Códigos Corretores de Erros

LUCAS MONTEIRO CHAVES[1]
KARINA DUTRA DE CARVALHO[1]
VANESSA GODOY KINOSHITA[1]

[1]UFLA – Universidade Federal de Lavras
DEX – Departamento de Ciências Exatas
Cx. Postal 37 – CEP 37.200-000 Lavras (MG)
lucas@ufla.br
dutra@comp.ufla.br
vakino@comp.ufla.br

Resumo: Os códigos corretores de erros se tornam cada vez mais uma ferramenta fundamental na teoria da informação. A necessidade de se garantir a integridade de uma grande quantidade de informação transmitida pelos mais variáveis meios exige o uso de sofisticados sistemas de códigos corretores de erros. Nesse artigo são descritos alguns aspectos básicos da teoria desses códigos.

Palavras Chaves: códigos corretores de erros, taxa de informação, teoria da informação, código de Golay, código de Reed-Muller.

1. Introdução

Teoria da informação como visto em [Jacobs (1992), p.155] trata dos aspectos quantitativos de armazenamento e transmissão das mensagens. Tem como um de seus objetivos principais garantir a integridade dos dados enviados através de algum tipo de canal. Na manipulação das mensagens, dois obstáculos são encontrados:

a) falta de capacidade no armazenamento ou transmissão das mensagens enviadas;

b) ruído na transmissão, ou seja, introdução aleatória de erros nas mensagens enviadas.

Ao contrário das teorias matemáticas que surgiram nas universidades e geralmente após um longo período de tempo migraram para as aplicações práticas em tecnologia e indústrias, a teoria de códigos corretores de erros surgiu nos laboratórios de empresas de telefonia e posteriormente se transformou em uma teoria matemática completa com aplicações em várias áreas como, por exemplo, geometria algébrica.

Um código corretor de erros visa recuperar informações que no processo de emissão tenham sofrido algum tipo de ruído. Pode-se afirmar que hoje praticamente todo sistema de envio de informações possui algum tipo de código corretor de erros. Como exemplos típicos, a telefonia digital, a transmissão de dados via satélite, a comunicação interna em computadores, armazenamento ótico de dados e armazenamento de dados em fitas ou disquetes magnéticos.

Segundo [Hefez (1994), p.5] todo sistema de envio de mensagem pode ser esquematizado da forma especificada na Figura 1:

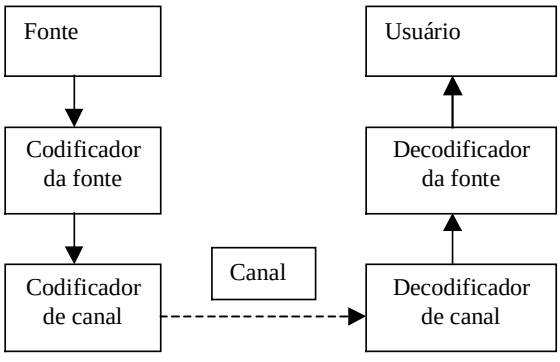

Figura 1: Esquema de transmissão.

O canal pode ser, por exemplo, circuito integrado digital, disco de armazenamento, cabo, canal de microondas, canal de radiofreqüência, etc.

2. Aplicações dos códigos corretores de erros

Com o aumento da confiabilidade nas comunicações digitais e a emergência do computador digital como ferramenta essencial na sociedade tecnológica, os códigos corretores de erros vêm conquistando uma posição prominente. Para ilustrar a praticidade e importância do uso de códigos corretores de erros temos:

a) uso do bit de paridade como um mecanismo detetor de erro - é um dos esquemas mais simples e conhecidos na comunicação computacional;

b) armazenamento em discos – estão sendo muito utilizados devido ao aumento da densidade. Quanto maior a densidade, a probabilidade de ocorrência de erros também aumenta;

c) transmissão de informação pelas naves espaciais:
   - em 1972 a espaçonave *Mariner* transmitiu figuras de Marte para a Terra com 64 tonalidades de cinza. Atividade solar e outras condições atmosféricas podem introduzir erros em sinais fracos vindos do espaço. O código utilizado foi o de Reed-Muller;
   - em 1979 a espaçonave *Voyager* começou a enviar imagens com 4096 tonalidades de cores. O código utilizado foi o de Golay;

d) áudio digital – o aumento da popularidade do áudio digital deve-se ao desenvolvimento dos códigos corretores de erros que facilita o processo de digitalização. Ao inicializar a leitura do CD, o sistema corrige os erros produzidos por marcas de dedos, arranhões e outras imperfeições, para logo em seguida transformar em sinais sonoros. O código utilizado é o de Reed- Solomon.

