bastante problemático em grandes redes, uma vez que cada usuário do sistema deve possuir uma chave distinta para se comunicar com cada um dos outros usuários, ou seja, numa rede com n usuários seria necessário gerar $\begin{pmatrix} n \\ 2 \end{pmatrix} = \frac{n(n-1)}{2}$ chaves. Assim, por exemplo, num sistema com 1000 usuários se faz necessário 499.500 chaves, que devem ser trocadas e mantidas seguras. O uso de um centro para gerenciamento de chaves reduz para n o número de chaves secretas, requeridas para comunicação entre cada usuário e o centro. Quando solicitado, o centro fornece uma chave de sessão, para dois usuários cadastrados que quiserem se comunicar em segurança.

Foi pensando nesses problemas que, em 1976, dois pesquisadores da Universidade de Stanford, Whitfield Diffie e Martin E. Hellman, publicaram um trabalho [14] no qual introduziam

[§]Técnica usada para obscurecer a relação entre o texto claro e o texto cifrado, sendo a substituição o modo mais fácil de obtê-la.

[¶]Técnica usada para tornar a correlação da mensagem original com a mensagem cifrada tão complexa quanto possível, sendo obtida de modo mais simples com o uso de permutação.

uma idéia inovadora no campo da criptografia, a criptografia de chave pública. Ao introduzir a idéia de criptografia de chave pública, Diffie e Hellman [14] estavam não só apresentando uma solução para os problemas de gerenciamento e distribuição de chave como também para o da autenticidade, permitindo a utilização de um processo equivalente à assinatura escrita, conhecido como assinatura digital, promovendo a partir dele a integridade, não repudiação e autenticação da origem dos dados.

Esta classe de cripto-sistemas é caracterizada pela existência de duas chaves para cada usuário, sendo uma pública (E) e outra privada (D). Desta forma, tal cripto-sistema também foi chamado cripto-sistema assimétrico. Cada uma das chaves é utilizada em um dos processos sem que a chave D possa ser obtida a partir da chave E, não havendo assim a necessidade de uma troca de chave como no cripto-sistema simétrico.

A idéia geral que foi apresentada em [14] era o uso de uma função unidirecional com *trapdoor*, que são funções unidirecionais[‖] cujo inverso é encontrado facilmente por aqueles que possuem certa informação secreta (*trapdoor*). Neste tipo de função unidirecional a chave pública dá uma informação geral sobre a função, que pode ser de conhecimento público, enquanto que a chave privada é o *trapdoor*. Assim, quem possui a chave privada e a chave pública pode calcular a função em ambas as direções (direta e inversa) facilmente, enquanto os possuidores apenas da chave pública só terão facilidade no cálculo na direção direta. Logo, a direção direta é usada para cifrar e verificar a assinatura digital e a direção inversa para decifrar e gerar a assinatura digital.

No trabalho apresentado por Diffie e Hellman nenhum cripto-sistema foi proposto, só algum tempo depois começaram a surgir propostas considerando o uso de funções unidirecionais. Alguns dos cripto-sistemas propostos foram baseados nos seguintes problemas matemáticos:

- Logaritmo discreto
- Problema da mochila
- Fatoração de inteiros

No decorrer dos anos, alguns cripto-sistemas de chave pública foram quebrados, e outros foram provados não práticos. Atualmente, apenas três tipos de cripto-sistemas assimétricos podem ser considerados seguros e eficientes. Esses cripto-sistemas se baseiam nos seguintes

[‖]Diz-se que uma função é unidirecional se ela é difícil de ser invertida. Entenda-se por "difícil de ser invertida" se dado o resultado $f = F(x)$ é computacionalmente inviável encontrar x dado f.

problemas: **Fatoração de inteiros**, **Problema do logaritmo discreto sobre corpos finitos (PLD)** e **Problema do logaritmo discreto sobre curvas elípticas (PLDCE)**. Para maiores detalhes sobre os cripto-sistemas assimétricos baseados nestes problemas consultar, [14]-[23].

B.2.2 Cripto-sistemas de chave secreta

Apesar de todas as vantagens da criptografia de chave pública apontadas com relação aos cripto-sistemas assimétricos existe uma desvantagem que muitas vezes é crucial em algumas aplicações, em especial naquelas em que o tempo de processamento de grande quantidade de informações é extremamente importante.

Como os cripto-sistemas assimétricos são baseados em problemas em que estão envolvidos números grandes, como é o caso, por exemplo, dos cripto-sistemas baseados no problema da fatoração de inteiro em que são necessários primos da ordem de 150 a 200 dígitos, a velocidade desse tipo de cripto-sistemas, se comparado a cripto-sistemas simétricos, chega a uma desvantagem da ordem de Mbps ou até Gbps. Assim, o que ocorre na prática é a união da vantagem dos dois tipos de cripto-sistemas, considerando a aplicação, implicando geralmente no uso de um cripto-sistema assimétrico no momento da autenticação das partes envolvidas e no processo de troca de chave e só então iniciando a cifragem dos dados utilizando um cripto-sistema simétrico.

Até a década de 90 o DES (*Data Encryption Standard*) foi o padrão de cifra simétrica para os EUA.

Após quase quatro anos de competições, em 2 de Outubro de 2000, o NIST (*National Institute of Standards and Technology*) anunciou o AES (*Advanced Encryption Standard*) [24], cifra substituta do DES. O processo de seleção contou inicialmente com 15 algoritmos que foram eliminados gradualmente por meio de participação e comentários públicos [25].

O AES, formalmente conhecido como Rijndael [26], foi escolhido na fase final entre cinco finalistas. Os outros quatro finalistas, MARS [27], RC6 [28], Serpent [29] e Twofish [30], foram considerados suficientemente seguros cabendo a resolução final a dois fatores adicionais:

1) Eficiência computacional e requisito de memória numa grande variedade de *softwares* e *hardwares*, incluindo *smart cards*;

2) Flexibilidade, simplicidade e facilidade de implementação.

A partir de então a cifra Rijndael vem sendo usada como padrão sem mostrar até o momento qualquer vulnerabilidade.

Na seção a seguir (seção B.3) são mostradas algumas das idéias introduzidas por Shannon no seu trabalho [10] em que foi feita uma análise de cripto-sistemas simétricos utilizando princípios da teoria da informação introduzidos por ele em [11].

B.3 Shannon e os sistemas de sigilo

Logo após a apresentação do revolucionário trabalho de Shannon [11] no qual era introduzida a teoria da informação, um outro trabalho usando a teoria ali introduzida aplicada a sistemas de sigilo foi apresentado [10].

O tratamento dado nesse trabalho foi direcionado a "verdadeiros" sistemas de sigilo em que o significado da mensagem é escondido por uma cifra ou código**, a existência de tal sistema de sigilo não é omitida, e assume-se que o inimigo possui qualquer equipamento especial necessário para interceptar e gravar o sinal transmitido. Além disso, o estudo foi limitado para o caso da informação discreta, i.e., a mensagem a ser cifrada consiste numa seqüência de símbolos discretos, cada um escolhido num conjunto finito de símbolos.

O artigo [10] é dividido em três partes:

- A primeira parte trata da estrutura matemática básica dos sistemas de sigilo, sendo iniciada pela criação de um modelo matemático de um sistema de sigilo, seguido da análise de sistemas criptográficos conhecidos, como as cifras de substituição simples, polialfabéticas, etc.

  Nesta parte também foram enumerados e comentados os cinco mais importantes critérios a serem usados na estimação do valor de um cripto-sistema proposto, sendo eles: quantidade de sigilo, comprimento da chave, complexidade das operações de cifragem e decifragem, propagação de erros e expansão da mensagem.

- A segunda parte trata do problema do "sigilo teórico", considerando questões como "Quão seguro um cripto-sistema é contra criptoanálise, uma vez que o inimigo tem tempo e recursos ilimitados para a análise dos textos cifrados interceptados?".

  Shannon observou que tal problema está relacionado a questões de comunicação na presença de ruído, e os conceitos de entropia e equivocação desenvolvidos em [11] para sistemas de

**um código é definido como uma substituição de palavras (algumas vezes sílabas) por um grupo de letras substitutas [10,p.667], enquanto que cifra é uma substituição de símbolos.

comunicação achavam aplicação direta em criptoanálise. Conceitos como "sigilo perfeito", "cifra ideal" e "cifra fortemente ideal" foram introduzidos no artigo.

- Para finalizar o artigo, foi considerado o caso do "sigilo prático". Dois sistemas utilizando chaves de mesmo comprimento podem ser solucionados de forma única quando N letras forem interceptadas, porém o volume de trabalho necessário para isso pode diferir bastante. Nessa parte uma análise sobre as fraquezas básicas dos sistemas de sigilo é feita, levando a métodos para a construção de sistemas de sigilo que vão demandar uma grande quantidade de trabalho para serem solucionados. Finalizando, incompatibilidades entre as várias qualidades desejadas para os sistemas de sigilo são discutidas.

B.3.1 Sigilo teórico

Quão imune à criptoanálise um cripto-sistema é, considerando que o criptoanalista tem tempo e recursos ilimitados disponíveis para a análise dos textos cifrados interceptados?

Um criptograma (texto cifrado) tem uma única solução (mesmo que seja necessária uma quantidade impraticável de trabalho para encontrá-la) e se não, quantas soluções aceitáveis existem?

Quanto texto cifrado deve ser interceptado num dado sistema a fim de se encontrar uma solução única?

Existem sistemas para os quais nunca se obtém uma solução única independente da quantidade de texto interceptado?

Para questões como essas os conceitos de entropia, redundância, assim como outros relacionados à área de teoria da informação acham grande aplicação.

Esquema de Shannon para um sistema de sigilo

Considere o esquema geral de um sistema de sigilo, originalmente introduzido por Shannon em [10](Figura B.3). No transmissor existem duas fontes, uma fonte de mensagem e uma fonte de chave. Como se observa, nesse esquema a chave é transmitida por algum meio seguro para poder ser compartilhada pelas pessoas envolvidas na comunicação, ficando claro aí que se trata de um cripto-sistema simétrico, o que é natural uma vez que, como já visto, a idéia de cripto-sistema assimétrico só foi introduzida quase trinta anos após o trabalho de Shannon sobre sigilo.

E_K e D_K denotam, respectivamente, as operações de cifragem e decifragem feitas utili-

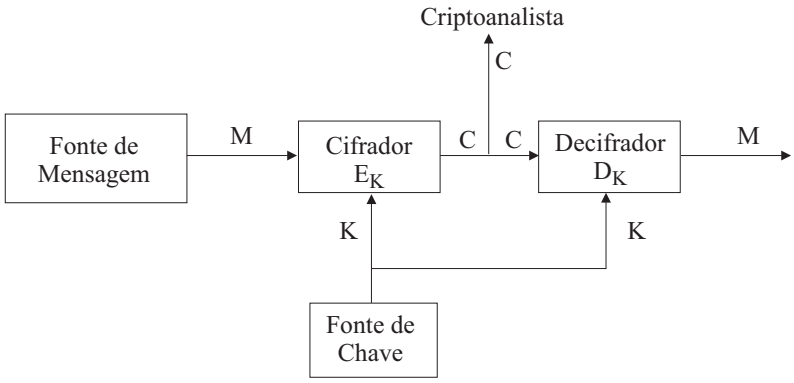


Figura B.3: Esquema geral de um sistema de sigilo segundo Shannon.

zando a chave K, M denota o texto claro, C o texto cifrado (criptograma).

Portanto, as operações de cifragem e decifragem são dadas respectivamente pelas expressões (B.4) e (B.5).

B.3.2 Sigilo perfeito

Suponha que as possíveis mensagens são finitas em número, i.e., $M_1, M_2, \ldots, M_n$ com probabilidades *a priori* $P(M_1), P(M_2), \ldots, P(M_n)$, sendo cifradas nos possíveis criptogramas $C_1, C_2, \ldots, C_n$ por

$$C = E_K(M).$$

O criptoanalista intercepta um C particular e pode então calcular, pelo menos em princípio, as probabilidades *a posteriori* para as várias mensagens, $P(M|C)$. É natural, portanto, definir "sigilo perfeito" pela condição que, para todo C as probabilidades *a posteriori* são iguais às probabilidades *a priori*. Nesse caso, interceptar a mensagem não fornece informação alguma ao criptoanalista.

Uma condição suficiente e necessária para se alcançar sigilo perfeito é demonstrada a seguir.

Pelo Teorema de Bayes,

$$P(M|C) = \frac{P(M)P(C|M)}{P(C)},$$

na qual

$P(M)$ = probabilidade *a priori* da mensagem M,

$P(C|M)$ = probabilidade condicional do criptograma C se a mensagem M é escolhida, i.e., a soma das probabilidades de todas as chaves que produzem o criptograma C a partir da mensagem M,

$P(C)$ = probabilidade de ocorrer o criptograma C,

$P(M|C)$ = probabilidade *a posteriori* da mensagem M ter sido enviada, quando o criptograma C é interceptado.

Para o sigilo perfeito $P(M|C)$ deve ser igual a $P(M)$ $\forall C, M$. Assim, ou $P(M) = 0$ (solução que deve ser excluída uma vez que se deseja que a igualdade seja válida independente dos valores de $P(M)$) ou

$$P(C|M) = P(C),$$

$\forall M, C$. Por outro lado, se $P(C|M) = P(C)$ então

$$P(M|C) = P(M),$$

e o sigilo perfeito é alcançado. Como resultado,

Teorema 6 *Uma condição necessária e suficiente para o sigilo perfeito é que*

$$P(C|M) = P(C),$$

$\forall M, C$. *Isto é,* $P(C|M)$ *deve ser independente de* M.

Vê-se que só é possível alcançar sigilo perfeito se "o número de chaves diferentes for pelo menos tantos quantos são os Ms" [10,p.681], i.e., para que um cripto-sistema possa alcançar o sigilo perfeito é necessário que o mesmo use chaves aleatórias e que não se repitam. O cripto-sistema que obedece a este princípio é conhecido como cripto-sistema de bloco descartável (*one-time pad*). Devido à grande quantidade de chaves que precisam ser geradas nesse tipo de cripto-sistema ele só se torna prático para quem necessita de comunicação ultra-secreta e que tenha recursos necessários para os enormes custos de geração e distribuição das chaves. Por exemplo, a linha de comunicação entre o presidente dos EUA e da Russia tem sua segurança baseada numa cifra de bloco descartável *one-time pad* [13,p.124].

B.3.3 Equivocação

Antes que qualquer material seja interceptado pode-se estimar as probabilidades *a priori* relacionadas às várias possíveis mensagens, e às várias chaves. A partir do momento que

algum material é interceptado, o criptoanalista calcula as probabilidades *a posteriori*; e com o crescimento de N (quantidade de texto interceptado) as probabilidades de certas mensagens ocorrerem cresce também, enquanto que a probabilidade das mensagens restantes decresce até que finalmente reste apenas uma, que terá probabilidade próxima de um, enquanto que as outras possíveis mensagens terão probabilidades próximas de zero.

O conjunto de probabilidades *a posteriori* descreve quanto o conhecimento do criptoanalista sobre a mensagem e a chave se torna mais preciso à medida que material cifrado é obtido. Uma situação similar ocorre na teoria da comunicação quando um sinal transmitido é perturbado por ruído. É necessário, neste caso, estabelecer uma medida apropriada da incerteza do que foi realmente transmitido conhecendo apenas a versão perturbada dada pelo sinal recebido. Em [11] foi mostrado que a medida matemática natural desta incerteza é a entropia condicional (Definição 9) do sinal transmitido quando o sinal recebido é conhecido. Essa entropia condicional foi denominada **equivocação**.

Com essas considerações em mente é natural usar a equivocação como um índice para sigilo teórico. Nota-se que existem dois tipos significativos de equivocação, uma relacionada à chave ($H(K|C)$) e outra à mensagem ($H(M|C)$), dadas respectivamente por:

$$H(K|C) = -\sum_{C,K} P(C,K) \log P(K|C)$$

$$H(M|C) = -\sum_{C,M} P(C,M) \log P(M|C)$$

nas quais

C, M e K denotam respectivamente o criptograma, a mensagem e a chave,

$P(C,K) =$ a probabilidade conjunta da chave K e do criptograma C,

$P(K|C) =$ a probabilidade *a posteriori* da chave K dado que o criptograma C é interceptado,

$P(C,M) =$ a probabilidade conjunta da mensagem M e do criptograma C,

$P(M|C) =$ a probabilidade *a posteriori* da mensagem M dado que o criptograma C é interceptado.

A soma em $H(K|C)$ é feita sobre todos os possíveis criptogramas de certo comprimento (por exemplo, N). Assim, tanto $H(K|C)$ quanto $H(M|C)$ são funções de N, o número de símbolos interceptados, sendo às vezes escrito explicitamente como $H(K|C,N)$ e $H(M|C,N)$, respectivamente.

Os mesmos argumentos usados no Apêndice A para justificar o uso da equivocação (entropia condicional) como medida de incerteza se aplica também aqui. Assim, equivocação zero significa que uma mensagem (ou chave) tem probabilidade um e todas as outras mensagens (ou chaves) zero, correspondendo, portanto ao conhecimento completo. Considerada como uma função de N, o decréscimo gradual da equivocação corresponde ao crescimento do conhecimento sobre a mensagem ou chave original. A curva de equivocação desenhada como função de N é chamada característica de equivocação do sistema de sigilo considerado.

Logo, do exposto, se conclui que todas as propriedades já mostradas e analisadas no Apêndice A com relação à entropia condicional (equivocação) são naturalmente válidas para $H(K|C,N)$ e $H(M|C,N)$.

