DECODIFICAÇÃO DE CÓDIGOS DE BLOCOS CORRETORES DE ERROS COM DECISÃO SUAVE

Walter Godoy Júnior *

ABSTRACT

The aim of this work is to present procedures to increase the reliability of data transmission with the error correcting codes aid.

It is proposed a simplification in the best algorithm of symbol-to-symbol soft decoding for blocks codes.

RESUMO

O objetivo deste trabalho é mostrar procedimentos para se aumentar a confiabilidade em transmissão de dados com o auxílio de códigos corretores de erros.

É proposta uma simplificação no algoritmo ótimo de decodificação suave símbolo-a-símbolo para códigos de blocos.

OBJETIVO

A utilização de códigos controladores de erros provém da necessidade de armazenar e/ou transmitir um volume muito grande de dados, muitos dos quais são sensíveis a erros. Os códigos controladores de erros, hoje, são largamente utilizados em sistemas de comunicação via satélite, em redes locais de computadores, em discos a laser, em sistemas de telessupervisão e controle (como por exemplo no metrô de São Paulo), e em automação bancária. Este tipo de código também é empregado em ambientes industriais, onde a interferência causada pelas máquinas influencia nos sistemas de comando e comunicação. Em suma, onde se deseja uma alta confiabilidade na transmissão e/ou arquivo de dados, faz-se necessária a implementação de sistemas codificadores e decodificadores para códigos controladores de erros.

Os códigos controladores de erros, de acordo com as suas aplicações, dividem-se basicamente em dois tipos:

— códigos detetores de erros,

— códigos corretores de erros.

Os sistemas que usam somente códigos para deteção de erros são mais simples e, geralmente, permitem uma interrupção no fluxo de dados, pois estão associados a protocolos do tipo "ARQ" (SOLICITAÇÃO AUTOMÁTICA DE RETRANSMISSÃO). A deteção de erros é largamente utilizada em redes locais de computadores[1].

A correção de erros é utilizada em sistemas de fluxo contínuo de dados, onde, por motivos vários, não é possível repetir a mensagem. A correção de erros é muito utilizada em sistemas de comunicação via satélite, onde, devido às limitações impostas pelo peso e pela potência de transmissão do satélite, a confiabilidade só pode ser aumentada com o auxílio destes códigos.

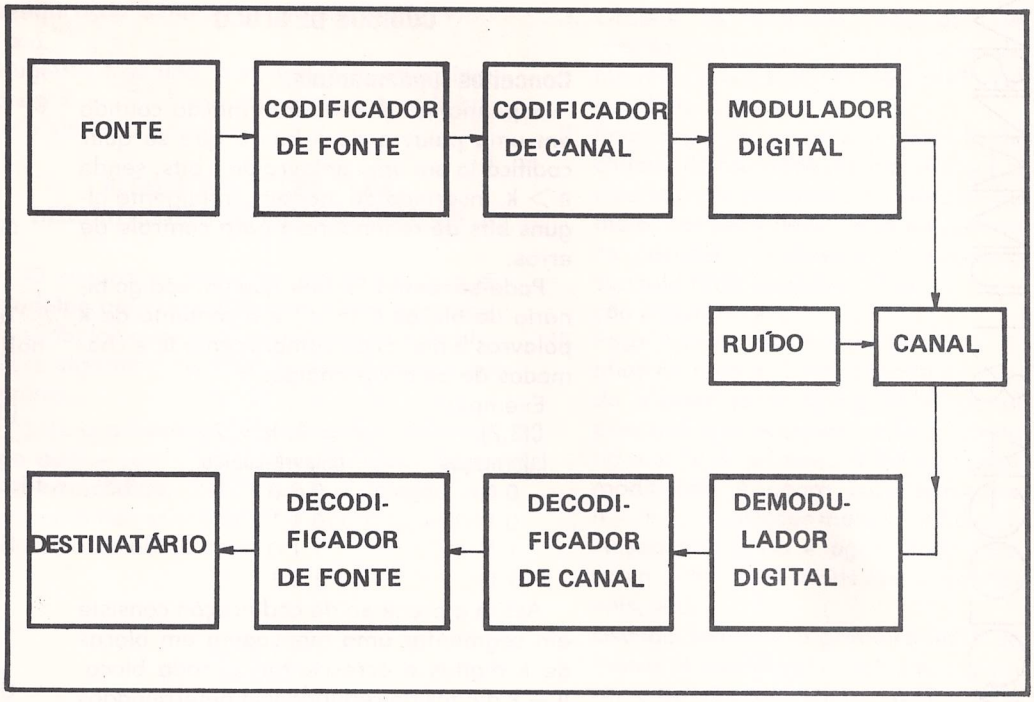
Existem, ainda em desenvolvimento, os chamados sistemas híbridos, que tentam conjugar as vantagens de ambos os sistemas.