3. Conceitos Fundamentais

O ponto de partida é um conjunto finito A chamado de *alfabeto*. Seja *n* um número natural, um *código corretor de erros* é um subconjunto próprio qualquer de A^n. Uma classe particular de códigos são os códigos lineares. Neste trabalho consideraremos apenas este tipo de código. Por exemplo, seja A={0,1} e vamos considerar A^n (alfabeto binário). Um código corretor de erros sobre A^3 poderia ser: (000), (010), (100), (110). A quantidade de palavras do código, ou seja, a cardinalidade do código é menor ou igual a cardinalidade do conjunto A^n ($\#A^n$). No exemplo acima, a cardinalidade é 4.

Durante a transmissão dessas palavras por um canal físico, a informação é freqüentemente distorcida pelos ruídos. Para manejar essa indesejável mas inevitável situação, alguma forma de redundância deve ser incorporada à mensagem original. Com essa redundância, mesmo se alguns erros são introduzidos (em um nível tolerável), a informação original pode ser recuperada, ou pelo menos a presença desses erros pode ser detectada. Consideraremos nos próximos exemplos o código C = {(00), (01), (10), (11)}. Introduzindo redundância nas palavras do código, transformaremos as palavras de 2 bits para 5 bits:

00 - 00000

01 - 01011

10 - 10110

11 - 11101

Observa-se que os dois primeiros bits da informação com redundância correspondem à mensagem original. Define-se *k* como sendo o tamanho da palavra original e *n* o tamanho da palavra com redundância, no exemplo acima $k = 2$ e $n = 5$.

Define-se taxa de informação R como sendo

$$R = \frac{k}{n}$$

ou seja, a relação entre a informação original pela informação enviada.

Para a introdução da redundância, utiliza-se uma matriz *k* x *n*, cujas linhas são base vetoriais para o código C. Essa matriz é denominada matriz geradora [Vanstone & Oorschot (1989), p.51]. Através de operações elementares nas linhas e colunas (permutação de duas linhas, multiplicação de uma linha por um escalar não nulo, adição de um múltiplo escalar de uma linha a outra, permutação de duas colunas e multiplicação de uma coluna por um escalar não nulo) , pode-se colocar a matriz geradora G na forma padrão:

$$G = [I_d \; A]$$

onde I_d representa a matriz identidade *k* e A uma matriz *k* x (*n* - *k*). Assim, a informação original

estará nas primeiras *k* posições da palavra com redundância.

Seguindo o exemplo dado, temos a seguinte matriz geradora G:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

A partir da matriz geradora G, podemos construir uma matriz de teste de paridade H utilizada para decodificação das palavras. Com a matriz H, pode-se determinar se uma palavra pertence ou não ao código.

$$H = [A^t \; I_d]$$

No exemplo,

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

Para saber se a palavra pertence ao código, basta multiplicar a palavra recebida r pela matriz teste de paridade. Se o resultado for o vetor nulo,

$$H.r^t = \vec{0}$$

a palavra pertence ao código. Qualquer outro vetor não nulo como resultado significa que a palavra recebida contém erro.

Suponhamos que a palavra recebida seja r_1 = (10110) ,

$$H.r^t = \vec{0}$$

isto é, r_1 é uma palavra do nosso código.

Seja a palavra r_2 = (01010) ,

$$H.r^t = (001)$$

então a palavra contém erro(s).

O conceito fundamental para se trabalhar as palavras do código é a distância de Hamming [Vanstone & Oorschot (1989), p.7]. Dado dois elementos *u* e *v* do código, a distância de Hamming é definida por

$$d(u,v) = \#\{i \mid u_i \neq v_i,\ 1 \leq i \leq n\}.$$

Por exemplo, d(100, 101) = 1 e d(000, 111) = 3.

A distância do código *C* é a distância mínima entre todas as palavras do código.

$$d = \min \{d(u, v) \mid u, v \in C \text{ e } u \neq v \}.$$

Por exemplo, num código *C'* com palavras (00000), (01011), (10110), (11101), a menor distância é 3. A distância de um código é importante para determinar o número de erros que esse código detecta, assim como o número de erros que ele corrige.