Viu-se que para obter sigilo perfeito é necessário que a quantidade de possíveis chaves (espaço de chaves) seja pelo menos igual à quantidade de possíveis mensagens (espaço de mensagens), o que seria uma quantidade infinita caso fosse permitido um comprimento ilimitado para a mensagem. Com um espaço de chaves limitado, a função equivocação da chave e a equivocação de mensagem geralmente se aproximam de zero quando N cresce. Na verdade é possível que em alguns casos $H(K|C)$ se mantenha constante no valor inicial $H(K)$. Então, independente da quantidade da material interceptado, não há uma única solução mas sim várias soluções com probabilidades comparáveis. Desta forma, a partir da equivocação de chave Shannon definiu o que seria um "cripto-sistema ideal" e o que seria um " cripto-sistema fortemente ideal".

Definição 30 *(**Função Equivocação de Chave**) Segundo Shannon [10], a função equivocação da chave, $f(N) = H(K|C)$, de um sistema criptográfico de chave secreta é a entropia condicional da chave dados os N primeiros dígitos do texto cifrado C, i.e., $f(N) = H(K|C)$, sendo, portanto a medida do número de valores da chave secreta K que são consistentes com os primeiros N dígitos de texto cifrado C. Como $f(N)$ decresce à medida que N cresce, Shannon chamou um cripto-sistema de **ideal** se $f(N)$ se aproxima de um valor positivo, quando N tende para o infinito ($\lim_{N\to\infty} f(N) = A$, $A > 0$) e de **fortemente ideal** se $f(N)$ é constante e igual a $H(K)$, i.e., $f(N) = H(K|C) = H(K)$ para todo N, o que é equivalente a dizer que a seqüência de texto cifrado é estatisticamente independente da chave (Vide gráfico na Figura B.4)* .

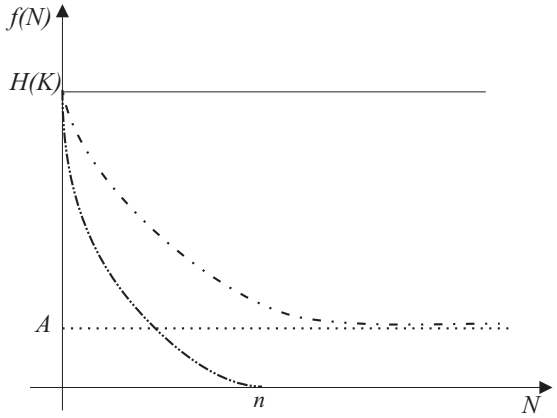


Figura B.4: Gráfico da função equivocação.

B.3.4 Redundância da linguagem

Associado a uma linguagem existe um parâmetro δ chamado de redundância da linguagem, desta forma δ mede quanto texto em certa linguagem pode ser reduzido em comprimento sem haver perda de informação [7].

A fim de definir matematicamente considere as seguintes medidas.

Definição 31 *(Taxa da linguagem) Define-se a taxa da linguagem, para mensagens de comprimento N como*

$$\tau = \frac{H(X)}{N}, \tag{B.10}$$

em que X representa o alfabeto da linguagem.

Esta taxa não é nada mais que a incerteza média por símbolo, i.e., considerando em binário, o número médio de *bits* de informação em cada símbolo (Apêndice A). Para a língua inglesa considerando N grande, $1 \leq \tau \leq 1,5$ *bit*/símbolo. Shannon estimou τ em 1,2.

Definição 32 *(Taxa absoluta da linguagem) Define-se a taxa absoluta da linguagem como a informação máxima que pode ser obtida por símbolo do alfabeto da linguagem considerada.*

$$\Upsilon = \log L, \tag{B.11}$$

em que L é o número de símbolos do alfabeto da linguagem considerada.

Tal definição é natural uma vez que no Apêndice A viu-se que a informação máxima de certa fonte de informação X que possui um alfabeto com L símbolos é dada por $\log L$ o que ocorre quando todos os seus símbolos são equiprováveis. Sabe-se porém que os símbolos numa

linguagem não são equiprováveis, então define-se redundância de uma linguagem da seguinte forma.

Definição 33 *(Redundância) Define-se a redundância da linguagem como a diferença entre a taxa absoluta (B.11) e a taxa da linguagem (B.10), i.e.,*

$$\delta = \Upsilon - \tau. \tag{B.12}$$

Por exemplo, para um alfabeto com $L = 23$ símbolos $\Upsilon = 4,52$ bits/símbolos, considerando $\tau = 1$ e $\delta = 3,52$, mostrando por meio da razão δ/Υ que a língua inglesa é, neste caso, $77,88\%$ redundante. Ao considerar $\tau = 1,5$, $\delta = 3,02$, implica em uma língua $66,81\%$ redundante.

B.3.5 Distância de unicidade

Definição 34 ***(Distância de unicidade)***[††] *A distância de unicidade é o menor N tal que $H(K|C)$ se aproxima de zero, i.e., N é a quantidade de texto que deve ser interceptado a fim de determinar unicamente a chave.*

Um cripto-sistema é dito incondicionalmente seguro se H(K|C) nunca se aproxima de zero mesmo que N seja muito grande, i.e., não importando a quantidade de texto cifrado interceptado. Note que Shannon usou o termo "cripto-sistema ideal"(Definição 30) para descrever os cripto-sistemas que apesar de não proporcionarem "sigilo perfeito"(cripto-sistema fortemente ideal) são mais resistentes à criptoanálise na medida que não fornecem informação suficiente para a obtenção da chave.

No Capítulo 2 é introduzida uma técnica que transforma qualquer cifra de chave secreta não-expansível[‡‡] numa cifra fortemente ideal, obtendo-se desta forma, um cripto-sistema incondicionalmente seguro.

Referências

[1] G. Zorpette,"Breaking the Enemy's Code", IEEE Spectrum, pp. 47-51, September 1987.

[2] A. S. Tanenbaum, "Computer Network", 3rd edition, Prentice Hall, 1996.

[3] B. Schneier, *Applied Cryptography Second Edition: protocols, algorithms and source in C*,Wiley Publishing, Inc., 1996.

[††]Na Figura B.4 n ilustra o valor da distância de unicidade

[‡‡]Uma cifra é dita não-expansível quando o texto claro e o texto cifrado possuem o mesmo comprimento.

[4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[5] W. Mao, *Modern Cryptography - Theory & practice*, Prentice Hall PTR, 2004.

[6] N. Fergunson and B. Schneier, *Practical Cryptography*, Wiley Publishing, Inc., 2003.

[7] D. E. R. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, Inc., 1983.

[8] An Introduction to Information Security; A Certicom White Paper; 1997. *http://www.certicom.com*

[9] N. Koblitz, *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics, Springer-Verlag, 2004.

[10] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Tech. J.*, vol.28, pp. 656-715, Oct. 1949.

[11] C. E. Shannon, "A mathematical theory of communication (parts I and II)". *Bell System Technical Journal*, XXVII:379-423.

[12] *New Enciclopaedia Britannica*, vol. 16, 15th edition, pp. 913-924B, 1986.

[13] S. Singh, *The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography.* Doubleday, 1999.

[14] W. Diffie and M. Hellman,"New Directions in Cryptography'", IEEE Transactions on Information Theory, Vol. IT.22, No. 6, pp. 644-654, November 1976.

[15] D. P. B. de A. Camara, "Criptografia de Chave Pública baseada em Curvas Elípticas com Aplicações", Dissertação de mestrado, Depto. de Eletrônica e Sistemas, Universidade Federal de Pernambuco, 2001.

[16] J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Advances in Computer Science Series, Prentice Hall, 1989.

[17] RSA Laboratories'Frequently Asked Questions About Today's Cryptography, versão 4.1, 2000.

[18] H. W. Lenstra Jr., "Factoring Integers with Elliptic Curves", *Annuals of Mathematics*, 126, pp. 649-673, 1987.

[19] J. P. Buhler, H. W. Lenstra and C. Pomerance, "The development of Number Field Sieve", *Lectures Notes in Computer Science*,Volume 1554, Springer-Verlag, 1994.

[20] J. Buchmann, J. Loho, and J. Zayer, "An Implementation of the General Number Field Sieve", *Advances in Cryptology Crypto 93'*, pp. 159-166, 1984.

[21] R. L.Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communications of the ACM*, 21(2), pp. 120- 126, February 1978.

[22] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, Vol. IT.31, No. 4, pp. 469-481, July 1985.

[23] D. Johnson e A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", *Technical Report CORR 99-31*, Depto. of C&O, University of Waterloo, Canada, 23 de Agosto de 1999. http://www.cacr.math.uwaterloo.ca

[24] AES home page, http://www.nist.gov/aes.

[25] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, *Report on the Development of the Advanced Encryption Standard (AES)*, Computer Security Division, Information Thecnology Laboratory, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Outubro 2000. http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

[26] J. Daemen e V. Rijman, AES Proposal: Rijndael, NIST AES Proposal, versão 2, Setembro 1999.

[27] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford, N. Zunic, *MARS: a candidate for AES*, IBM Corporation, Revised, 22 de Setembro 1999. http://www.research.ibm.com/ security/mars.pdf

[28] R. Rivest, M. Robshaw, R. Sidney e Y. Yin, *The RC6 Block Cipher*, Agosto 1998. ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/rc6v11.pdf

[29] R. Anderson, E. Biham e L. Knudsen, *Serpent: A Proposal for the Advanced Encryption Standard*, NIST AES Proposal, Junho 1998. http://www.cl.cam.ac.uk/ rja14/serpent.html

[30] B. Scheneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-Bit Block Cipher, 15 Junho de 1998. http://www.counterpane.com/twofish.pdf

APÊNDICE C

ALGORITMO MAX-ENT POR PASSO

C.1 Descrição do Algoritmo MAX-ENT por passo

Seja $\Pi_D = \{\pi_0, \pi_1, \ldots, \pi_{D-1}\}$ a distribuição de probabilidade dos dígitos das palavras de homofonema. Os homofonemas são selecionados como nós terminais na árvore D-ária enraízada T com probabilidades, de tal modo que de cada nó emanam D ramos com probabilidades $\pi_0, \pi_1, \ldots, \pi_{D-1}$, respectivamente. O rótulo de um caminho em T é representado por uma seqüência D-ária, formada pelos números inteiros $0, 1, 2, \ldots, D-1$, associada aos ramos que constituem este caminho. Denote-se por $\pi_0^{\lambda_0}, \pi_1^{\lambda_1}, \ldots, \pi_{D-1}^{\lambda_{D-1}}$ a probabilidade de um caminho em T, de comprimento $\sum_{i=0}^{D-1} \lambda_i$ dígitos, contendo λ_i vezes o dígito i, $0 \leq i \leq D-1$. Para uma dada fonte o algoritmo MAX-ENT simultaneamente encontra a decomposição da probabilidade de cada símbolo da fonte, como uma soma finita ou infinita de termos $\pi_0^{\lambda_0}\pi_1^{\lambda_1}\ldots\pi_{D-1}^{\lambda_{D-1}}$, e a correspondente palavra livre de prefixo, na qual o dígito i, $0 \leq i \leq D-1$ ocorre λ_i vezes. Denote-se por $v(i,j)$ o j-ésimo homofonema alocado ao símbolo da fonte u_i, $1 \leq i \leq K$, $j = 1, 2, \ldots$, e denotemos por $\alpha(i,j)$ a probabilidade de $v(i,j)$.

Definição 35 *Define-se a soma corrente de símbolo $\gamma_m(i)$ para $U = u_i$ na m-ésima iteração do algoritmo MAX-ENT como*

$$\gamma_m(i) = P_U(u_i) - \sum_{k=1}^{j-1} \alpha(i,k),$$

com $\gamma_m(i) = P_U(u_i)$ para $j = 0$, na qual j denota o número de homofonemas alocados a u_i

até a m-ésima iteração.

Definição 36 *Define-se o conjunto de soma corrente* Γ_m *na m-ésima iteração do algoritmo MAX-ENT como*

$$\Gamma_m = \{\gamma_m(i) | \gamma_m(i) > 0, 1 \leq i \leq K\},$$

com $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

Seja $\gamma_{\max} = \max\ \gamma_m(i) \in \Gamma_m,\ 1 \leq i \leq K$. Quando $m = 0$ no algoritmo MAX-ENT constroi-se T a partir da raiz, começando com apenas D folhas. Daí então nós expande-se cada nó terminal em T, cuja probabilidade exceda $\gamma_{\max}$, em um número mínimo de ramos suficiente para fazer com que as probabilidades dos nós terminais extendidos resultantes sejam iguais ou menores que $\gamma_{\max}$. Chama-se a árvore resultante de *árvore D-ária enraízada e processada com probabilidades*, T_p. Na m-ésima iteração, $m \geq 1$, um homofonema é alocado a um nó terminal da correspondente T_p, de modo que o nó terminal não utilizado que possua a maior probabilidade, denotada por P_M, seja alocado como um homofonema para o símbolo u_r que apresente o mínimo valor não negativo para a diferença entre sua soma corrente de símbolo $\gamma_m(r)$ e P_M, i.e., tal que $\min_i\{\gamma_m(i) - P_M | (\gamma_m(i) - P_M) \geq 0\} = \gamma_m(r) - P_M \geq 0,\ 1 \leq i \leq K$.

1. Faça $m = 0$. Seja Γ_0 o conjunto cujos elementos são as probabilidades dos símbolos $P_U(u_i),\ 1 \leq i \leq K$, ordenados em ordem decrescente.

2. Determine $\gamma_{\max}$ e construa a árvore D-ária enraízada e processada T_p, com probabilidades, para a m-ésima iteração expandindo na árvore construída para a $(m-1)$-ésima iteração, $m \geq 1$, cada nó terminal não usado cuja probabilidade exceda $\gamma_{\max}$, em um número mínimo de ramos suficiente para fazer a probabilidade dos nós terminais resultantes menores ou iguais a $\gamma_{\max}$. Faça $(i, j) = (i, 1)$ e $\gamma_0(i) = P_U(u_i),\ 1 \leq i \leq K$.

3. Encontre em T_p o caminho não usado E_l cuja probabilidade $P(E_l)$ é a maior dentre aquelas dos caminhos não-usados, i.e., $P(E_l) = P_M$. Denote-se por l o comprimento de E_l.

4. Seja u_r o símbolo da fonte ao qual corresponde a máxima soma corrente de símbolo $\gamma_{\max}$ na m-ésima iteração. Associe a u_r o homofonema (nó terminal) $v(r, j)$ e a palavra D-ária de homofonema de comprimento l, cujos símbolos constituem o rótulo de E_l in T_p. Isto implica $\alpha(r, j) = P(E_l)$. Faça $(r, j) \leftarrow (r, j + 1)$. Calcule a soma corrente de símbolo $\gamma_m^{'}(r)$ após esta decomposição e faça $\Gamma_m^{'} = \Gamma_m - \{\gamma_{\max}\}$. Se $\gamma_m^{'}(r) = 0$

então faça $\Gamma_{m+1} = \Gamma_m^{'}$. A decomposição de $P_U(u_r)$ estará agora concluída e conterá j homofonemas, e se $\Gamma_{m+1} = \phi$ então FIM. Em caso contrário, i.e., se $\gamma_m^{'}(r) > 0$ então faça $\Gamma_{m+1} = \Gamma_m^{'} \cup \{\gamma_m^{'}(r)\}$.

5. Faça $m \leftarrow m + 1$.

6. Vá para o passo 2.

APÊNDICE D

ALGORITMO MIN-ENT POR PASSO

D.1 Descrição do Algoritmo MIN-ENT por passo

São apresentados a seguir os passos do algoritmo MIN-ENT [38], seguindo a mesma notação do apêndice C.

O algoritmo consiste dos seguintes passos:

1. Faça $m = 0$. Faça $\gamma_0(i) = P_U(u_i)$, $1 \leq i \leq K$. Faça $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

2. Determine $\gamma_{\max}$ e construa a árvore T_p para a m-ésima iteração expandindo cada nó terminal não usado na árvore construída para a $(m-1)$-ésima iteração, $m \geq 1$, cuja probabilidade exceda $\gamma_{\max}$, em um número mínimo de ramos suficiente para fazer a probabilidade dos nós terminais resultantes menores ou iguais a $\gamma_{\max}$.

3. Encontre em T_p, o caminho não usado E_l cuja probabilidade $P(E_l)$ seja a maior dentre as dos caminhos não usados, i.e., $P(E_l) = P_M$. Denote-se por l o comprimento de E_l.

4. Se, para $1 \leq i \leq K$, $\min_i\{\gamma_m(i) - P_m | (\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0$, então associa-se a u_r o homofonema (nó terminal) $v(r, j)$ e a palavra de homofonema D-ária de comprimento l, cujos símbolos constituem o rótulo de E_l em T_p. Isto implica $\alpha(r, j) = P_M$. Compute a soma corrente de símbolo $\gamma_m^{'}(r)$ após esta decomposição e faça $\Gamma_m^{'} = \Gamma_m - \{\gamma_m(r)\}$. Se $\gamma_m^{'}(r) = 0$ então faça $\Gamma_{m+1} = \Gamma_m^{'}$. A decomposição de $P_U(u_r)$ estará agora concluída e conterá j homofonemas, e se $\Gamma_{m+1} = \phi$ então FIM. Em caso contrário, i.e., se $\gamma_m^{'}(r) > 0$, então faça $\Gamma_{m+1} = \Gamma_m^{'} \cup \{\gamma_m^{'}(r)\}$.

5. Faça $m \leftarrow m + 1$.

6. Vá para o passo 2.

APÊNDICE E

SBT'04 - GERAÇÃO DE UMA DISTRIBUIÇÃO DISCRETA USANDO MOEDAS DESBALANCEADAS

Trabalho apresentado no XXI Simpósio Brasileiro de Telecomunicações-SBT'04, 06-09 de setembro de 2004, Belém, PA.