Neste trabalho, abordar-se-á somente alguns algoritmos utilizados para códigos de bloco corretores de erros.

O CANAL DE COMUNICAÇÃO DIGITAL

De um modo geral, os sistemas de comunicação digital podem ser representados conforme o diagrama de blocos da fig. 1.

(*) **Walter Godoy Júnior.** *Mestre em Engenharia Elétrica — Telecomunicações pelo Instituto Eletrotécnico de Comunicações de Leningrado - URSS; Doutorando em Engenharia Elétrica, área de Comunicação da UNICAMP, Campinas, SP; Professor do Curso de Pós-Graduação em Informática Industrial (ênfase Telemática) do CEFET-PR.*



De acordo com esta figura, tem-se as seguintes funções:

— **Fonte:** gera a informação a ser transmitida;

— **Codificador de fonte:** codifica de uma maneira mais compacta os dados da fonte;

— **Codificador de canal:** adiciona redundância controlada à saída do codificador da fonte com a finalidade de combater os efeitos do ruído;

— **Modulador:** translada o sinal da saída do codificador para uma forma de onda adequada para a transmissão através do canal;

— **Canal:** meio físico pelo qual trafega a informação antes de chegar ao receptor. Pode ser um radioenlace, linha telefônica, qualquer meio de gravação;

— **Demodulador:** estima a forma de onda que foi enviada pelo transmissor e fornece, na sua saída, a versão digital correspondente;

— **Decodificador de canal:** tenta corrigir os possíveis erros e estima, então, os dígitos entregues pelo codificador de fonte;

— **Decodificador de fonte:** através de um processamento digital, repõe a redundância da informação, a qual foi removida na transmissão, antes de entregá-la ao destinatário; e,

— **Destinatário:** recebedor final da informação transmitida.

HISTÓRIA DOS CÓDIGOS CONTROLADORES DE ERRO

A história dos códigos controladores de erros teve início em 1948, com a publicação do artigo de Claude Shannon. Shannon mostrou que existe um número C, chamado de capacidade de canal e medido em bits por segundo, que está associado a cada canal, e que possui o seguinte significado: sempre que a taxa de transmissão R, em bits por segundo, de um sistema de comunicações for menor que C, então é possível projetar, para este canal, um sistema de comunicação com códigos controladores de erros, cuja probabilidade de erro na saída do sistema é tão pequena quanto se queira. Shannon não disse, porém, como encontrar estes códigos.

Em 1950 muito esforço foi concentrado para encontrar uma regra de formação de classes de códigos que produzissem a prometida probabilidade de erro. A primeira tentativa veio com os códigos de bloco com uma forte estrutura algébrica. O primeiro código de blocos foi introduzido por Hamming, em 1950, com a correção de apenas um erro. Desde então muitos tipos de códigos de blocos foram descobertos, sendo que os maiores progressos foram quando Bose e Ray-Chaudhuri (1960) e Hocquenghem (1959) encontraram uma grande classe de códigos corretores de múltiplos erros (códigos BCH) e quando Reed e Solomon (1960) encontraram a mesma classe de códigos para os canais não binários. A segunda tentativa veio com os códigos convolucionais. Nos códigos convolucionais os bits de redundância são entrelaçados com os de informação. Estes códigos podem ser vistos como códigos de blocos de comprimento infinito, sendo que para a sua decodificação é feita uma truncagem na seqüência recebida. Em 1967 foi desenvolvido o algoritmo de Viterbi para a decodificação destes códigos. Este algoritmo ganhou popularidade pela sua baixa complexidade. Antes disto, os códigos convolucionais eram decodificados por algoritmos seqüenciais.