Seja *C* um código com distância mínima *d*. Então *C* pode detectar até *d* - 1 erros e corrigir até α erros , onde

$$\alpha = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Por exemplo, no código *C* de distância 3 visto acima, pode-se detectar 2 erros e corrigir 1.

4. Decodificação

Para se decodificar uma palavra recebida *r*, uma estratégia deve ser adotada. Quando o decodificador recebe essa palavra, ele deve tomar uma decisão que pode ser:

a) nenhum erro ocorreu e *r* é aceita como uma palavra do código.

b) erros ocorreram, mas *r* é corrigida para uma palavra do código.

c) erros ocorreram ultrapassando o limite de correção do código, consequentemente *r* não pode ser recuperada.

Em geral, o decodificador nem sempre tomará a decisão certa, por exemplo, se muitos erros tiverem ocorridos durante a transmissão mudando uma palavra para outra do código, a informação está irremediavelmente perdida. Assumindo que o canal introduz erros aleatoriamente, o objetivo do decodificador é tomar a decisão com maior probabilidade de ser correta. Como exemplo de um algoritmo de decodificação temos o algoritmo do vizinho mais próximo. Quando uma palavra *r* é recebida, calcula-se a probabilidade de *r* ser *c*, para toda palavra *c* pertencente a *C*, onde *C* é um código . A palavra *r* será decodificada para aquela que tiver a maior probabilidade.

Ex.: Considerando o código

C = { (00000), (10110), (01011), (11101)}

e supondo que a probabilidade de ocorrência de erro seja *p* = 0,1 e que a palavra recebida seja *r* = (11111), calculamos todas as probabilidades:

$P(r, (00000)) = (0,1)^5 = 0,00001$

$P(r, (10110)) = (0,1)^2 \cdot (0,9)^3 = 0,00729$

$P(r, (01011)) = (0,1)^2 . (0,9)^3 = 0,00729$

$P(r, (11101)) = (0,1)^1 . (0,9)^4 = 0,06561$

Logo a palavra recebida r é corrigida para a palavra do código c = (11101).

Note que são necessários M cálculos, onde M representa a cardinalidade de *C*. Em um código grande (situações comuns), o cálculo fica inviável, comprometendo a decodificação, pois a complexidade do algoritmo é linear. Algumas classes particulares de códigos admitem um tratamento mais simples. Este é o caso dos códigos de Hamming [Vanstone & Oorschot (1989), p.65], que são capazes de corrigir um erro com um algoritmo bem simples, como se segue:

Seja H a matriz de paridade do código e r a palavra recebida.

(1) Calcule Hr^t.

(2) Se $Hr^t = 0$, então r é aceita como sendo a palavra transmitida.

(3) Se $Hr^t = s^t \neq 0$, então comparamos s^t com as colunas de H.

(4) Se há uma coluna i tal que $s^t = \alpha h_i$, então o erro e está na n-tupla com α na posição i e 0's nas outras posições; corrigimos r para $c = r - e$.

(5) Senão, mais de um erro ocorreu.

Em outros códigos mais complexos, a decodificação é mais precisa e eficiente.

5. Códigos Especiais

Dois dos códigos especiais são o de Golay (fotos coloridas) e o de Reed-Muller (fotos branco - preto) [Vanstone & Oorschot (1989), p.115].

O de Golay possui palavras de tamanho 24 (12 da informação original e 12 de redundância) e distância mínima 8. Assim, podemos corrigir 3 erros.

O de Reed-Muller possui palavras de tamanho 2^r (r+1 de informação original) e distância mínima 2^{r-1}. Assim, podemos corrigir 2^r erros.

6. Conclusão

Os códigos corretores de erros constituem hoje uma área de pesquisa ativa, tanto pelos aspectos matemáticos como pelos aspectos computacionais. Muitas questões ainda se encontram em aberto, por exemplo, encontrar o melhor código dado uma taxa de informação.

7. Referência bibliográfica

Vanstone, S. A. & Oorschot, P. "An introduction to error correcting codes with applications". *Klumer Academic Publishers*, 1989.

Jacobs, K. "Discrete Stochastics". *Birkhäuser Verlag Basel* , 1992.

Hefez, A. "Introdução à teoria dos códigos". *UNICAMP*, 1994.