Danielle P. B. de A. Camara, Valdemar C. da Rocha Jr e Cecílio Pimentel

Resumo - A geração eficiente de uma distribuição de probabilidade discreta é de interesse atual nas áreas de criptografia e de geração de números aleatórios, para testes e simulação de sistemas de comunicações. Neste trabalho é apresentado um algoritmo para gerar uma distribuição discreta através do lançamento de duas ou mais moedas, sendo algumas delas desbalanceadas. Em particular, esta abordagem contribui com uma solução alternativa do problema clássico da geração de uma distribuição discreta uniforme usando duas ou mais moedas desbalanceadas.
Palavras-chave: Geração de números aleatórios, criptografia, teoria da informação.

Abstract - The efficient generation of a discrete probability distribution is of current interest in the areas of cryptography and random number generation. This paper presents an algorithm for generating a discrete distribution using two or more coins, being one of them unbiased. In particular, this approach contributes

to an alternative solution to the classical problem of generating a discrete uniform probability distribution using two or more unbiased coins.

Keywords - Random number generation, cryptography, information theory.

E.1 Introdução

O problema da geração de uma distribuição de probabilidade discreta usando lançamentos de uma moeda desbalanceada é antigo e de grande importância nas áreas de criptografia e de geração de números aleatórios, usados para testes e simulação de sistemas de comunicações, assim como em muitas outras aplicações computacionais. Há mais de quarenta anos von Neumann [1] introduziu um algoritmo simples para gerar uma seqüência de bits estatisticamente independentes e equiprováveis a partir do lançamento de uma moeda com viés desconhecido. A partir daí, muitos pesquisadores têm considerado o problema e estudado a geração de variáveis aleatórias uniformes sob diferentes pontos de vista [2]-[11].

Basicamente, dois aspectos são levados em conta neste tipo de problema: a geração considerando um tempo limite curto (*short bounded time*) ou mais tradicionalmente considerando um tempo esperado curto, que será o nosso caso. Feldman et al. [12] provaram em seu trabalho, entre outros resultados, que os resultados do lançamento de um dado honesto de n faces, i.e., os valores de uma variável aleatória que assume n valores equiprováveis, podem ser simulados em um intervalo de tempo limitado usando lançamentos de apenas um tipo de moeda, com distribuição racional apropriada de cara e coroa, se e só se, n é uma potência de 2 ([12], teorema 2), e que um dado honesto de n faces sempre pode ser simulado usando duas moedas, com distribuição de cara e coroa apropriadas, usando no máximo $\lceil 2 \log n \rceil + 1$ lançamentos, onde $\lceil x \rceil$ denota o menor número inteiro maior ou igual a x.

Um dos resultados obtidos por Gargano e Vaccaro [13] foi a melhoria de tal cota. Através do algoritmo proposto em [13], a geração de um dado honesto de n faces usando duas moedas, sendo uma delas honesta e a outra com viés, é feita com um número máximo de lançamentos igual a

$$1 + \lfloor \log n \rfloor + \lceil \log(n - 2^{\lfloor \log n \rfloor}) \rceil + pw(n) \tag{E.1}$$

e um número médio de lançamentos igual a

$$\begin{aligned} 1 + \lfloor \log n \rfloor + (2^{pw(n)}/n)(\lceil \log r(n) \rceil 2^{\lceil \log r(n) \rceil} \\ - r(n)(\lfloor \log r(n) \rfloor - pw(n))), \end{aligned} \tag{E.2}$$

onde $pw(n)$ =max$\{i : 2^i$ divides $n\}$ (Teorema 1, [13]).

Na *Seção E.2* introduzimos um novo algoritmo para a geração de uma distribuição de probabilidade discreta através do lançamento de duas ou mais moedas, algumas delas com viés (ou desbalanceadas). Convém ressaltar que o algoritmo proposto por Gargano e Vaccaro é específico para uma dada escolha de moedas. Na *Seção E.3* a aplicação deste algoritmo será ilustrada através de exemplos, nos quais gera-se uma distribuição de probabilidade uniforme usando duas moedas, uma honesta e outra desbalanceada. Finalizando, na *Seção E.4* apresentaremos algumas conclusões sobre este trabalho, assim como sugestões para pesquisas futuras.

E.2 Novo algoritmo

O algoritmo introduzido em [14] trata de um esquema de substituição homofônica no qual cada palavra binária de homofonema tem como símbolos variáveis aleatórias independentes e identicamente distribuídas, obedecendo a uma distribuição de probabilidade arbritária. Em outras palavras, trata da geração de uma distribuição de probabilidade discreta através do uso de apenas uma moeda com viés.

Nossa proposta nesta seção é a generalização do algoritmo MIN-ENT por passo apresentado em [14], a fim de gerar uma distribuição discreta, utilizando duas ou mais moedas com viés, obtendo resultados equivalentes aos obtidos por Gargano e Vaccaro [13], com a diferença de não necessariamente usar a distribuição de cara e coroa dependente de n, como no algoritmo sugerido em [13].

E.2.1 Descrição do algoritmo

O algoritmo aqui proposto segue essencialmente os mesmos passos daquele apresentado em [14] com a importante distinção de que, ao invés de usar apenas uma moeda, são usadas duas ou mais moedas e a cada passo observa-se qual moeda deve ser escolhida para lançamento, levando em conta a minimização da entropia naquele passo.

Sejam $m_1 = \{p_1, 1-p_1\}$, $m_2 = \{p_2, 1-p_2\}$, $\ldots$, $m_r = \{p_r, 1-p_r\}$ as distribuições de probabilidade das moedas e $P_U = P_U(u_1), \ldots, P_U(u_K)$ a distribuição de probabilidade a ser gerada.

Segue-se a descrição do algoritmo proposto.

1. Lançar cada uma das moedas, associando a cada uma delas uma árvore.

2. Para cada uma das árvores, verificar se a maior probabilidade dos ramos é menor ou igual ao maior valor de $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

   (Obs: Depois da primeira iteração será considerada uma expressão Γ, em substituição a Γ_0, a qual é descrita em detalhes no apêndice.)

   (a) Se alguma(s) árvore(s) verificar(em) esta condição, manter a(s) mesma(s) e eliminar as outras. Continuar o algoritmo aplicando às árvores que foram mantidas o procedimento indicado no Apêndice A.

   (b) Caso contrário, ir para o passo 3.

3. Fazer a expansão de cada árvore, considerando todas as moedas. Ir para o passo 2.

E.3 Exemplos ilustrativos

A título comparativo, iremos aplicar o algoritmo por nós sugerido usando as moedas que seriam usadas no algoritmo de Gargano e Vaccaro para a geração de uma distribuição de probabilidade uniforme usando duas moedas, uma honesta e outra com distribuição dada por

$$\left(2^{\lceil \log r(m) \rceil}/m, 1 - 2^{\lceil \log r(m) \rceil}/m\right), \tag{E.3}$$

onde $n = 2^t m$ e $r(m) = m - 2^{\lfloor \log m \rfloor}$. Observando que o valor de n usado em [13] refere-se ao produto de uma potência de 2 por um número ímpar m.

Chamamos atenção mais uma vez para o fato que o algoritmo aqui proposto funciona para qualquer escolha das moedas, enquanto o algoritmo proposto por Gargano e Vaccaro é específico para uma dada escolha de moedas.

Exemplo 41 *Consideremos $n = 6$, logo as moedas a serem usadas serão $m_1 = (1/2, 1/2)$ e $m_2 = (2/3, 1/3)$.*

Pelo primeiro passo do algoritmo, observamos que $1/2 > 1/6$ (Árvore A1, mostrada na Fig. E.1) e $2/3 > 1/6$ (Árvore A2 e Árvore A3 mostradas, respectivamente, nas Fig.E.2 e Fig.E.3), desta forma é necessária a expansão.

Feita a primeira expansão observa-se nas árvores A1 e A2 que as maiores probabilidades obtidas ainda são maiores que $1/6$, sendo assim necessária mais uma expansão desses elementos. Observa-se também que se expandido o nó da árvore A3 cuja probabilidade é 4/9,

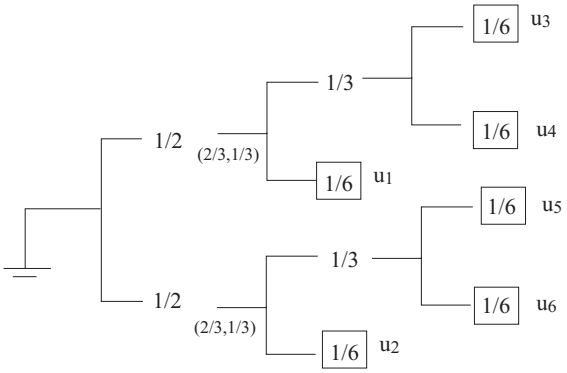


Figura E.1: Árvore A1 referente a n=*6.*

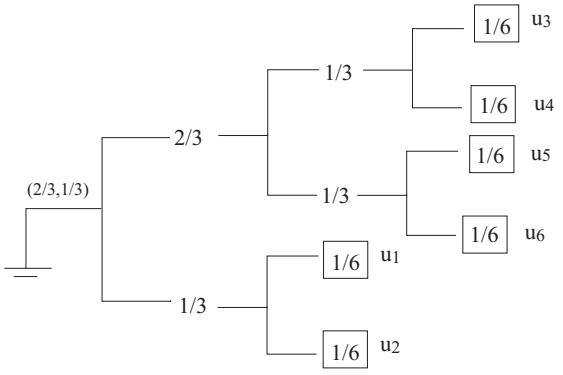


Figura E.2: Árvore A2 referente a n=*6.*

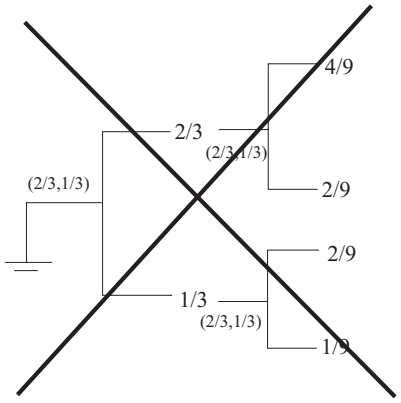


Figura E.3: Árvore A3 referente a n=*6, eliminada por não atender o critério de diferença mínima.*

seja usando a moeda honesta ou a desbalanceada, o resultado obtido ainda será maior que 1/6, diferentemente do que ocorrerá nas outras duas árvores. Desta forma, a árvore A3 é eliminada.

Segue-se com o algoritmo, resultando assim duas possíveis árvores, ambas com mesmo comprimento médio $E[T]$ *e comprimento máximo* L_{max}*, dados por:*

$$E[T] = \sum_x p(x) l_T(x), \tag{E.4}$$

$$L_{max} = \max_x l_T(x) \tag{E.5}$$

onde $p(x)$ é a probabilidade da seqüência de cara e coroa associada ao único caminho da fonte ao ramo x da árvore e $l_T(x)$, é o comprimento deste caminho.

Assim, temos como resultados para este exemplo:

$$E[T] = 2,67.$$

$$L_{max} = 3.$$

Pelo algoritmo sugerido por Gargano e Vaccaro (seção E.2, [13]) é obtida a mesma árvore ilustrada na Figura E.1, assim ambos os algoritmos apresentam mesmo comprimento médio e comprimento máximo.

Exemplo 42 *Consideremos $n = 7$. Neste caso o nosso algoritmo produz uma árvore de comprimento infinito, porém o valor $E[T]$ obedece a expressão (E.2).*

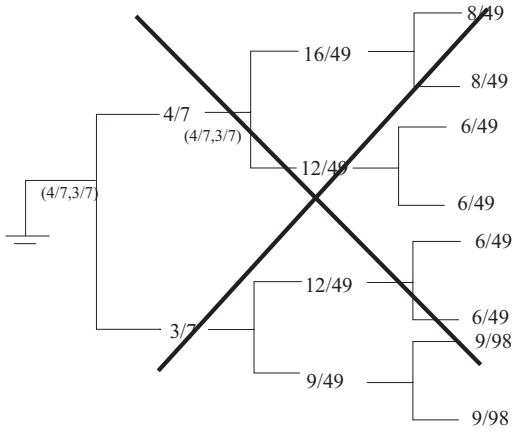


Figura E.4: Árvore A4 referente a n=*7, eliminada por não atender o critério de diferença mínima.*

Pelos mesmos motivos apontados no exemplo anterior escolhemos a árvore A5 (Fig. E.5) e eliminamos a árvore A4 (Fig. E.4).

Observa-se que o comprimento médio da árvore da Figura E.5 é dado por

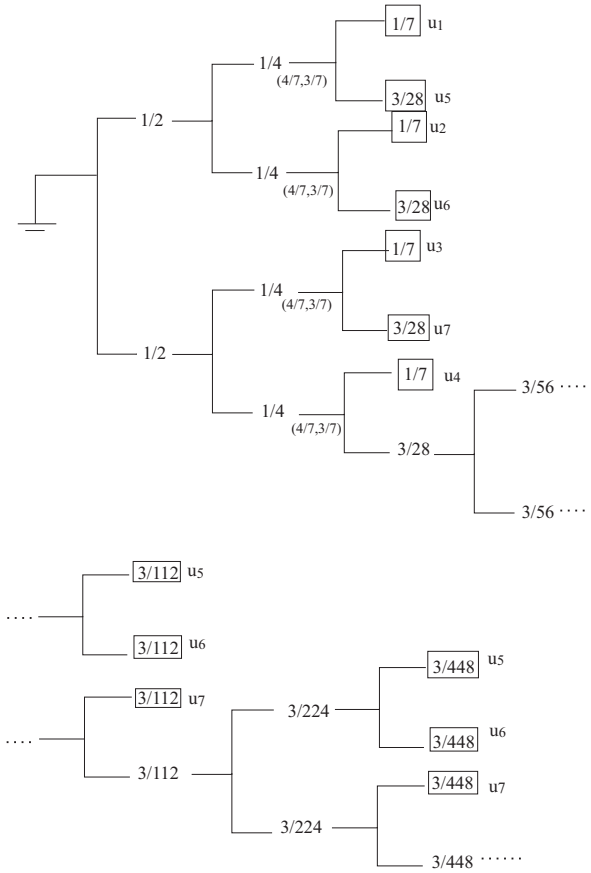


Figura E.5: Árvore A5 referente a n=7.

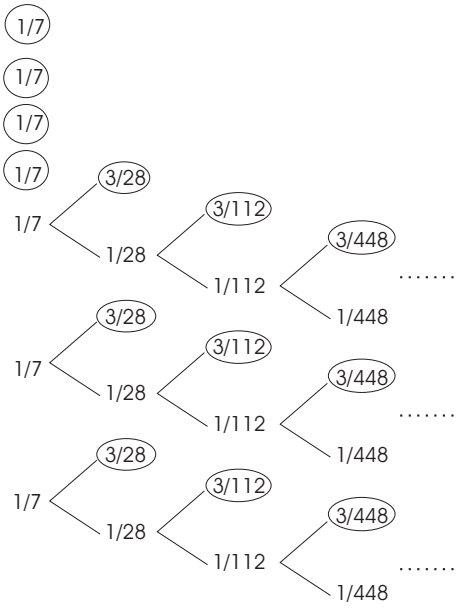


Figura E.6: Geração de fonte uniforme com $n = 7$ usando o algoritmo MIN-ENT por passo.

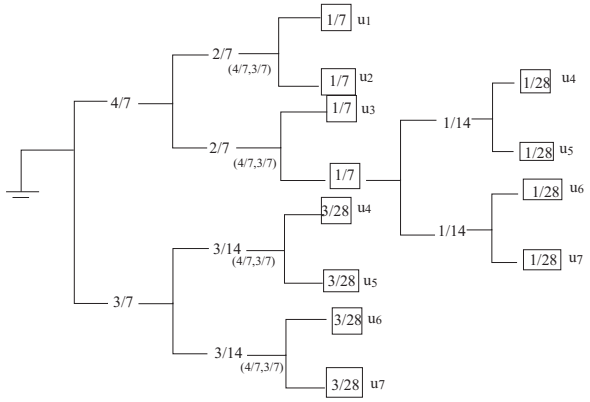


Figura E.7: Árvore referente ao n=*7 usando o algoritmo proposto por Gargano e Vaccaro.*

$$\begin{aligned} E[T] &= 1+\frac{4}{7}+\frac{3}{7}+\frac{2}{7}+\frac{2}{7}+\frac{3}{14}+\frac{3}{14}+\frac{3}{28}+\frac{3}{56} \\ &\quad +\frac{3}{56}+\frac{3}{112}+\frac{3}{224}+\frac{3}{224}+\frac{3}{448}+... \\ &= 3+\frac{6}{7}\sum_{i=1}^{\infty}(\frac{1}{4})^i \\ &= 3+0,29=3,29 \end{aligned}$$

o mesmo comprimento médio obtido pela árvore da Figura E.7, construída usando o algortimo de Gargano e Vaccaro.

E.4 Conclusões

Introduzimos neste trabalho um algoritmo para gerar uma distribuição discreta através do lançamento de duas ou mais moedas, sendo algumas delas desbalanceadas. Tal algoritmo mostrou ter resultados equivalentes aos obtidos em [13], para a geração de uma distribuição de probabilidade discreta uniforme usando duas moedas. Em contraposição ao algoritmo de Gargano e Vaccaro, nosso algoritmo tem a vantagem de poder operar com quaisquer que sejam as moedas disponíveis, independentes de n. Notou-se que o desempenho do algoritmo, medido em termos de tempo esperado curto, varia dependendo do grupo de moedas usadas. Esta observação sugere a exis-tência de um grupo de moedas desbalanceadas que otimize o mesmo. Um possível critério de escolha de moedas a fim de otimizar o algoritmo ainda encontra-se sob investigação. Sugerimos para trabalhos futuros, além da definição do grupo de moedas que otimiza o algoritmo, caso o mesmo exista, uma investigação da possibilidade do algoritmo MIN-ENT por passo ser implementado com árvores finitas quando n for primo, mesmo sabendo que $E[T]$ satisfaz a expressão (E.2).