Neste artigo, abordar-se-á somente os códigos de blocos binários.

CÓDIGOS DE BLOCO

Conceitos fundamentais.

Suponha-se ter uma informação contida em uma palavra de **k** bits e que se quer codificá-la em uma palavra de **n** bits, sendo $n > k$, inserindo de maneira inteligente alguns bits de redundância para controle de erros.

Pode-se, então, definir que um código binário de blocos C (n, k) é o conjunto de **k** palavras binárias de comprimento **n**, e chamadas de palavras-código.

Exemplo:

C(3,2)	n = 3, k = 2
informação	palavra-código
0 0	0 0 0
0 1	0 1 1
1 1	1 1 0
1 0	1 0 1

Assim o processo de codificação consiste em segmentar uma mensagem em blocos de **k** dígitos e acrescentar, a cada bloco, **n — k** dígitos de redundância determinados a partir dos **k** dígitos da mensagem.

Peso de uma palavra-código: é o número de posições não nulas da mesma.

Distância de Hamming: a distância de Hamming entre duas palavras de mesmo número de componentes é o número de posições onde os dois vetores diferem.

Distância mínima de um código: é a menor distância de Hamming encontrada entre suas palavras.

Código de blocos linear: um código de blocos linear binário é aquele que possui a palavra-código zero e que qualquer combinação (soma módulo-2) de duas ou mais palavras do código, gera uma palavra que também pertence ao código. Assim um código linear constitui um subespaço de 2^k palavras-código pertencentes ao espaço de 2^n palavras.

Matriz geradora: como um código linear constitui um subespaço, conseqüentemente qualquer palavra-código pode ser representada por uma combinação linear de palavras-código que são independentes e constituem, por isto, a base do subespaço. Os vetores da base podem ser escritos como linhas de uma matriz chamada de matriz geradora do código.

Matriz de cheque de paridade: Dada uma matriz geradora G de um código linear, com k linhas e n colunas, é possível formar uma outra matriz H, usada na decodificação, com n — k linhas e n colunas, de maneira tal que o subespaço gerado por esta matriz seja ortogonal ao subespaço gerado pela matriz G. Assim se V_i é um vetor do subespaço de G, então $V_i.H^T$ é a transposta da matriz H.

Exemplo:

Para um código de blocos C(5, 3), temos o seguinte conjunto de vetores:

(00000) (10011) (01010) (11001)

(00101) (10110) (01111) (11100)

que formam um subespaço vetorial V, e assim um código binário linear de blocos. O peso mínimo das palavras-código é igual a 2 e assim a distância mínima é também igual a 2. A matriz geradora para este código pode ser:

$$G = \begin{vmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} \text{ ou } G = \begin{vmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{vmatrix}$$

Temos o seguinte espaço nulo (ortogonal):

(00000) (11010) (10101) (01111)

A matriz de cheque de paridade será então:

$$H = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{vmatrix}$$

DECISÃO SUAVE

Usualmente nos sistemas de comunicações digitais, o canal de comunicação é tido como analógico, variando continuamente a amplitude no tempo. Como foi visto no início deste trabalho, um sistema de comunicação que utiliza canal analógico inclui o modulador/demodulador (modem) para transformar o canal analógico em um canal discreto, ligando assim o codificador/ decodificador (codec). Os códigos controladores de erro fornecem melhores resultados quando existe uma interação inteligente entre os projetos do modem e do codec. Nesta configuração, existe uma interação entre as teorias de comunicação, da informação e dos códigos corretores de erros.