E.4.1 Algoritmo MIN-ENT por passo

Seja $\Pi_D = \{\pi_0, \pi_1, \ldots, \pi_{D-1}\}$ a distribuição de probabilidade dos dígitos das palavras de homofonema. Para uma dada fonte o algoritmo MIN-ENT por passo simultaneamente encontra a decomposição da probabilidade de cada símbolo da fonte, como uma soma finita ou infinita de termos $\pi_0^{\lambda_0}\pi_1^{\lambda_1}\ldots\pi_{D-1}^{\lambda_{D-1}}$, e a correspondente palavra livre de prefixo, na qual o dígito $i,\ 0 \leq i \leq D-1$ ocorre λ_i vezes. Os homofonemas são selecionados como nós terminais na árvore D-ária enraízada T com probabilidades, de tal modo que de cada nó emanam D ramos com probabilidades $\pi_0, \pi_1, \ldots, \pi_{D-1}$, respectivamente. Denotemos por $v(i,j)$ o j-ésimo homofonema alocado ao símbolo da fonte u_i, $1 \leq i \leq K$, $j = 1, 2, \ldots$, e denotemos por $\alpha(i,j)$ a probabilidade de $v(i,j)$.

Definição 37 *Definimos a soma corrente de símbolo $\gamma_m(i)$ para $U = u_i$ na m-ésima iteração do algoritmo MIN-ENT como*

$$\gamma_m(i) = P_U(u_i) - \sum_{k=1}^{j-1} \alpha(i,k),$$

com $\gamma_m(i) = P_U(u_i)$ para $j = 0$, na qual j denota o número de homofonemas alocados a u_i até a m-ésima iteração.

Definição 38 *Definimos o conjunto de soma corrente Γ_m na m-ésima iteração do algoritmo MIN-ENT por passo como*

$$\Gamma_m = \{\gamma_m(i) | \gamma_m(i) > 0, 1 \leq i \leq K\},$$

com $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

Seja $\gamma_{\max} = \max\ \gamma_m(i) \in \Gamma_m,\ 1 \leq i \leq K$. Quando $m = 0$ no algoritmo MIN-ENT por passo nós construímos T a partir da raiz, começando com apenas D folhas. Daí então nós expandiremos cada nó terminal em T, cuja probabilidade exceda $\gamma_{\max}$, em um número mínimo de ramos suficiente para fazer com que as probabilidades dos nós terminais estendidos resultantes sejam iguais ou menores que $\gamma_{\max}$. Chamaremos a árvore resultante de *árvore D-ária enraízada e processada com probabilidades*, T_p. Na m-ésima iteração, $m \geq 1$, um homofonema é alocado a um nó terminal da correspondente T_p, de modo que o nó terminal não utilizado que possua a maior probabilidade, denotada por P_M, seja alocado como um homofonema para o símbolo u_r que apresente o mínimo valor não negativo para a diferença

entre sua soma corrente de símbolo $\gamma_m(r)$ e P_M, i.e., tal que $\min_i\{\gamma_m(i)-P_M|(\gamma_m(i)-P_M) \geq 0\} = \gamma_m(r) - P_M \geq 0,\ 1 \leq i \leq K$. O algoritmo consiste dos seguintes passos.

1. Faça $m = 0$. Faça $\gamma_0(i) = P_U(u_i),\ 1 \leq i \leq K$. Faça $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

2. Determine $\gamma_{\max}$ e construa a árvore T_p para a m-ésima iteração expandindo cada nó terminal não usado, na árvore construída para a $(m-1)$-ésima iteração, $m \geq 1$, cuja probabilidade exceda $\gamma_{\max}$, em um número mínimo de ramos suficiente para fazer a probabilidade dos nós terminais resultantes menores ou iguais a $\gamma_{\max}$.

3. Encontre em T_p, o caminho não usado E_l cuja probabilidade $P(E_l)$ seja a maior dentre as dos caminhos não usados, i.e., $P(E_l) = P_M$. Denotemos por l comprimento de E_l.

4. Se, para $1 \leq i \leq K$, $\min_i\{\gamma_m(i) - P_m|(\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0$, nós então associamos a u_r o homofonema (nó terminal) $v(r, j)$ e a palavra de homofonema D-ária de comprimento l, cujos símbolos constituem o rótulo de E_l em T_p. Isto implica $\alpha(r, j) = P_M$. Compute a soma corrente de símbolo $\gamma_m^{'}(r)$ após esta decomposição e faça $\Gamma_m^{'} = \Gamma_m - \{\gamma_m(r)\}$. Se $\gamma_m^{'}(r) = 0$ então faça $\Gamma_{m+1} = \Gamma_m^{'}$. A decomposição de $P_U(u_r)$ estará agora concluída e conterá j homofonemas, e se $\Gamma_{m+1} = \phi$ então FIM. Em caso contrário, i.e., se $\gamma_m^{'}(r) > 0$, então faça $\Gamma_{m+1} = \Gamma_m^{'} \cup \{\gamma_m^{'}(r)\}$.

5. Faça $m \leftarrow m + 1$.

6. Vá para o passo 2.

Referências

[1] J.von Neumann, "Various techniques used in connection with random digits", notes by G. E. Forsythe, *National Bureau of Standards, Applied Math Ser.*, vol. 12, pp. 36-38; reprinted in von Neumann's Collected Works., vol. 5. Oxford, U.K.: Pergamon, 1963, pp. 768-770.

[2] J. Abrahams, "Generation of discrete distributions from biased coins ", *IEEE Trans. on Inform. Theory*, vol. 42, pp. 1541-1546, 1996.

[3] M. Blum, "Independent unbiased coin flips from a correlated biased source-A finite state Markov chain", *Combinatorica*, vol. 6, no. 2, pp. 97-108, 1986.

[4] E. W. Dijkstra, "Making a fair roulette from a possibly biased coin", *Inform. Processing Lett.*, vol. 36, p. 193, 1990.

[5] P.Elias, “The efficient computation of an unbiased random sequence”, *Ann. Math. Statist.*, vol. 43, pp. 865-870, 1972.

[6] W. Hoeffding and G. Simons, “Unbiased coin tossing with a biased coin”, *Ann. Math. Statist.*, vol. 41, pp. 341-352, 1970.

[7] T. S. Han and M. Hoshi, “Interval algorithm for random number generation”, *IEEE Trans. on Inform. Theory*, vol. 43, pp. 599-611, March 1997.

[8] Y. Horibe, “Entropy and optimal random number transformation”, *IEEE Trans. on Inform. Theory*, vol. 27,pp.527-529, July 1981.

[9] D.E. Knuth and A. C. Yao, “The complexity of nonuniform random number generation", *in Algorithms and Complexity, New Directions and Results*, J. F. Traub, Ed. New York: Academic, 1976, pp.357-428.

[10] R. Motwani and P. Raghavan, *Randomized Algorithms. Cambridge*, U.K.: Cambridge Univ. Press, 1996.

[11] Q. F. Stout and B. Warren, “Tree algorithms for unbiased coin tossing with a biased coin”, *Ann. Probab.*, vol. 12, pp. 212-222, 1984.

[12] D. Feldman,R. Impagliazzo, M. Naor, N. Nisan, S. Rudich, and A. Shamir, “On dice and coins: Models of computation for random generation”, *Inform. Comput.*, vol. 104, pp. 159-174, 1993.

[13] L. Gargano and Ugo Vaccaro, “ Efficient generation of fair dice with few biased coins ”, *IEEE Trans. on Inform. Theory*, vol. 45, pp. 1600-1606, July 1999.

[14] V. C. da Rocha Jr., C. Pimentel e M. M. Vasconcelos, “Substituição homofônica ótima com restrição”, XX Simpósio Brasileiro de Telecomunicações, págs. 273 - 277, Rio de Janeiro, Brasil, 05-08 de outubro de 2003.

APÊNDICE F

ISIT'2006 - REDUNDANCY IN HOMOPHONIC CODING AND A NEW HOMOPHONIC CODING TECHNIQUE

Trabalho aceito e publicado nos anais do 2006 *IEEE International Symposium on Information Theory* ocorrido em The Westin Seattle - Seattle, Washington de 9 a 14 de julho de 2006.

V. C. da Rocha Jr., C. Pimentel and D. P. B. de A. Camara

Abstract - This paper has two purposes the first of which is to introduce a precise definition of redundancy in homophonic coding and the second is to introduce a perfect homophonic coding technique. The new homophonic coding technique generalizes often with advantage an earlier scheme due to Rocha and Massey.

F.1 Introduction

Homophonic coding is a technique whereby a multiplicity of "homophones" are probabilistically substituted for each plaintext letter [1], [2]. Each homophone is one-to-one mapped to a binary word so as to hide the redundancy of the resulting new "plaintext". In secret-key cryptographic systems the use of homophonic coding increases the unicity distance of the cipher [3], and hence makes it harder to break, at the cost of some plaintext expansion. In

traditional homophonic coding, each letter of the original message is replaced by a substitute or homophone in a larger alphabet to form the plaintext message that is then encrypted. The homophone is chosen uniformly at random from a set of substitutes reserved in the larger alphabet for that letter in the original alphabet, the size of these sets being (roughly) proportional to the relative frequencies of the letters in the original alphabet. Consequently, the overall probability distribution of homophones is a uniform distribution and all homophones have the same length. In 1988, Günther [1] made an important contribution to homophonic coding by introducing variable-length homophonic substitution, in which the homophones for a particular letter can have different lengths and different probabilities of selection. Günther showed that this technique could be used to hide in the homophonically coded sequence all the redundancy in the original plaintext and thus can be used to construct what Shannon calls a strongly ideal cipher [3] while also reducing plaintext expansion. In [2] Jendal, Kuhn and Massey presented an information-theoretic approach to homophonic coding. More recently other contributions to homophonic coding have appeared in the literature [4], [5]. A homophonic coding scheme is defined by a *homophonic channel* [2] and by the way such a homophonic channel is used.

Our purpose in this paper is twofold. First we present a precise definition of redundancy in homophonic coding and second we introduce a perfect homophonic coding technique called letter-by-letter (LBL) homophonic coding. The LBL technique always requires a bounded number of fair coin tosses to select a homophone. This condition, which is also satisfied by an earlier homophonic coding scheme due to Rocha and Massey (RM) [6], is an important practical aspect to be considered. Furthermore the LBL scheme generalizes often with advantage the RM scheme.

In *Section G.2* we introduce some basic terminology. In *Section F.3* we define redundancy in a homophonic coding scheme, in *Section F.4* we briefly review the RM scheme and in *Section F.5* we introduce the LBL scheme. In *Section G.5* we review the homophonic channel and introduce and discuss the noisy homophonic channel. Also in *Section G.5* we show an interesting analogy between the K-ary symmetric erasure channel and the RM scheme, and between a K-ary asymmetric erasure channel and the LBL scheme. Finally, in *Section H.4* we close this paper with conclusions.

F.2 Basic terminology

Let U denote a K-ary discrete memoryless source (DMS) with alphabet $\{u_1, u_2, \ldots, u_K\}$ and entropy $H(U)$. For simplicity, we consider in this paper only binary homophonic coding of the output sequence $U_1, U_2, U_3, \ldots$ and notice that homophones will also be referred to as binary words. The homophonic coding problem then reduces to that for a single K-ary random variable U, but the theory is easily modified to handle discrete sources with memory simply by replacing the probability distribution for U_i with the conditional probability distribution for U_i given the observed values of $U_1, U_2, \ldots, U_{i-1}$. Furthermore, we assume that U has a probability distribution with rational entries $P_U(u_i) = m_i/n_i,\ 1 \leq i \leq K$, where m_i and n_i are relatively prime positive integers.

The homophonic channel is a memoryless channel with input alphabet $\{u_1, u_2, \ldots, u_K\}$ coinciding with the set of possible values of U, and an output alphabet $V = \{v_1, v_2, \ldots\}$ which is either finite or countably infinite, and whose transition probabilities $P(V = v_j|U = u_i)$ have the property that for each j there is exactly one i such that $P(V = v_j|U = u_i) \neq 0$. In general, we shall consider those v_j for which $P(V = v_j|U = u_i) > 0$ to be the homophones for u_i, however we will show later that in some homophonic coding schemes some v_j's will represent a dummy symbol. Let $I(U;V)$ denote the mutual information [7,p.16] between U and V, i.e., let $I(U;V)$ denote the maximum number of bits per channel use produced by a given homophonic coding scheme applied to U.

By a binary prefix-free encoder we mean a device that assigns a binary sequence to each v_j under the constraint that this codeword is neither the same as another codeword nor forms the first part (or "prefix") of a longer codeword. This provision ensures that, when $X_1, X_2, \ldots$ is a sequence of codewords, the end of each codeword can be recognized without examining any following symbols in the sequence. It is well-known in information theory [7,p.49] that such coding is general in the sense that for any binary uniquely-decodable code there is a binary prefix-free code with exactly the same codeword lengths. Let $E(W)$ denote the expected value of the random variable W, where W denotes the length of a homophone.

Plaintext expansion was defined earlier [2] as the average homophone length less the source entropy, and it was implicitly assumed there that $H(U|V) = 0$. This definition of plaintext expansion is useful when comparing two homophonic coding systems which produce the same number of bits per symbol at the output of the homophonic channel. As we shall see, that is not always the case and then we propose to compare two distinct homophonic coding

systems in terms of a new definition of *redundancy* ρ, introduced in *Section F.3*. In general, redundancy as defined in *Section F.3* turns out to be the appropriate unit to compare different homophonic coding systems.

F.3 Redundancy in homophonic coding

In the context of source coding, for a given discrete memoryless source U and an associated uniquely decodable code, the coding efficiency η is defined [8,p.86] as the ratio between the source entropy $H(U)$ and the average codeword length $E(W)$, i.e., $\eta = H(U)/E(W)$. The redundancy ρ is defined as $\rho = 1 - \eta$, i.e. $\rho = [E(W) - H(U)]/E(W)$.

Let R denote the rate of information transmission in a given homophonic coding scheme, i.e., let R denote the number of bits per symbol produced by a given homophonic coding scheme at the output of the homophonic channel. As we shall see shortly, there are homophonic coding schemes, as for example the LBL homophonic coding scheme, for which $H(U|V) \neq 0$, and the earlier definition of cleartext expansion [2] is not adequate. For that reason we now define cleartext expansion as $E(W) - R$. We now generalize the earlier definition of redundancy restating it as follows.

Definição 39 *The redundancy ρ of a homophonic coding scheme is defined as the ratio between the cleartext expansion $E(W) - R$ and the average length of a homophone $E(W)$, i.e.,*

$$\rho = [E(W) - R]/E(W) = 1 - R/E(W). \tag{F.1}$$

In a manner analogous to that in source coding, we define the efficiency η of a homophonic coding scheme as follows.

Definição 40 *The efficiency η of a homophonic coding scheme is defined as*

$$\eta = 1 - \rho = R/E(W). \tag{F.2}$$

Jendal-Kuhn-Massey (JKM) [2] defined homophonic coding as *perfect* if the new plaintext sequence is irredundant and as optimum if it is both perfect and minimizes cleartext expansion. We remark that a smaller plaintext expansion does not necessarily implies a smaller redundancy. For example, a homophonic scheme with rate $R_1 = 8$ and $E(W_1) = 10$ has plaintext expansion $E(W_1) - R_1 = 2$ and redundancy $[E(W_1) - R_1]/E(W_1) = 0.2$, while a homophonic scheme with rate $R_2 = 3$ and $E(W_2) = 4$ has plaintext expansion $E(W_2) - R_2 = 1$

and redundancy $[E(W_2) - R_2]/E(W_2) = 0.25$. Lower redundancy means more entropy bits per homophone (binary homophonic code digit) while lower cleartext expansion by itself lacks an objective interpretation. This fact illustrates the relevance of our definition of redundancy (resp. plaintext expansion) for comparing distinct homophonic coding schemes. We therefore introduce the following definition of an *optimum* homophonic coding scheme.

Definição 41 *A homophonic coding scheme is defined to be optimum if it is both perfect and its redundancy is as small as possible.*

F.4 Rocha-Massey homophonic coding

In the Rocha-Massey (RM) homophonic coding scheme [6] a K-ary DMS U is assumed with a probability distribution having rational entries $P_U(u_i) = m_i/n,\ 1 \leq i \leq K$, where m_i and n are positive integers and n is as small as possible, i.e., $n_i = n, 1 \leq i \leq K$, in $P_U(u_i) = m_i/n_i$. The source U is augmented to become $\tilde{U}$ by adding to the original alphabet a "dummy" letter Δ with assigned probability $P_{\tilde{U}}(\Delta) = (2^N - n)/2^N$ where $N = \lceil \log_2 n \rceil$. This forces the choices $P_{\tilde{U}}(u_i) = (n/2^N)P_U(u_i) = m_i/2^N$ for $1 \leq i \leq K$. The letter probabilities for the augmented source are thus rational numbers with a common denominator of 2^N and hence at most N fair coin flips are required to choose a homophone if standard variable-length homophonic coding [2] is now applied.

Exemplo 43 *Consider the binary DMS with $P_U(u_1) = 1/3$ and $P_U(u_2) = 2/3$. For the RM scheme $N = \lceil \log_2 3 \rceil = 2$, we augment U with a dummy letter Δ for which $P_{\tilde{U}}(\Delta) = (4-3)/4 = 1/4$. Then $P_{\tilde{U}}(u_1) = (3/4)(1/3) = 1/4$ and $P_{\tilde{U}}(u_2) = (3/4)(2/3) = 1/2$ so at most two fair coin flips are needed to select a homophone. All letter probabilities for $\tilde{U}$ are negative integer powers of 2 and hence $E[\tilde{W}] = H(\tilde{U})$. The average number of letters from the original source U that are encoded with the encoding of one letter of $\tilde{U}$ is $p = 1 - P_{\tilde{U}}(\Delta) = n/2^N = 3/4$.*

The RM scheme can be implemented as follows. One first tests for the occurrence of an event of probability $p = 1 - P_{\tilde{U}}(\Delta) = n/2^N$, which requires at most N flips of a fair coin. If the event occurs, one calls on the source U to emit a letter that then becomes the output of $\tilde{U}$. Otherwise, the dummy letter Δ becomes the output of $\tilde{U}$. Decoding is very simple, it requires just deleting the dummy letters from the reconstructed output sequence of $\tilde{U}$ to obtain the output sequence of U.