Os algoritmos de decodificação que usam informação adicional do demodulador, são chamados de algoritmos de decisão suave. Assim para uma comunicação em BPSK, o demodulador fornecerá não apenas o sinal (+/—) da decisão abrupta, mas também a grandeza da amplitude do sinal. Devido a dificuldades de implementação, a amplitude do sinal entregue ao decodificador é quantizada (geralmente em oito níveis). Os decodificadores que utilizam decisão suave possuem um desempenho superior ao da decisão abrupta, porém à custa de um aumento de complexidade do circuito dos mesmos. Deste modo, para os códigos de bloco, estes decodificadores são utilizados para códigos de pequeno comprimento.

Existem duas regras básicas para a concepção da decisão suave. Uma é escolher a palavra-código que minimiza a distância Euclidiana entre esta palavra e o vetor recebido. Esta regra minimiza a probabilidade de erro da seqüência recebida. Uma outra regra consiste em minimizar a taxa média de erro de bit. Neste caso a seqüência decodificada não necessariamente será uma palavra-código. Os decodificadores que minimizam a taxa de símbolo utilizam os algoritmos de Massey (APP), de Hartmann-Rudolf (algoritmo ótimo para de-

codificação símbolo-a-símbolo) e de Weldon.

Neste trabalho, abordar-se-á, resumidamente, o algoritmo ótimo para decodificação símbolo-a-símbolo.

ALGORITMO ÓTIMO PARA DECODIFICAÇÃO SÍMBOLO-A-SÍMBOLO

O algoritmo proposto por Hartmann e Rudolph para decodificação ótima símbolo-a-símbolo[3] minimiza a taxa de erro de bit. Este algoritmo consiste basicamente no seguinte:

Seja c'_i a i-ésima palavra-código do código dual e seja c'_{ij} o j-ésimo símbolo desta palavra-código. Definir-se-á a relação de máxima verossimilhança ϕ_j para o j-ésimo símbolo recebido como:

$$\phi_j = \frac{P_r\,(r_j/1)}{P_r\,(r_j/0)}$$

onde $P_r(r_j/1)$ é a probabilidade do símbolo recebido ser 1 e $P_r\,(r_j/0)$ é a probabilidade do símbolo recebido ser 0.

Definiremos ainda a seguinte relação:

$$P_j = \frac{1 - \phi_j}{1 + \phi_j}$$

A regra de decodificação é a seguinte: Decodifique $C_M = 0$ se, e somente se,

$$f_d = \sum_{\lambda=1}^{2^{n-k}} \prod_{j=0}^{n-1} P_j^{\,c'_{ij} \oplus \delta_{jm}} \geqslant 0$$

onde δ_{jm} é igual a 1 quando $j = m$ e igual a 0 (zero) em caso contrário.

SIMPLIFICAÇÃO DO ALGORITMO DE HARTMANN/RUDOLFH

1 — Aproximação de Greenberger

Greenberger[2] propôs um método alternativo para a redução do número de equações de cheque de paridade usadas no algoritmo de HR. A base para esta técnica é de que os símbolos de baixa confiabilidade não contribuem com muita informação, e, portanto, as equações de paridade que contenham estes símbolos podem ser descartadas. O procedimento deste algoritmo é o seguinte:

I. Ordene os símbolos recebidos de acordo com as suas confiabilidades de maneira que o símbolo mais confiável encabece a lista.
II. Rearrange as colunas da matriz de cheque de paridade de maneira que a coluna correspondente ao símbolo de maior confiabilidade fique na primeira posição à esquerda, o segundo símbolo mais confiável fique na posição seguinte, etc.
III. Faça operações elementares de linhas na matriz H reordenada de modo a criar zeros acima da diagonal principal nas posições mais à direita na matriz. A primeira linha da matriz modificada é agora toda zero nas n — k — 1 posições menos confiáveis. A segunda linha é agora toda zero nas n — k — 2 posições menos confiáveis, etc.
IV. Usando somente a primeira linha da matriz H modificada, aplique o algoritmo de HR para estimar cada um dos símbolos recebidos. Esta operação usará somente duas palavras do código dual: a palavra de símbolos tudo zero e a palavra correspondente à primeira linha da matriz H.
V. Considere agora as primeiras duas linhas da matriz modificada H. Estas duas linhas gerarão quatro palavras do código dual. Duas destas palavras serão as duas geradas previamente e duas serão novas e conterão contribuições dos k + 2 símbolos mais confiáveis. Use as duas novas palavras para auxiliarem na estimativa dos símbolos recebidos.
VI. Continue adicionando novas linhas uma de cada vez e fazendo com que elas contribuam para a estimativa dos símbolos recebidos. Termine quando as estimativas tendam a se estabilizar ou quando um número pré-determinado de operações ocorrerem.
VII. Com base no mais recente conjunto de estimativas, escolha os k símbolos mais confiáveis que formem um conjunto de informação e codifique-os para gerar a palavra código.
VIII. Reordene os símbolos de maneira que os elementos da palavra voltem à sua ordem inicialmente recebida.

Os resultados parciais da simulação da simplificação de Greenberger para o código C (7,4) estão na figura 2. O passo de número 7 não foi considerado. Greenberger usou este procedimento para decodificar o código de Golay (23,12). Ele concluiu que esta técnica é particularmente eficiente para baixas relações sinal/ruído. O resultado que obtivemos nos leva à mesma conclusão.

Este algoritmo possui a desvantagem de que a forma particular da matriz H não pode ser computada antecipadamente e por isto não se pode utilizar as vantagens das propriedades cíclicas do código. Tem-se, ainda, que as operações com a matriz H e

com o vetor recebido são bastante complicadas. Levando esta última observação em consideração, propõe-se a seguinte modificação para este algoritmo:

— Para cada seqüência recebida escolhe-se um número fixo de bits menos confiáveis (por exemplo n — k — 1 bits).

— As combinações lineares da matriz H são feitas uma única vez e são escolhidas as palavras da mesma que contiverem o maior número de zeros nas posições dos bits menos confiáveis.

— Seqüencialmente se aplica o algoritmo de HR nestas palavras até que o limiar da soma seja atingido e aí, então, faz-se a decisão do bit.

Os resultados da modificação proposta estão na figura 2. O passo número 7 do algoritmo de Greenberger não existe nesta modificação, bem como as operações a matriz H e com o vetor recebido são mais simples. A degradação devido a esta modificação é muito pequena, como pode ser visto na figura 2. Para aumentar a velocidade de decodificação pode-se considerar que os K bits mais confiáveis estão corretos e assim para estes aplica-se a decisão abrupta. A degradação decorrente desta simplificação é pequena, como foi observado através de simulação.

COMENTÁRIO FINAL

Atualmente, no curso de Pós-graduação em Informática Industrial do CEFET-PR, está se desenvolvendo um projeto para o estudo e implementação de decodificadores que utilizam códigos de bloco e decisão suave. O grupo de pesquisa é composto pelo autor do presente trabalho e por alunos dos cursos de Pós-graduação em Informática Industrial e graduação em Engenharia Elétrica (Telecomunicações). Conta com o apoio financeiro do CONCITEC e está firmando convênio com o Centro de Pesquisa da Telebrás (CPqD) em Campinas, SP.