F.5 Letter-by-letter homophonic coding

For a K-ary DMS U with letter probabilities $P_U(u_i) = m_i/n_i,\ 1 \leq i \leq K$, where m_i and n_i are relatively prime positive integers, i.e., such that the m_i/n_i are rational numbers, our new scheme is described as follows.

a) For each source letter $U = u_i,\ 1 \leq i \leq K$, with probability $P_U(u_i) = m_i/2^{s_i}$, i.e., for which $n_i = 2^{s_i}$, where s_i is a positive integer, we write m_i in base 2 and to each term in this base 2 decomposition we associate one homophone.

b) For each source letter $U = u_i,\ 1 \leq i \leq K$, with probability $P_U(u_i) = m_i/n_i$, for which n_i is not a power of 2, we associate two symbols called respectively a letter homophone and a dummy homophone. Given that U selects a letter u_i, an experiment is performed where a letter homophone is selected with probability $P_i/P_U(u_i)$, where P_i is the largest term in the base 2 representation of $P_U(u_i) = m_i/n_i$, and a dummy homophone Δ_i is selected with probability $P(\Delta_i) = 1 - P_i/P_U(u_i)$.

c) Let V denote the DMS having as letters the letter homophones from U and the dummy homophone Δ with probability $P(\Delta) = P_U(u_1)P(\Delta_1)+P_U(u_2)P(\Delta_2)+\ldots+P_U(u_K)P(\Delta_K)$. We notice that V imposes no information loss since to recover U we do not need to distinguish among the various dummy homophones.

d) Letter-by-letter binary coding of U is done as follows. We encode the letters of V one-to-one with the codewords of a binary uniquely decodable Huffman code with average codeword length $E(W)$. Whenever a dummy homophone Δ_i is produced in step b), the dummy letter Δ is produced by V and the selection experiment is repeated as many times as necessary until the corresponding letter homophone is selected. The source U is then called to select the next letter for encoding and so on.

e) Decoding is immediate, we just erase the received codewords representing the dummy homophone Δ and map the remaining codewords one-to-one to letters in U.

Exemplo 44 *Consider the $K = 3$ DMS U with $P_U(u_1) = 1/4, P_U(u_2) = 1/3$ and $P_U(u_3) = 5/12$. For the LBL scheme, since $P_U(u_1) = 1/4$, it follows that $P_1 = 1/4$ and that $P(\Delta_1) = 0$, i.e. we need no dummy homophone Δ_1. Since $P_U(u_2) = 1/3 = (1/4)\sum_{i=0}^{\infty}(1/4)^i$, it follows that $P_2 = 1/4$ and $P(\Delta_2) = 1 - P_2/P_U(u_2) = 1 - 3/4 = 1/4$. Since $P_U(u_3) = 5/12 =$*

$1/4+(1/8)\sum_{i=0}^{\infty}(1/4)^i$ *it follows that* $P_3 = 1/4$ *and* $P(\Delta_3) = 1-P_3/P_U(u_3) = 1-3/5 = 2/5$. *For this example* $P(\Delta) = P_U(u_1)P(\Delta_1) + P_U(u_2)P(\Delta_2) + P_U(u_3)P(\Delta_3) = 0 + 1/12 + 1/6 = 1/4, H(U) = 1.554$ *and* $E(W) = H(V) = 2$.

F.6 The homophonic channel

When the homophonic channel is a noiseless non-trivial channel [8,p.111] but the binary encoding is trivially prefix-free because all codewords have the same length m (i.e., the code is a "block code"), then we have conventional homophonic substitution. In the case where both the homophonic channel is noiseless and the binary encoding is non-trivially prefix-free, then we have variable-length homophonic substitution as introduced by Günther [1]. A third possibility in which $H(U|V) \neq 0$ is described next where the homophonic channel is represented by an erasure channel.

F.6.1 The K-ary erasure channel

The binary erasure channel (BEC) [7,p.92] is a discrete memoryless channel model with a binary input $U = \{u_1, u_2\}$ and a ternary output $V = \{v_1, v_2, v_3\}$, where $P_{V|U}(v_1|u_1) = P_{V|U}(v_2|u_2) = 1-\epsilon$ and $P_{V|U}(v_3|u_1) = P_{V|U}(v_3|u_2) = \epsilon$, and ϵ is the symbol erasure probability. The capacity C_{BEC} of the BEC is given by $C_{BEC} = 1-\epsilon$ [7,p.93].

An immediate generalization of the BEC is provided by the K-ary erasure channel (KEC), $K \geq 2$. The KEC is a discrete memoryless channel model with a K-ary input $U = \{u_1, u_2, \ldots, u_K\}$ and a $(K+1)$-ary output $V = \{v_1, v_2, v_3, \ldots, v_{K+1}\}$, where $P_{V|U}(v_i|u_i) = 1-\epsilon$ and $P_{V|U}(v_{K+1}|u_i) = \epsilon$, $1 \leq i \leq K$, where ϵ is the symbol erasure probability. It is an easy exercise to show that the capacity C_{KEC} of the KEC is given by

$$C_{KEC} = [1-\epsilon] \log K. \tag{F.3}$$

Gallager [7,p.506] gives a problem where a BEC is operated with noiseless feedback to tell the sender which symbol was received. Whenever one source symbol is transmitted, encoding consists of repeating that symbol as long as erasures are received through the feedback link. The moment the sender receives the correct symbol the source can then select the next symbol for transmission. Surprisingly, it turns out that this encoding strategy achieves capacity in the BEC, i.e., on average the source transmits $1-\epsilon$ bits per channel use, or 1 bit per $1/(1-\epsilon)$ channel uses on average. It is immediate to use a similar strategy in the KEC and to check

that operation at capacity is also achieved.

The reader may have noticed the analogy between this noiseless feedback strategy for the KEC and the behavior of the RM scheme. In order to make it clear we will describe an equivalent implementation of the RM scheme.

Alternative description of the Rocha-Massey scheme

Let the source select a symbol $U = u_i$ for transmission. We then perform a binary experiment which produces at the output of the expanded (by one dummy symbol) source $\tilde{U}$ a dummy symbol Δ with probability $P_{\tilde{U}}(\Delta)$ or a symbol $\tilde{u}_i$ with probability $1 - P_{\tilde{U}}(\Delta)$. Whenever a dummy symbol is produced the experiment is repeated as many times as necessary until a symbol $\tilde{u}_i$ is produced. The source can then select the next symbol for transmission. The source probability distribution however may not be a capacity achieving distribution and all we can say is that the rate R_{RM} of information transmission in the RM scheme is $H(U)$ bits per $1/[1 - P_{\tilde{U}}(\Delta)]$ "channel uses" on average, i.e.,

$$R_{RM} = [1 - P_{\tilde{U}}(\Delta)]H(U). \tag{F.4}$$

It follows for the RM homophonic channel that the mutual information $I(U;V)_{RM}$ is precisely $[1 - P_{\tilde{U}}(\Delta)]H(U)$. Therefore we conclude that the RM scheme produces information at the highest possible rate with zero-error and achieves capacity whenever $H(U) = \log K$ for a K-ary source.

Exemplo 45 *(Example 1 cont.) The plaintext expansion of the RM scheme is thus* $E[\tilde{W}] - pH(U) = H(\tilde{U}) - pH(U) = 3/2 - (3/4)h(1/3) = 0.811$*, where* $h(.)$ *denotes the binary entropy function.*

F.6.2 The K-ary asymmetric erasure channel

We consider now the K-ary asymmetric erasure channel (K-AEC), $K \geq 2$. The K-AEC is a discrete memoryless channel model with a K-ary input $U = \{u_1, u_2, \ldots, u_K\}$ and a $(K+1)$-ary output $V = \{v_1, v_2, v_3, \ldots, v_{K+1}\}$, where $P_{V|U}(v_i|u_i) = 1 - \epsilon_i, P_{V|U}(v_{K+1}|u_i) = \epsilon_i$, and $P_V(v_{K+1}) = P(\Delta) = \sum_{i=1}^{K} P_U(u_i)\epsilon_i,\ 1 \leq i \leq K$, where ϵ_i is the erasure probability for the i^{th} source symbol.

The analogy between the K-AEC and the LBL homophonic coding scheme is now clear. The mutual information $I(U;V)_{LBL}$ between the input U and the output V of the LBL

homophonic channel, i.e., the maximum rate of information generation in bits "per channel use" of the LBL scheme (for a given input probability distribution) is

$$\begin{aligned} I(U;V)_{LBL} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)(1-\epsilon_i)}\right] \\ &+ P(\Delta)\log\left[\frac{1}{P(\Delta)}\right] - \sum_{i=1}^{K} p_U(u_i)h(\epsilon_i). \end{aligned} \tag{F.5}$$

If we now consider the noiseless feedback scheme, described earlier for the "symmetric"K-ary erasure channel, the following rate R_{LBL} of information transmission is achieved.

$$\begin{aligned} R_{LBL} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right] \\ &= H(U) - \sum_{i=1}^{K}\epsilon_i p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right]. \end{aligned} \tag{F.6}$$

We notice that, unlike the case for the "symmetric"K-ary erasure channel where $R_{RM} = I(U;V)_{RM}$, for the K-ary asymmetric erasure channel it follows from (G.3) and (G.4) that

$$I(U;V)_{LBL} = R_{LBL} + \sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right]. \tag{F.7}$$

Lema 5

$$\sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] \geq 0. \tag{F.8}$$

Demonstração: We will prove this lemma by using the fundamental inequality of information theory, i.e., by applying the inequality $\ln(1/x) \geq 1 - x$ to the left hand side in (G.6). It the follows that

$$\begin{aligned} \sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] &\geq \frac{1}{\ln 2}\sum_{i=1}^{K} p_U(u_i)\epsilon_i\left[1-\frac{P(\Delta)}{\epsilon_i}\right] \\ &= \frac{1}{\ln 2}\left[P(\Delta) - P(\Delta)\right] = 0. \end{aligned}$$

■

From (G.5) and (G.6) it follows that $R_{LBL} \leq I(U;V)_{LBL}$. However, operation with zero-error is guaranteed in both RM and LBL schemes. We do not know the zero-error capacity for the K-ary asymmetric erasure channel and thus propose that R_{LBL} as given in (G.4) be considered as a lower bound on the zero-error capacity of this channel with noiseless feedback.

Exemplo 46 *(Example 2 cont.) For the LBL scheme the mutual information is calculated for the $K-AEC$ with $\epsilon_1 = 0,\ \epsilon_2 = 1/4,\ \epsilon_3 = 2/5$ and is given by*

$$\begin{aligned} I(U;V)_{LBL} &= H(V) - H(V|U) \\ &= 2 - (1/3)h(1/4) - (5/12)h(2/5) \\ &= 1.325 \end{aligned}$$

and the rate is

$$\begin{aligned} R_{LBL} &= (1/4)\log 4 + (3/4)[(1/3)\log 3] \\ &\quad +(3/5)[(5/12)\log(12/5)] \\ &= 1.211, \end{aligned}$$

i.e., $R_{LBL} = 0.91 I(U;V)_{LBL}$. The efficiency is $\eta_{LBL} = R_{LBL}/E(W) = 1.211/2 = 0.605$. The RM technique applied to U with $P_{\tilde{U}}(\Delta) = 1/4$ produces an average homophone length $E(W) = 2.375$, with efficiency $\eta_{RM} = [1 - P_{\tilde{U}}(\Delta)]H(U)/E(W) = (3/4)1.554/2.375 = 0.491$ giving thus a poorer performance.

F.7 Conclusion

The reason for the LBL scheme to perform usually better than the RM scheme should be clear by now, since the former employs various Δ_i conveniently selected while the latter employs a single Δ.

We remark that, in some cases, it is possible to improve the efficiency in the LBL scheme by expanding a given source letter probability using the first two largest terms in its binary representation instead of using only one term. Proceeding in this manner the value of $P(\Delta)$ will diminish, i.e., $p = 1 - P(\Delta)$ will increase. However $E(W)$ will also increase and η should be computed in order to decide whether this extra effort is worthwhile.

Finally, Sahai [9] states the following: "It can be shown that the Shannon classical capacity of the erasure channel is $1 - \epsilon$ bits per channel use regardless of whether the encoder has feedback. Furthermore, because a long string of erasures is always possible, the Shannon zero-error capacity of this channel is 0 as long as $\epsilon > 0$." This result is strictly true if block codes are employed. However if the restriction of using block codes is removed that result is no longer true. As we have mentioned earlier, Gallager [7] describes a feedback stratagem with a non-block code by which zero-error capacity of $1 - \epsilon$ bits per channel use is achieved

for the binary erasure channel, and we have extended that result for the K-ary symmetric erasure channel.

Acknowledgment

The authors acknowledge partial support from the Brazilian National Council for Scientific and Technological Development (CNPq) under Grants No. 305226/2003-7, 301253/2004-8 and 141215/2002-0, respectively.

References

[1] Ch. G. Günther, "A Universal Algorithm for Homophonic Coding", *Advances in Cryptology-Eurocrypt'88*, Lecture Notes in Computer Science, No.330. Heidelberg and New York: Springer, pp. 405-414, 1988.

[2] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An Information-Theoretic Approach to Homophonic Substitution", *Advances in Cryptology-Eurocrypt'89* (Eds. J.-J. Quisquater and J. Vandewalle), LNCS No. 434. Springer, pp. 382-394, 1990.

[3] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Tech. J.*, vol.28, pp. 656-715, Oct. 1949.

[4] B. Ryabko and A. Fionov, "Efficient Homophonic Coding", *IEEE Trans. on Info. Theory*, vol.45, no.6, pp.2083-2091, Sept. 1999.

[5] M. Hoshi and T.S. Han, "Interval Algorithm for Homophonic Coding", *IEEE Trans. on Info. Theory*, vol.47, no.3, pp.1021-1031, March 2001.

[6] V. C. da Rocha and J. L. Massey, "Better than "optimum" homophonic substitution", *Proc. IEEE International Symposium on Information Theory*, 25-30 June 2000, Sorrento, Italy, p. 241.

[7] R. G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, Inc., New York, 1968.

[8] N. Abramson, *Information Theory and Coding*, McGraw Hill, 1963.

[9] A. Sahai, "Evaluating channels for control: capacity reconsidered", *Proceedings of the American Control Conference*, Chicago, Illinois, USA, pp.2358-2362, June 2000.

APÊNDICE G

ITS'2006 - BINARY CONSTRAINED LETTER-BY-LETTER HOMOPHONIC CODING

Trabalho apresentado no VI International Telecommunications Symposium (ITS2006), September 3-6, 2006, Fortaleza-CE, Brazil.

V. C. da Rocha Jr., D. P. B. A. Camara and C. Pimentel

Abstract - In a perfect binary homophonic coding scheme the letters in each homophonic codeword are independent and identically distributed equally likely binary random variables. The main purpose of this paper is to introduce a new binary-constrained homophonic coding scheme coding, by which is meant that the letters in each homophonic codeword are independent and identically distributed but not equally likely binary random variables. Furthermore, this homophonic coding scheme requires a finite number of coin tosses to produce a homophone. This type of homophonic coding system may find application in situations where the cost of storing or transmitting 0's and 1's are distinct.

G.1 Introduction

Homophonic coding (substitution) is a well-known cryptographic technique for reducing the redundancy of a message to be enciphered at the cost of some plaintext expansion [1,2]. This technique consists of a replacement (one-to-many) of each letter of the original message by a substitute or *homophone*, in a larger alphabet, to form the plaintext message that is then encrypted. Each homophone is then associated with a codeword, usually in such a manner as to hide the redundancy of the resulting new "plaintext", i.e., to produce uniformly distributed and statistically independent code letters. In secret-key cryptographic systems the use of homophonic coding increases the unicity distance of the cipher [3], and hence makes it harder to break, at the cost of some plaintext expansion as described previously.

In classical homophonic coding the homophone is chosen uniformly at random from a set of substitutes reserved in the larger alphabet for that letter in the original alphabet, the size of these sets being (roughly) proportional to the relative frequencies of the letters in the original alphabet. Consequently, the overall probability distribution of homophones is a uniform distribution and all homophones have the same length. Although this procedure achieves the goal of homophonic coding that is to produce statistically independent homophonic codeword letters it is rather inefficient in terms of extra bits needed by each homophone on average. In 1988, Günther [1] made an important contribution to homophonic coding by introducing *variable-length homophonic coding* in which the homophones for a particular letter can have different lengths and different probabilities of being chosen. Günther showed that this technique could be used to hide in the homophonically coded sequence all the redundancy in the original plaintext and thus can be used to construct what Shannon calls a *strongly ideal cipher* [3] while also reducing plaintext expansion.