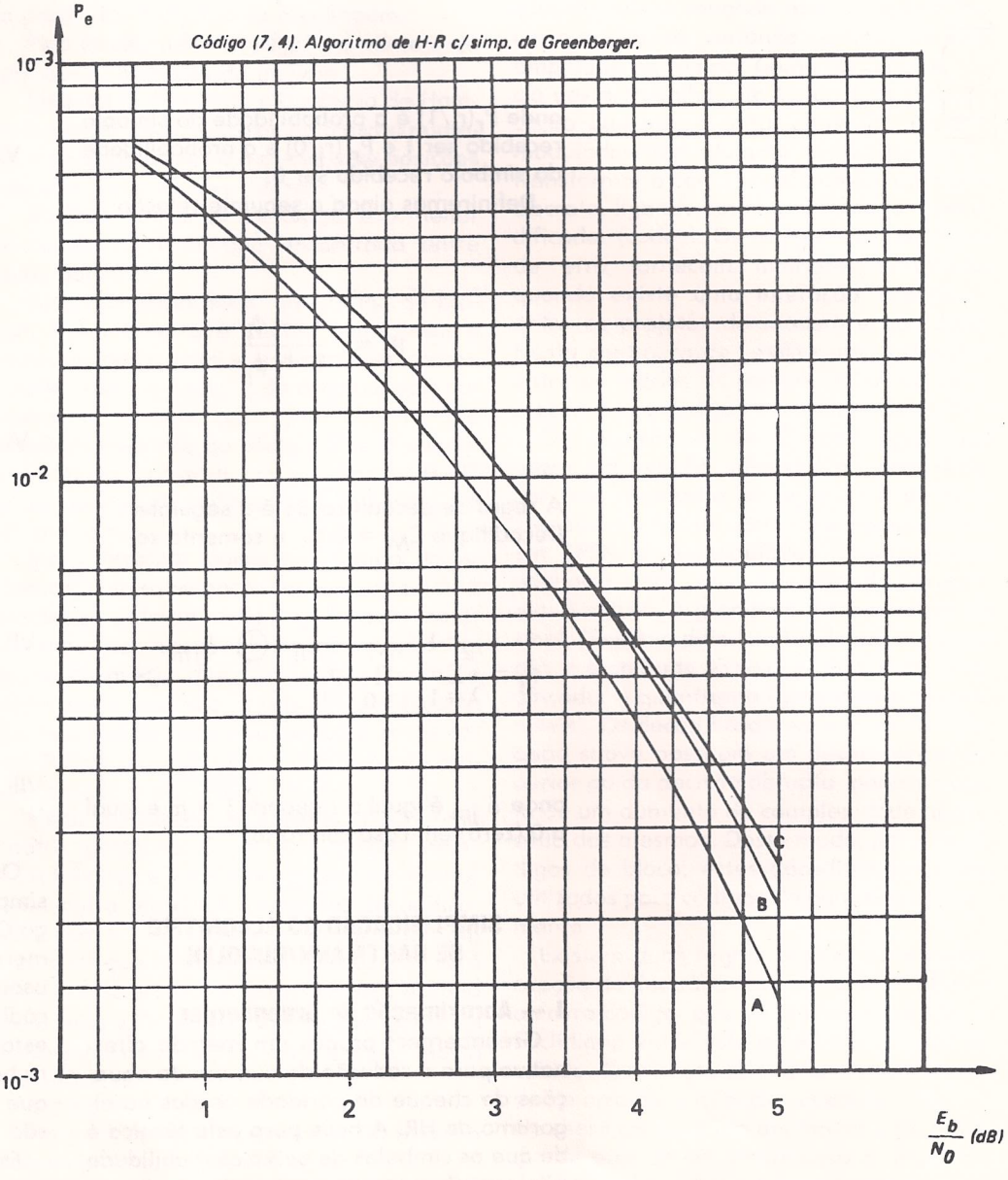


FIG. 2 – (A) Algoritmo de H – R completo. (B) Simplificação de Greenberger (limiar da soma: | 4,0 |) (sem inf. set). (C) Simplificação de Greenberger modificada $\{C_D\}$: 3 (sem inf. set).

REFERÊNCIAS BIBLIOGRÁFICAS

1. GIOZZA, W.F. [et all]. "Redes Locais de Computadores, Tecnologia e Aplicações", São Paulo, Mac Graw-Hill, 1986.

2. GREENBERGER, H. An Iterative Algorithm for Decoding Black Codes Transmitted over a memoryless Channel. J.P.L, DSN Progress. Report 42-47, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, July/Aug. 1978.

3. HARTMANN, C.R.P. & RUDOLPH, L.D. An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes. IEEE, Trans. on Inf. Theory, vol. II-22, nº 5, Sept. 1976.