Binary-constrained homophonic coding is a binary homophonic coding scheme where the homophonic codeword letters obey an arbitrary probability distribution, i.e., not necessarily a uniform distribution. It constitutes a generalization of ordinary binary homophonic coding and finds application in cases where the cost of storing or transmitting 0's and 1's are distinct. In [4] and [5] the first and the third authors presented homophonic coding schemes in which the letters in each homophonic codeword are independent and identically distributed binary random variables obeying an arbitrary probability distribution $\Pi_2 = \{p, 1-p\}$, where $p \geq 1/2$. Each of these papers provided a distinct solution to the problem posed by Knuth and Yao [6,p.427] on the generation of probability distributions using a biased coin. Until then only

particular solutions to the Knuth and Yao problem had been proposed [7]. The algorithms proposed in [4] and [5] perform the expansion of a set of source letters into a set of homophones in steps. At each step one new homophone is produced in both cases. The expansion in [4] is performed in a manner that maximizes the entropy of the set of homophones at each step while the expansion in [5] is performed in a manner that minimizes the entropy of the set of homophones at each step. For obvious reason these homophonic coding schemes are called *maximum-entropy* per step and *minimum-entropy* per step, and for short we shall henceforth refer to them as MAX-ENT per step and MIN-ENT per step, respectively. When using either the MAX-ENT per step or the MIN-ENT per step schemes there are cases in which there is no bound for the number of biased coin tosses. The main purpose of this paper is to introduce a technique where we can perform constrained homophonic coding with a finite number of coin tosses.

In *Section G.2* we introduce some basic terminology relevant to homophonic coding, in *Section G.3* review the main ideas behind constrained homophonic coding, mentioning two previously introduced algorithms and presenting example. In *Section G.4* we introduce the binary constrained LBL scheme and in *Section G.5* we review the homophonic channel and discuss an interesting analogy between a K-ary asymmetric erasure channel and the binary constrained LBL scheme. Finally, in *Section H.4* we close this paper with some conclusions illustrated by data from the examples.

G.2 Basic terminology

For simplicity, we consider in the sequel only the homophonic binary coding of the output sequence $U_1, U_2, U_3, \ldots$ of a K-ary discrete memoryless source (DMS) and notice that homophones will also be referred to as binary words. The theory is easily modified to handle discrete sources with memory simply by replacing the probability distribution for U_i with the conditional probability distribution for U_i given the observed values of $U_1, U_2, U_3, \ldots, U_{i-1}$.

The homophonic channel is a memoryless channel with input alphabet $\{u_1, u_2, \ldots, u_K\}$ coinciding with the set of possible values of U, and an output alphabet $V = \{v_1, v_2, \ldots\}$ which is either finite or countably infinite, and whose transition probabilities $P(V = v_j|U = u_i)$ have the property that for each j there is exactly one i such that $P(V = v_j|U = u_i) \neq 0$. In general, we shall consider those v_j for which $P(V = v_j|U = u_i) > 0$ to be the homophones for u_i, however we will show later that in some homophonic coding schemes some v_j's will represent

a dummy symbol. Let $I(U;V)$ denote the mutual information [8,p.16] between U and V, i.e., let $I(U;V)$ denote the maximum number of bits per channel use produced by a given homophonic coding scheme applied to U.

For D- ary variable-length homophonic enconding $V = (X_1, X_2, \ldots, X_W)$ denotes a homophonic codeword, where each X_i, $1 \leq i \leq W$, is a D-ary random variable, taking value in the alphabet $\{0, 1, 2, \ldots, D-1\}$, and where the codeword length W is in general also a random variable. It is required that $X_1, X_2, \ldots, X_W$ be a prefix-free encoding of V, i.e., such that the specific codewords $x_1 x_2 \ldots x_W$ are all distinct and none forms the first part (or "prefix") of a longer codeword. This provision ensures that, when $X_1, X_2, \ldots$ is a sequence of codewords, the end of each codeword can be recognized without examining any following letters in the sequence. Let $E(W)$ denote the expected value of the random variable W, where W denotes the length of a homophone.

Plaintext expansion was defined earlier [2] as the average homophone length less the source entropy, and it was implicitly assumed there that $H(U|V) = 0$. This definition of plaintext expansion is useful when comparing two homophonic coding systems which produce the same number of bits per letter at the output of the homophonic channel. As we shall see shortly, there are homophonic coding schemes, as for example the homophonic coding scheme proposed in [9], for which $H(U|V) \neq 0$, and the earlier definition of cleartext expansion [2] is not adequate. Hereafter all entropies are assumed to be in bits and all logarithms are understood to be in base 2.

In the context of source coding, for a given discrete memoryless source U and an associated uniquely decodable code, the coding efficiency η [10,p.86] is defined as the ratio between the source entropy $H(U)$ and the average codeword length $E(W)$, i.e., $\eta = H(U)/E(W)$. The redundancy ρ is defined as $\rho = 1 - \eta$, i.e. $\rho = [E(W) - H(U)]/E(W)$. Let R denote the rate of information transmission in a given homophonic coding scheme, i.e., let R denote the number of bits per letter produced by a given homophonic coding scheme at the output of the homophonic channel. In [9] cleartext expansion was defined as $E(W) - R$, and the earlier definition of redundancy was restated as follows.

Definição 42 *The redundancy ρ of a homophonic coding scheme is defined as the ratio between the cleartext expansion $E(W) - R$ and the average length of a homophone $E(W)$, i.e.,*

$$\rho = [E(W) - R]/E(W) = 1 - R/E(W). \tag{G.1}$$

In a manner analogous to that in source coding, the efficiency η of a homophonic coding scheme was defined as follows.

Definição 43 *The efficiency η of a homophonic coding scheme is defined as*

$$\eta = 1 - \rho = R/E(W). \tag{G.2}$$

Jendal-Kuhn-Massey (JKM) [2] defined homophonic coding as *perfect* if the new plaintext sequence is irredundant and as *optimum* if it is both perfect and minimizes cleartext expansion. We remark that a smaller plaintext expansion does not necessarily implies a smaller redundancy. For example, a homophonic scheme with rate $R_1 = 8$ and $E(W_1) = 10$ has plaintext expansion $E(W_1) - R_1 = 2$ and redundancy $[E(W_1) - R_1]/E(W_1) = 0.2$, while a homophonic scheme with rate $R_2 = 3$ and $E(W_2) = 4$ has plaintext expansion $E(W_2) - R_2 = 1$ and redundancy $[E(W_2) - R_2]/E(W_2) = 0.25$. Lower redundancy means more entropy bits per homophone (binary homophonic code digit) while lower cleartext expansion by itself lacks an objective interpretation. This fact illustrates the relevance of the new definition of redundancy (resp. plaintext expansion) for comparing distinct homophonic coding schemes. This remark motivates us to introduce the following definition of an *optimum* constrained homophonic coding scheme.

Definição 44 *A constrained homophonic coding scheme is defined to be optimum if it is both perfect and its redundancy is as small as possible.*

G.3 Constrained coding

D-ary homophonic coding is characterized by the fact that it performs its tasks in two distinct steps [2]. In the first step each source probability is individually decomposed as a finite or infinite sum of negative powers of D, whose terms constitute the homophone probabilities. In the second step a prefix-free code is constructed for the decomposed source, employing the homophone probabilities to produce a uniquely decodable code.

In standard D-ary homophonic coding the designer benefits from the fact that a given letter probability $P_U(u_i),\ 0 < P_U(u_i) < 1$, has an essentially unique base D decomposition. This follows because $P_U(u_i)$ either has a unique decomposition as an infinite sum of negative powers of D, or it has both a decomposition as a finite sum of distinct negative powers of D and a decomposition as an infinite sum of distinct negative powers of D in which the smallest

term in the finite decomposition is expanded as an infinite sum of successive negative powers of D. For example, for $D = 3$, $P_U(u_i) = 4/9$ can be decomposed as either $P_U(u_i) = 1/3 + 1/9$ or as $P_U(u_i) = 1/3 + (1/27)\sum_{i=0}^{\infty}(2/3)^i$.

Constrained homophonic coding unfortunately does not inherit the essentially unique probability decomposition property just mentioned. This means that in order to split the source letters into homophones we need to work with the whole set of source letter probabilities, instead of working with only one letter probability at a time to perform the letter decomposition into homophones. This situation was handled with the MAX-ENT per step and the MIN-ENT per step homophonic coding algorithms, in [4] and [5], respectively. For the benefit of the reader we describe both the MAX-ENT per step and the MIN-ENT per step homophonic coding algorithms in the *Appendix*.

Exemplo 47 *Let U be the $K = 2$ DMS with $P_U(u_1) = 14/27$ and $P_U(u_2) = 13/27$. We consider the binary-constrained homophonic coding of U when $\Pi_2 = \{3/5, 2/5\}$ is the code alphabet probability distribution using the MAX-ENT per step.*

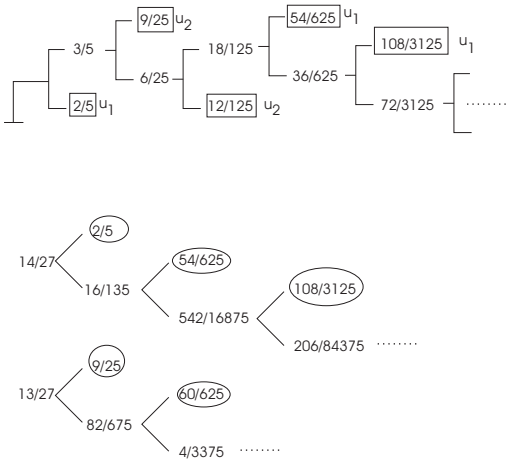


Figura G.1: The MAX-ENT per step algorithm applied to the binary DMS with letter probabilities $P_U(u_1) = 14/27$ and $P_U(u_2) = 13/27$ when $\Pi_2 = \{3/5, 2/5\}$ is the code alphabet probability distribution.

The entropy for this source is $H(U) = 0.999$. By the tree illustrated in Figure G.1 and using the path length lemma [11,p.29] we compute the average codeword length as $E(W) = 2.08$. It follows from (G.1) and (G.2) that the redundancy is $\rho = 0.5197$ and the efficiency is $\eta = 0.4803$, respectively. The homophones for u_1 are $1, 0100, 01010, \ldots$ and the homophones for u_2 are $00, 011, \ldots$.

Exemplo 48 *Let U be the $K = 2$ DMS with $P_U(u_1) = 14/27$ and $P_U(u_2) = 13/27$. We consider the binary-constrained homophonic coding of U when $\Pi_2 = \{3/5, 2/5\}$ is the code alphabet probability distribution using the MIN-ENT per step scheme.*

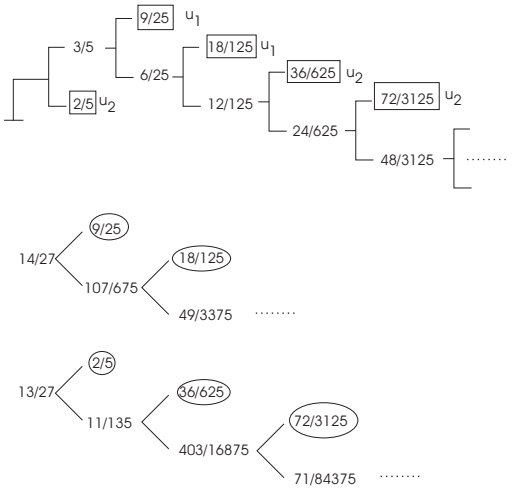


Figura G.2: The MIN-ENT per step algorithm applied to the binary DMS with letter probabilities $P_U(u_1) = 14/27$ and $P_U(u_2) = 13/27$ when $\Pi_2 = \{3/5, 2/5\}$ is the code alphabet probability distribution.

From the tree in Figure G.2 we compute the average codeword length as $E(W) = 2$. Using $E(W) = 2$ and the entropy $H(U) = 0.999$, the redundancy is computed as $\rho = 0.5005$ and the efficiency as $\eta = 0.4995$. The homophones for u_1 are $00, 010, \ldots$ and the homophones for u_2 are $1, 0110, 01110, \ldots$.

G.4 Constrained letter-by-letter homophonic coding

Let $l_T(x)$ denote the depth level of the leaf x in a tree T and let $L_{\max} = \max_x l_T(x)$. As we mentioned earlier, there will be cases where both the MAX-ENT per step and the MIN-ENT per step algorithms will produce unbounded trees, i.e., trees for which there is no finite maximal length $L_{\max}$. We shall now address the main goal of this paper which is to introduce a new binary constrained homophonic coding scheme where the maximal length of the tree is always a finite positive integer.

G.4.1 Algorithm description

As we explained earlier, in constrained homophonic coding we need to work with the whole set of source letter probabilities, instead of working with only one source letter probability

at a time, to perform a source letter decomposition into homophones. In the description that follows we shall assume that a homophone probability is selected using any constrained homophonic coding scheme, in particular, the MAX-ENT per step and the MIN-ENT per step algorithms can be used for this purpose. Furthermore, the number of homophones for a given source letter can be selected more or less arbitrarily, i.e., in general we can associate with a given source letter $1, 2, 3, \ldots, S$ homophones plus a dummy symbol denoted by Δ. In general, the larger the number of homophones associated with a source letter the lower the homophonic coding redundancy, however at the cost of an increase in complexity for implementation. We call this algorithm the constrained *letter-by-letter* (LBL) homophonic coding scheme.

Source letter decomposition algorithm

a) Apply a constrained homophonic coding (CHC) scheme to the given K-ary source, i.e., for each source letter $U = u_i,\ 1 \leq i \leq K$, with probability $P_U(u_i)$, apply a CHC algorithm generating a predefined number of homophones for each source letter. For each source letter that is not fully represented by the homophones obtained so far, the residual probability, that otherwise would be expanded, is kept to contribute to the dummy symbol probability.

b) The sum of all residual probabilities constitute the probability of the dummy symbol Δ.

Constrained LBL coding algorithm

1. Given that U selects a letter u_i, an experiment is performed where a letter homophone v_{ij} is selected with probability $P_{ij}/P_U(u_i)$, and a dummy homophone Δ_i is selected with probability $P(\Delta_i) = 1 - \sum_{i,j} P_{ij}/P_U(u_i)$.

2. Let V denote the DMS having as letters the letter homophones from U and the dummy homophone Δ with probability $P(\Delta) = P_U(u_1)P(\Delta_1)+P_U(u_2)P(\Delta_2)+\ldots+P_U(u_K)P(\Delta_K)$. We notice that V imposes no information loss since to recover U we do not need to distinguish among the various dummy homophones.

3. Constrained LBL binary coding of U is done as follows. The labelling of each homophone in V is done by the CHC algorithm using an associated tree [4], and the labelling of the dummy symbol is that of the unused leaf in this tree. Whenever a dummy homophone Δ_i is produced in step b), the dummy letter Δ is produced by V and the selection experiment is repeated as many times as necessary until the corresponding letter homophone is selected. The source U is then called to select the next letter for encoding and so on.

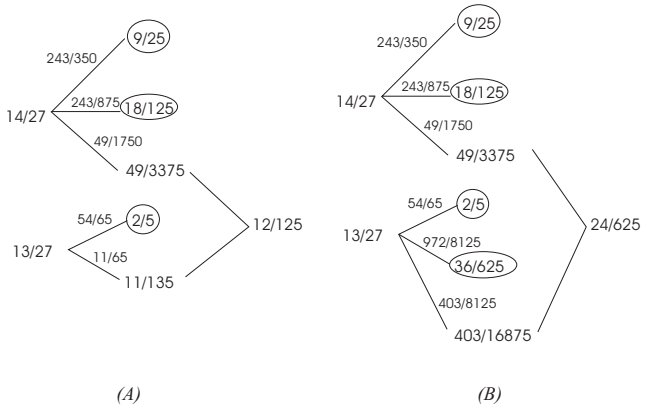


Figura G.3: Expansion of $14/27$ *and* $13/27$ *using the MIN-ENT per step algorithm with homophone letter probabilities* $2/5$ *and* $3/5$. (A) $P(\Delta) = 12/125$ *and* (B) $P(\Delta) = 24/625$.

4. Decoding is immediate, we just erase the received codewords representing the dummy homophone Δ and map the remaining codewords one-to-one to letters in U.

Exemplo 49 *Let* U *be the* $K = 2$ *DMS with* $P_U(u_1) = 14/27$ *and* $P_U(u_2) = 13/27$. *We consider the binary-constrained homophonic coding of* U *when* $\Pi_2 = \{3/5, 2/5\}$ *is the code alphabet probability distribution using the constrained LBL scheme.*

We consider again Figure G.2 for borrowing some of the results from Example 48. In Figure G.3 (A) *we used the MIN-ENT per step algorithm to expand* $14/27$ *into two homophones having probabilities* $9/25$ *and* $18/125$, *respectively, and leaving the probability* $49/3375$ *(to expanded further or) to be added to the dummy probability and finish the expansion of* $14/27$. *Similarly, we expand* $13/27$ *into one homophone having probability* $2/5$ *and leaving the probability* $1/135$ *(to be expanded further or) to be added to the dummy probability and finish the expansion of* $13/27$. *It follows that* $P(\Delta_1) = 49/3375$ *and* $P(\Delta_2) = 11/135$ *so* $P(\Delta) = P_U(u_1)P(\Delta_1) + P_U(u_2)P(\Delta_2) = (14/27)(49/1750) + (13/27)(11/65) = 12/125$. *In Figure G.3*(B) *we provide an alternative expansion for the same source probabilities, for which* $P(\Delta_1) = 49/3375$ *and* $P(\Delta_2) = 403/16875$ *so* $P(\Delta) = P_U(u_1)P(\Delta_1)+P_U(u_2)P(\Delta_2) = (14/27)(49/1750) + (13/27)(403/8125) = 24/625$.

G.5 The homophonic channel

The homophonic channel was formally treated in [2]. When the homophonic channel is a noiseless non-trivial channel [10,p.111] but the binary encoding is trivially prefix-free

because all codewords have the same length m (i.e., the code is a "block code"), then we have conventional homophonic substitution. In the case where both the homophonic channel is noiseless and the binary encoding is non-trivially prefix-free, then we have variable-length homophonic substitution as introduced by Günther [1]. A third possibility in which $H(U|V) \neq 0$ is described next where the homophonic channel is represented by an erasure channel. In [9] an analogy was presented between the Rocha-Massey (RM) scheme [12], which is a standard homophonic coding scheme, and the K-ary erasure channel. As a result it was concluded that the RM scheme produces information at the highest possible rate with zero-error and achieves the capacity of the K-ary erasure channel whenever $H(U) = \log K$ for a K-ary source. In [9] the analogy was considered between the K-ary asymmetric erasure channel a standard LBL homophonic coding technique, i.e., the case where the homophone letter probabilities are uniformly distributed. We will now extend that analogy by considering the K-ary asymmetric erasure channel and the constrained LBL homophonic coding technique. In order to make the analysis simpler we will consider that only one letter homophone and a "dummy" homophone are associated to each source letter.

In general, as we have seen earlier, we can have more than one letter homophone per source letter. By associating more letter homophone to each source letter a smaller value for $P(\Delta)$ will result. Consequently η will become closer to the value that is reached when an algorithm is used for which there is no bound for the number of biased coin tosses.

G.5.1 The K-ary asymmetric erasure channel

We now consider the K-ary asymmetric erasure channel (K-AEC), $K \geq 2$. The K-AEC is a discrete memoryless channel model with a K-ary input $U = \{u_1, u_2, \ldots, u_K\}$ and a $(K+1)$-ary output $V = \{v_1, v_2, v_3, \ldots, v_{K+1}\}$, where $P_{V|U}(v_i|u_i) = 1 - \epsilon_i, P_{V|U}(v_{K+1}|u_i) = \epsilon_i$, and $P_V(v_{K+1}) = P(\Delta) = \sum_{i=1}^{K} P_U(u_i)\epsilon_i,\ 1 \leq i \leq K$, where ϵ_i is the erasure probability for the i^{th} source symbol.

The analogy between the K-AEC and the constrained LBL homophonic coding scheme should be clear by now. The mutual information $I(U;V)_{LBL}$ between the input U and the output V of the constrained LBL homophonic channel, i.e., the maximum rate of information generation in bits "per channel use" of the constrained LBL scheme (for a given input

probability distribution) is as follows.

$$\begin{aligned} I(U;V)_{LBL} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)(1-\epsilon_i)}\right] \\ &+ P(\Delta)\log\left[\frac{1}{P(\Delta)}\right] - \sum_{i=1}^{K} p_U(u_i)h(\epsilon_i). \end{aligned} \tag{G.3}$$

In [8,p.506] a binary erasure channel (BEC) is described operating with noiseless feedback to tell the sender which letter was received. Whenever one source letter is transmitted, encoding consists of repeating that letter as long as erasures are received through the feedback link. The moment the sender receives the correct letter the source can then select the next letter for transmission. This rather simple encoding strategy achieves capacity in the BEC, i.e., on average the source transmits $1-\epsilon$ bits per channel use, or 1 bit per $1/(1-\epsilon)$ channel uses on average. It is immediate to use a similar strategy in the K-AEC and to check that operation at capacity is also achieved. In the case of constrained LBL, the analogy with the K-AEC leads to the following rate R_{LBL} of information transmission.

$$\begin{aligned} R_{LBL} &= \sum_{i=1}^{K}[1-\epsilon_i]p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right] \\ &= H(U) - \sum_{i=1}^{K}\epsilon_i p_U(u_i)\log\left[\frac{1}{p_U(u_i)}\right]. \end{aligned} \tag{G.4}$$

It follows from (G.3) and (G.4) that

$$I(U;V)_{LBL} = R_{LBL} + \sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right]. \tag{G.5}$$

Lema 6

$$\sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] \geq 0. \tag{G.6}$$

Demonstração: We prove this lemma by using the fundamental inequality of information theory, i.e., by applying the inequality $\ln(1/x) \geq 1-x$ to the left hand side in (G.6). It the follows that

$$\begin{aligned} \sum_{i=1}^{K} p_U(u_i)\epsilon_i \log\left[\frac{\epsilon_i}{P(\Delta)}\right] &\geq \frac{1}{\ln 2}\sum_{i=1}^{K} p_U(u_i)\epsilon_i\left[1-\frac{P(\Delta)}{\epsilon_i}\right] \\ &= \frac{1}{\ln 2}\left[P(\Delta)-P(\Delta)\right] = 0. \end{aligned}$$

■

From (G.5) and (G.6) it follows that $R_{LBL} \leq I(U;V)_{LBL}$. However, operation with zero-error is guaranteed in the constrained and LBL scheme.

Tabela G.1: Values of rate (R, R_{LBL}), η and ρ for the MIN-ENT per step and MIN-ENT per step based constrained LBL schemes.

	MIN-ENT	LBL 1 $P(\Delta) = 12/125$	LBL 2 $P(\Delta) = 24/625$
RATE	$H(U) = 0.999$	$R_{LBL} = 0.899$	$R_{LBL} = 0.984$
$L_{\max}$	unbounded	3	4
$E(W)$	2	1.84	1.936
η	0.499	0.489	0.496
ρ	0.500	0.511	0.504

G.6 Conclusions

Table G.1 shows values of rate, η, ρ, $L_{\max}$ and $E(W)$, obtained in the examples, for the MIN-ENT per step and the MIN-ENT per step based constrained LBL schemes (for two values of $P(\Delta)$). We observe that smaller values for $P(\Delta)$ make the value of η for the constrained LBL scheme closer and closer to the value reached by the MIN-ENT per step scheme, with the advantage of having a bounded $L_{\max}$ in the cases where the MIN-ENT per step has no bound for the number of biased coin tosses.

Appendix

In this appendix we describe the MAX-ENT per step algorithm [4] and the MIN-ENT per step algorithm [5]. For a given DMS source, both homophonic coding algorithms find the decomposition of each source letter probability as a sum (finite or infinite) of negative powers of D and the corresponding source code as described next.

G.6.1 MAX-ENT per step algorithm

Let $\Pi_2 = \{p, 1-p\},\ p \geq 1/2$, be the probability distribution for the homophonic codeword symbols. For a given source, this binary-constrained homophonic coding algorithm simultaneously finds the decomposition of each source symbol probability as a sum (finite or infinite) of terms $p^{\lambda}(1-p)^{l-\lambda}$, and the corresponding prefix-free homophonic code, where λ is the number of 1's and $l-\lambda$ is the number of zeroes of a homophonic codeword of length l. The algorithm consists of the following steps.

1. Order the source probabilities $P_U(u_1), P_U(u_2), \ldots, P_U(u_K)$, in a list in decreasing order.

2. Without loss of essential generality, assume that $P_U(u_i) = P(i,1)$ is the largest probability in the list. If there are two or more probabilities with the same highest value, just pick any one of them at random to start.

3. Let $j = 1$.

4. Find the least positive number $l_{i,j}$ such that the node probability $P_n(l_{i,j})$, at depth $l_{i,j}$, satisfies one of the following two relations

$$P_n(l_{i,j}) > P(i,j) \geq pP_n(l_{i,j}) \tag{G.7}$$

$$pP_n(l_{i,j}) > P(i,j) \geq (1-p)P_n(l_{i,j}). \tag{G.8}$$

   Associate to u_i the homophone $v_{i,j}$ and the binary homophonic codeword corresponding to the labeling of an unused path of length $l_{i,j}$ in the binary tree with probabilities, starting at the root node and ending at a leaf $v_{i,j}$. Let $P(i,j+1) = P(i,j) - pP_n(l_{i,j})$ if (G.7) is true, or let $P(i,j+1) = P(i,j) - (1-p)P_n(l_{i,j})$,if (G.8) is true. If $P(i,j+1) = 0$ then the decomposition of $P_U(u_i)$ is now complete and contains j homophones.

5. Remove $P(i,j)$ from the list. Add the entry $P(i,j+1)$ to the list if $P(i,j+1) > 0$. If the list is empty then END, otherwise reorder it in decreasing order.

6. Let $P(i',j')$ be the largest probability in the list. Let $i \leftarrow i'$ and let $j \leftarrow j'$.

7. Go to step 4.

G.6.2 MIN-ENT per step algorithm

Let $\Pi_2 = \{p, 1-p\},\ p \geq 1/2$, be the probability distribution for the homophonic codeword symbols. For a given source, the MIN-ENT per step algorithm simultaneously finds the decomposition of each source symbol probability as a sum (finite or infinite) of terms $p^{\lambda}(1-p)^{l-\lambda}$, and the corresponding prefix-free homophonic code, where λ is the number of 1's and $l-\lambda$ is the number of zeroes of a homophonic codeword of length l. The homophones are selected as terminal nodes in the binary rooted tree with probabilities, T. From any non-terminal node in this tree two branches emanate with probabilities p and $1-p = \overline{p}$, respectively. The label of a path in T is represented by the sequence of zeroes and ones associated with the branches constituting the path. The probability of a path of length l in T, containing λ 1's and $l-\lambda$ zeroes, is $p^{\lambda}(1-p)^{l-\lambda}$. In particular, for computing the probability of a terminal node we consider the path extending from the root node to that terminal node.

Let $v(i,j)$ denote the j^{th} homophone assigned to the source symbol u_i, $1 \leq i \leq K$, $j = 1, 2, \ldots$. Let $\alpha(i,j)$ denote the probability of $v(i,j)$.

Definição 45 *We define the symbol running sum $\gamma_m(i)$, associated with the symbol u_i, $1 \leq i \leq K$, at the m^{th} iteration of the MIN-ENT per step algorithm as*

$$\gamma_m(i) = P_U(u_i) - \sum_{k=1}^{j} \alpha(i,k),$$

with $\gamma_m(i) = P_U(u_i)$ for $j = 0$, where j denotes the number of homophones allocated to u_i up to the m^{th} iteration.

Definição 46 *We define the running sum set Γ_m at the m^{th} iteration of the algorithm as*

$$\Gamma_m = \{\gamma_m(i) | \gamma_m(i) > 0, 1 \leq i \leq K\},$$

with $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

Let $\gamma_{\max} = \max\, \gamma_m(i) \in \Gamma_m,\ 1 \leq i \leq K$. At $m = 0$ we grow T from the root, starting with only two leaves. We will expand each terminal node in T, whose probability exceeds $\gamma_{\max}$, by the least number of branches sufficient to make the resulting extended terminal node probability less than or equal to $\gamma_{\max}$. We call the resulting tree the *processed binary rooted tree with probabilities*, T_p. At the m^{th} iteration, $m \geq 1$, a homophone is assigned to a terminal node of the corresponding T_p, in a manner that the unused terminal node with largest probability P_m is assigned as a homophone to the symbol u_r with minimum nonnegative value for the difference between its homophone running sum $\gamma_m(r)$ and P_m, i.e., such that $\min_i\{\gamma_m(i) - P_m | (\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0,\ 1 \leq i \leq K$. The algorithm consists of the following steps.

1. Let $m = 0$. Let $\gamma_0(i) = P_U(u_i),\ 1 \leq i \leq K$. Let $\Gamma_0 = \{P_U(u_1),\ P_U(u_2), \ldots, P_U(u_K)\}$.

2. Determine $\gamma_{\max}$ and produce the tree T_p for the m^{th} iteration by expanding each terminal node in the tree from the $(m-1)^{th}$ iteration, $m \geq 1$, whose probability exceeds $\gamma_{\max}$, by the least number of branches sufficient to make the resulting extended terminal node probability less than or equal to $\gamma_{\max}$.

3. Find the unused path E_l of length l in T_p whose probability is largest among unused paths, and denote this largest probability by P_m.

4. If, for $1 \leq i \leq K$, $\min_i\{\gamma_m(i) - P_m | (\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0$, then we associate to u_r the homophone (terminal node) $v(r, j)$ and the binary homophonic codeword of length l, whose digits constitute the labelling of E_l in T_p. This implies $\alpha(r, j) = P_m$. Compute the symbol running sum $\gamma_m^{'}(r)$ after this decomposition and let $\Gamma_m^{'} = \Gamma_m - \{\gamma_m(r)\}$. If $\gamma_m^{'}(r) = 0$ then let $\Gamma_{m+1} = \Gamma_m^{'}$. The decomposition of $P_U(u_r)$ is now complete and contains j homophones, and if $\Gamma_{m+1} = \phi$ then END. Otherwise, i.e., if $\gamma_m^{'}(r) > 0$, then let $\Gamma_{m+1} = \Gamma_m^{'} \cup \{\gamma_m^{'}(r)\}$.

5. Let $m \leftarrow m + 1$.

6. Go to step 2.

Acknowledgments

The authors acknowledge partial support from the Brazilian National Council for Scientific and Technological Development (CNPq) under Grants No. 305226/2003-7, 141215/2002-0 and 301253/2004-8, respectively.

References

[1] Ch. G. Günther,"A universal algorithm for homophonic coding", pp. 405-414 in *Advances in Cryptology - Eurocrypt ´88*, Lecture Notes in Computer Science. No. 330. Heidelberg and New York: Springer 1988.

[2] H. N. Jendal, Y. J. B Kuhn and J. L. Massey, "An information-theoretic approach to homophonic substitution", pp. 382-394 in *Advances in Cryptology - Eurocrypt ´89* (Eds. J.-J. Quisquater and J. Vandewalle). Lecture Notes in Computer Science No. 434. Heidelberg and New York: Springer 1990.

[3] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Tech. J.*, vol.28, pp. 656-715, Oct. 1949.

[4] V. C. da Rocha and C. Pimentel, "Binary-constrained homophonic coding", *VI International Symposium on Communication Theory and Applications*, Ambleside, England,pp. 263-268, 15 - 20 July 2001.

[5] V. C. da Rocha Jr. and C. Pimentel, "Optimum binary-constrained homophonic coding", *VII International Symposium on Communication Theory and Applications*, Ambleside,

England,pp. 64-69, 13 - 18 July 2003.

[6] D.W. Knuth and A.C. Yao, "The complexity of random number generation", In J.F. Traub, editor,*Algorithms and Complexity: Recent Results and New Directions. Proceedings of the Symposium on New Directions and Recent Results in Algorithms and Complexity, Carnegie Mellon University, 1976.* Academic Press, New York, 1976.

[7] Julia Abrahams, "Generation of Discrete Distributions form Biased Coins", *IEEE Trans. Inform. Theory*, vol. IT-42, pp.1541-1546, September 1996.

[8] R. G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, Inc., New York, 1968.

[9] V. C. da Rocha Jr., C. Pimentel and D. P. B. A. Camara, "Redundancy in homophonic coding and a new homophonic coding technique", submited to *IEEE Int. Symp. on Information Theory, ISIT2006.*

[10] N. Abramson, *Information Theory and Coding.* MacGraw-Hill, 1963.

[11] J. L. Massey, "Applied Digital Information Theory I", *Class notes at the ETH Zurich*, http://www.isi.ee.ethz.ch/education/public/pdfs/aditI.pdf, 1980-1998.

[12] V. C. da Rocha and J. L. Massey, "Better than "optimum" homophonic substitution", *Proc. IEEE International Symposium on Information Theory*, 25-30 June 2000, Sorrento, Italy, p. 241.

APÊNDICE H

ISITA'2006 - GENERATION OF A DISCRETE DISTRIBUTION USING BIASED COINS

Trabalho aceito e publicado nos anais *ISITA 2006 - The 2006 International Symposium on Information Theory and its Applications* ocorrido em COEX, Seul, Korea, de 29 de outubro a 01 de novembro de 2006.

Danielle P. B. de A. CAMARA, Valdemar C. da ROCHA Jr. and Cecilio PIMENTEL

Abstract - The efficient generation of a discrete probability distribution is of current interest in areas like cryptography and random number generation. This paper presents an algorithm for generating a discrete distribution using two or more coins, being one of them unbiased. In particular, this approach contributes an alternative solution to the classical problem of generating a discrete uniform probability distribution using two or more distinct coins.

H.1 Introduction

The generation of a discrete probability distribution using flips of an biased coin is considered one of the oldest and of great importance problem in the areas of cryptography and random number generation which are used to perform tests and simulation of communication systems as well as many other computational applications. It is about forty years since von

Neumann [1] introduced a simple algorithm to generate a string of bits statistically independent and equally likely from flips of a coin with unknown bias. Since his work [1] several researchers have considered and studied the generation of uniform random variables under a variety of different assumptions [2]-[13]. Basically, the study of the generation of uniform random variables considers two approaches: *short bounded time* and *short expected time*, where the latter is the more traditional approach. The algorithm proposed in this paper considers the *short expected time* approach.

Feldman et al.[12] proved in their work, among several results, that the outcomes of a n-sided fair die, that is, the outcome of a random variable which takes n equiprobable values, can be simulated in bounded time by using flips of just one type of coin of appropriate rational bias if and only if n is a power of 2 ([12], theorem 2), and that a general n-sided fair die can always be simulated by using two coins of the appropriate bias and at most $\lceil 2 \log n \rceil + 1$ coin flips, where $\lceil x \rceil$ denotes the smallest integer number greater or equal to x. One of the results obtained by Gargano and Vaccaro [13] was the improvement of this bound.

In [13] several algorithmic questions were considered, related to the classical problem of simulating the outcomes of a uniform random variable by using a limited number of biased coins, and an algorithm was given to generate an n-sided fair die using only a fair coin and a biased coin. The biased coin has probability distribution for heads and tails given by

$$\left(2^{\lceil \log r(m) \rceil}/m, 1 - 2^{\lceil \log r(m) \rceil}/m\right), \tag{H.1}$$

where m is the largest odd factor of n and $r(m) = m - 2^{\lfloor \log m \rfloor}$. In the worst case

$$1 + \lfloor \log n \rfloor + \lceil \log(n - 2^{\lfloor \log n \rfloor}) \rceil + pw(n) \tag{H.2}$$

coin flips are required, where $pw(n) = \max\{i : 2^i \text{ divides } n\}$, and in average

$$\begin{aligned} 1 + \lfloor \log n \rfloor + (2^{pw(n)}/n)(\lceil \log r(n) \rceil 2^{\lceil \log r(n) \rceil} \\ - r(n)(\lfloor \log r(n) \rfloor - pw(n))), \end{aligned} \tag{H.3}$$

coin flips are required.

In Section H.2 we introduce a new algorithm for the generation of a discrete probability distribution using the flips of two or more coins, some of them biased. It is important to emphasize that the algorithm proposed by Gargano and Vaccaro is specific for a given choice of coins. In Section H.3 the application of this algorithm will be illustrated through some examples, in which a uniform probability distribution is generated using two coins, one fair

coin and a biased coin. Summing up, in Section H.4 we present some conclusions about this work as well as some suggestions for future research.

H.2 A new algorithm

The algorithm introduced in [14] deals with a scheme of homophonic substitution in which every binary word representing a homophone has as symbols random variables which are independent and identically distributed, obeying an arbitrary probability distribution. In other words, it deals with the generation of a discrete probability distribution using flips of one biased coin. In this section we present a generalization of the minimum entropy (MIN-ENT) per step algorithm introduced in [14], in the sense that a discrete probability distribution is generated using two or more biased coins, obtaining results similar to Gargano and Vaccaro´s [13] with the distinction that not necessarily the heads and tails distribution is dependent on n as in the algorithm suggested in [13].

We introduce next some notation that will be used in the sequel. A tree T is used to indicate the choice of coins by the algorithm to produce the desired distribution, and a labelled leaf in T is associated one-to-one with one of the outcomes. Given a tree T and a leaf x of T, let $l_T(x)$ denote the depth level of x in T, that is, the length of the path from the root of T to the leaf x, and let $p(x)$ denote the probability of a leaf x being reached. We denote the longest path in T as $L_{\max} = \max_x l_T(x)$ and the average length of the tree as $E[T] = \sum_x p(x) l_T(x)$.

For all trees in this paper we assume that from each node emanates two branches. Each node is labelled with a coin distribution. If a node has no indication we assume the coin used is an unbiased coin, if there is some indication of the kind $(p, 1-p)$ this means a biased coin is used with probability of a head equal to p and probability of a tail equal to $1-p$. Each branch is labelled with a probability.

In our proposed algorithm there are cases where the maximal length $L_{\max}$ is not bounded, but even in these cases shorter values for $E[T]$ result as compared to those in [13]. Our proposal is basically a generalization to more than one biased coin of the algorithm introduced in [14], obtaining equivalent and in some cases even better results than those in [13].

H.2.1 Description of the algorithm

The algorithm proposed here follows essentially the same steps of the one introduced in [14] with the important difference that instead of using only one coin it uses two or more coins. At each step we select which one of the coins must be chosen to be flipped, considering the minimization of the entropy in that step. For the benefit of the reader we describe the MIN-ENT per step algorithm in the Appendix.

Let $m_1 = \{p_1, 1-p_1\}$, $m_2 = \{p_2, 1-p_2\}$, ..., $m_r = \{p_r, 1-p_r\}$ be the probabilities distributions of the coins and $P_U = \{P_U(u_1), \ldots, P_U(u_K)\}$ the probability distribution to be generated.

1. Flip one of each coins and associate to each one tree.
2. To each one of the trees check whether the largest leaf probability is less than or equal to the largest value of $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

   (P.S.: After the first iteration Γ_0 is replaced by Γ, substituting Γ_0, as described in the Appendix)

   (a) If some of this (these) tree(s) obey this condition keep it (them) and eliminate the other(s). Go on with the algorithm by applying the MIN-ENT algorithm (see the Appendix) to the surviving trees.

   (b) Other case, go to step 3.
3. Make the expansion of each tree, considering all the coins. Go to step 2.

H.3 Examples

In order to compare our results with those in [13] we will apply the proposed algorithm using the same coins as indicated in Gargano and Vaccaro´s algorithm [13] to the generation of a uniform probability distribution using two coins, one fair and the other with distribution given by (H.1). We emphasize that the biased coins employed in our proposed algorithm are arbitrary, i.e., they do not depend on n as is the case with those in the algorithm in [13].

Exemplo 50 *Consider generating the probability distribution of the faces of a fair die , i.e.,* $n = 6$*, using the coins* $m_1 = (1/2, 1/2)$ *e* $m_2 = (2/3, 1/3)$*. The same tree is obtained (Figure*

H.1) for both the algorithm in [13] and our proposed algorithm. We compute for this tree the values $E[T] = 2.67$ *and* $L_{\max} = 3$.

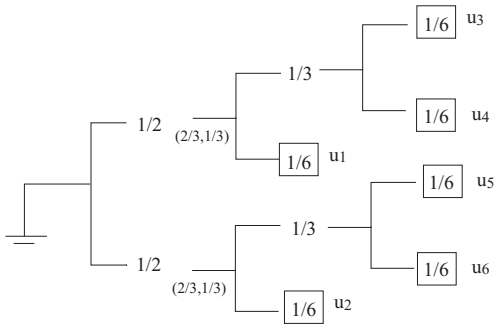


Figura H.1: Tree obtained for $n = 6$ *for both the algorithm in [13] and our algorithm.*

Exemplo 51 *Consider generating a uniform probability distribution for a random variable with* $n = 7$ *possible outcomes, using the coins* $m_1 = (1/2, 1/2)$ *and* $m_2 = (3/7, 4/7)$. *The tree in Figure H.2 results from the algorithm in [13], for which we compute the values* $E[T] = 3.29$ *and* $L_{\max} = 4$.

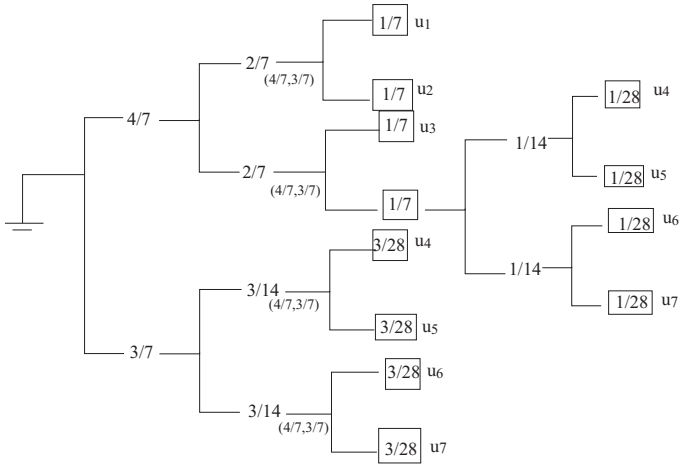


Figura H.2: Tree obtained using the algorithm in [13] for $n = 7$.

On the other hand using our algorithm, $L_{\max}$ *is unbounded (Figure H.3), but* $E[T] = 3.1902$ *which is a better result than that using the algorithm in [13].*

H.4 Conclusions

In this paper we presented a new algorithm for the generation of a discrete probability distribution using the flips of two or more coins, some of them biased. In particular, this

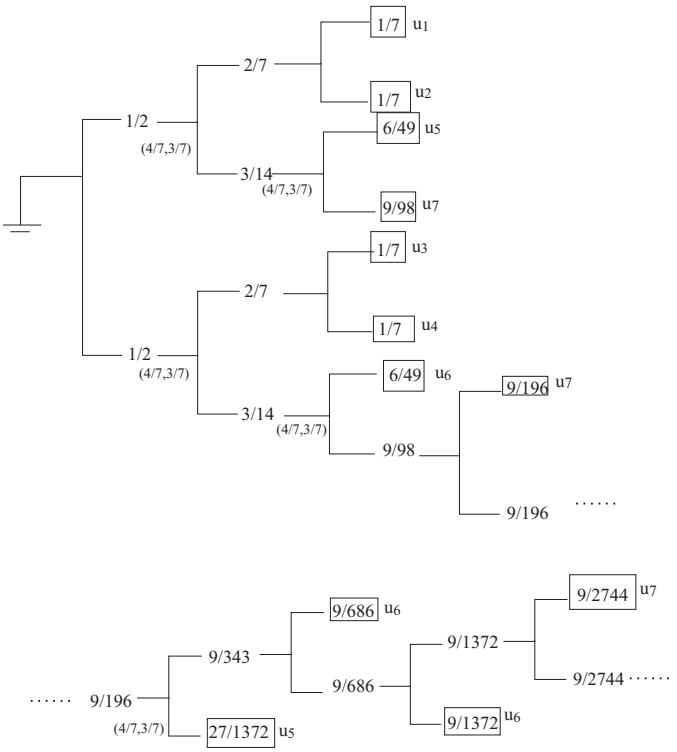


Figura H.3: Tree obtained using our algorithm for $n = 7$.

approach contributes an alternative solution to the classical problem of generating a discrete uniform probability distribution using two or more biased coins. It was shown by some simple examples that with this algorithm it is possible to obtain equivalent and in some cases even better results than those in [13] considering the short expected time approach. It is important to notice that the biased coins employed in our proposed algorithm are arbitrary, i.e., they do not depend on n as is the case with the algorithm in [13].

As a suggestion for future research we find interesting an investigation into ways to limit $L_{\max}$ in those cases where our proposed algorithm gave unbounded results, as long as the value of $E[T]$ remains smaller than that in [13].

Appendix

MIN-ENT per step algorithm

Let $\Pi_2 = \{p, 1-p\},\ p \geq 1/2$, be the probability distribution for the homophonic codeword symbols. For a given source, the MIN-ENT per step algorithm simultaneously finds the decomposition of each source symbol probability as a sum (finite or infinite) of terms $p^{\lambda}(1-$

$p)^{l-\lambda}$, and the corresponding prefix-free homophonic code, where λ is the number of 1's and $l-\lambda$ is the number of zeroes of a homophonic codeword of length l. The homophones are selected as terminal nodes in the binary rooted tree with probabilities, T. From any non-terminal node in this tree two branches emanate with probabilities p and $1-p=\overline{p}$, respectively. The label of a path in T is represented by the sequence of zeroes and ones associated with the branches constituting the path. The probability of a path of length l in T, containing λ 1's and $l-\lambda$ zeroes, is $p^{\lambda}(1-p)^{l-\lambda}$. In particular, for computing the probability of a terminal node we consider the path extending from the root node to that terminal node. Let $v(i,j)$ denote the j^{th} homophone assigned to the source symbol u_i, $1 \leq i \leq K$, $j = 1, 2, \ldots$. Let $\alpha(i,j)$ denote the probability of $v(i,j)$.

Definição 47 *We define the symbol running sum $\gamma_m(i)$, associated with the symbol u_i, $1 \leq i \leq K$, at the m^{th} iteration of the MIN-ENT per step algorithm as*

$$\gamma_m(i) = P_U(u_i) - \sum_{k=1}^{j} \alpha(i,k),$$

with $\gamma_m(i) = P_U(u_i)$ for $j = 0$, where j denotes the number of homophones allocated to u_i up to the m^{th} iteration.

Definição 48 *We define the running sum set Γ_m at the m^{th} iteration of the algorithm as*

$$\Gamma_m = \{\gamma_m(i) | \gamma_m(i) > 0, 1 \leq i \leq K\},$$

with $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

Let $\gamma_{\max} = \max \gamma_m(i) \in \Gamma_m$, $1 \leq i \leq K$. At $m = 0$ we grow T from the root, starting with only two leaves. We will expand each terminal node in T, whose probability exceeds $\gamma_{\max}$, by the least number of branches sufficient to make the resulting extended terminal node probability less than or equal to $\gamma_{\max}$. We call the resulting tree the *processed binary rooted tree with probabilities*, T_p. At the m^{th} iteration, $m \geq 1$, a homophone is assigned to a terminal node of the corresponding T_p, in a manner that the unused terminal node with largest probability P_m is assigned as a homophone to the symbol u_r with minimum nonnegative value for the difference between its homophone running sum $\gamma_m(r)$ and P_m, i.e., such that $\min_i\{\gamma_m(i) - P_m | (\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0$, $1 \leq i \leq K$. The algorithm consists of the following steps.

1. Let $m = 0$. Let $\gamma_0(i) = P_U(u_i)$, $1 \leq i \leq K$. Let $\Gamma_0 = \{P_U(u_1), P_U(u_2), \ldots, P_U(u_K)\}$.

2. Determine $\gamma_{\max}$ and produce the tree T_p for the m^{th} iteration by expanding each terminal node in the tree from the $(m-1)^{th}$ iteration, $m \geq 1$, whose probability exceeds $\gamma_{\max}$, by the least number of branches sufficient to make the resulting extended terminal node probability less than or equal to $\gamma_{\max}$.

3. Find the unused path E_l of length l in T_p whose probability is largest among unused paths, and denote this largest probability by P_m.

4. If, for $1 \leq i \leq K$, $\min_i\{\gamma_m(i) - P_m | (\gamma_m(i) - P_m) \geq 0\} = \gamma_m(r) - P_m \geq 0$, then we associate to u_r the homophone (terminal node) $v(r,j)$ and the binary homophonic codeword of length l, whose digits constitute the labelling of E_l in T_p. This implies $\alpha(r,j) = P_m$. Compute the symbol running sum $\gamma_m^{'}(r)$ after this decomposition and let $\Gamma_m^{'} = \Gamma_m - \{\gamma_m(r)\}$. If $\gamma_m^{'}(r) = 0$ then let $\Gamma_{m+1} = \Gamma_m^{'}$. The decomposition of $P_U(u_r)$ is now complete and contains j homophones, and if $\Gamma_{m+1} = \phi$ then END. Otherwise, i.e., if $\gamma_m^{'}(r) > 0$, then let $\Gamma_{m+1} = \Gamma_m^{'} \cup \{\gamma_m^{'}(r)\}$.

5. Let $m \leftarrow m+1$.

6. Go to step 2.

Acknowledgements

The authors acknowledge partial support of this research by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grants No. 141215/2002-0, 305226/2003-7 and 301253/2004-8, respectively.

References

[1] J.von Neumann, "Various techniques used in connection with random digits", notes by G. E. Forsythe, National Bureau of Standards, Applied Math Ser., vol. 12, pp. 36-38; reprinted in von Neumann's Collected Works., vol. 5. Oxford, U.K.: Pergamon, 1963, pp. 768-770.

[2] J. Abrahams, "Generation of discrete distributions from biased coins", *IEEE Trans. on Inform. Theory*, vol. 42, pp. 1541-1546, 1996.

[3] M. Blum, "Independent unbiased coin flips from a correlated biased source-A finite state Markov chain", *Combinatorica*, vol. 6, no. 2, pp. 97-108, 1986.

[4] E. W. Dijkstra, “Making a fair roulette from a possibly biased coin”, *Inform. Processing Lett.*, vol. 36, p. 193, 1990.

[5] P.Elias, “The efficient computation of an unbiased random sequence”, *Ann. Math. Statist.*, vol. 43, pp. 865-870, 1972.

[6] W. Hoeffding and G. Simons, “Unbiased coin tossing with a biased coin”, *Ann. Math. Statist.*, vol. 41, pp. 341-352, 1970.

[7] T. S. Han and M. Hoshi, “Interval algorithm for random number generation”, *IEEE Trans. on Inform. Theory*, vol. 43, pp. 599-611, March 1997.

[8] Y. Horibe, “Entropy and optimal random number transformation”, *IEEE Trans. on Inform. Theory*, vol. 27,pp.527-529, July 1981.

[9] D.E. Knuth and A. C. Yao, “The complexity of nonuniform random number generation", in Algorithms and Complexity, New Directions and Results, J. F. Traub, Ed. New York: Academic, 1976, pp.357-428.

[10] R. Motwani and P. Raghavan, *Randomized Algorithms. Cambridge*, U.K.: Cambridge Univ. Press, 1996.

[11] Q. F. Stout and B. Warren, “Tree algorithms for unbiased coin tossing with a biased coin”, *Ann. Probab.*, vol. 12, pp. 212-222, 1984.

[12] D. Feldman,R. Impagliazzo, M. Naor, N. Nisan, S. Rudich, and A. Shamir, “On dice and coins: Models of computation for random generation”, *Inform. Comput.*, vol. 104, pp. 159-174, 1993.

[13] L. Gargano and Ugo Vaccaro, “Efficient generation of fair dice with few biased coins ”, *IEEE Trans. on Inform. Theory*, vol. 45, pp. 1600-1606, July 1999.

[14] V. C. da Rocha Jr. and C. Pimentel, “Optimum binary-constrained homophonic coding”, *VII International Symposium on Communication Theory and Applications*, 13 - 18 July 2003, Ambleside, England, pp. 64-69.

Sobre a Autora

A autora nasceu em Recife, Pernambuco, no dia 9 de junho de 1974. Formada em Engenharia Elétrica, modalidade Eletrônica pela Universidade de Federal de Pernambuco (UFPE).

Obteve o título de Mestre em Engenharia Elétrica, área de concentração em Comunicações pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco, sob a orientação do Prof. Ricardo Campello Menezes de Souza, Ph.D., com a dissertação intitulada: "Criptografia de Chave Pública Baseada em Curvas Elípticas com Aplicações."

Entre suas áreas de interesse estão Criptografia, Teoria da Informação, Códigos Corretores de Erro e Biometria.

Endereço: Av. Manoel Borba, 738, apto: 902
Boa Vista
Recife – PE, Brasil
C.E.P.: 50.060 – 140

e-mail: dpbac@hotlink.com.br

Esta tese foi diagramada usando LaTeX 2_ε* pela autora.

*LaTeX 2_ε é uma extensão do LaTeX. LaTeX é uma coleção de macros criadas por Leslie Lamport para o sistema TeX, que foi desenvolvido por Donald E. Knuth. TeX é uma marca registrada da Sociedade Americana de Matemática ($\mathcal{AMS}$). O estilo usado na formatação desta tese foi escrito por Dinesh Das, Universidade do Texas. Modificado em 2001 por Renato José de Sobral Cintra, Universidade Federal de Pernambuco, e em 2005 por André Leite Wanderley.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo