UM DECODIFICADOR PARA CÓDIGOS DE HAMMING

Valdemar Cardoso da Rocha Júnior
Departamento de Eletrônica e Sistemas - UFPE
Cidade Universitária 50.741, Recife-PE

R E S U M O

Neste artigo mostra-se, inicialmente, que qualquer código de Hamming pode ser expresso como uma combinação linear de códigos simples, quais sejam, os códigos de repetição e de um único dígito de verificação de paridade. Tal propriedade permite tanto gerar como decodificar códigos de Hamming de modo recursivo, isto é, um código de Hamming de comprimento 2^m-1 pode ser obtido a partir de um código de Hamming de comprimento $2^{m-1}-1$, combinado com um código de repetição e um código de um único dígito de verificação de paridade, ambos de comprimento $2^{m-1}-1$. Quando apresentados nesta forma, os códigos de Hamming admitem um procedimento de decodificação simples e prático.

O desenvolvimento aqui apresentado refere-se aos códigos de Hamming ordinários e pode ser deduzido a partir da teoria dos códigos Reed-Muller, porém deve ser enfatizado que a referida teoria lida com os códigos de Hamming extendidos.

1. INTRODUÇÃO

Neste artigo mostra-se, inicialmente, que qualquer código de Hamming pode ser expresso como uma combinação linear de códigos simples, quais sejam, os códigos de repetição e de um único dígito de verificação de paridade. Tal propriedade permite tanto gerar como decodificar códigos de Hamming de modo recursivo, isto é, um código de Hamming de comprimento 2^m-1 pode ser obtido a partir de um código de Hamming de comprimento $2^{m-1}-1$, combinado com um código de repetição e um código de um único dígito de verificação de paridade, ambos de comprimento $2^{m-1}-1$. Quando representados nesta forma, os códigos de Hamming admitem um procedimento de decodificação simples e prático.

O desenvolvimento aqui apresentado refere-se aos códigos de Hamming ordinários e pode ser deduzido a partir da teoria dos códigos Reed-Muller, porém deve ser enfatizado que a referida teoria lida com os códigos de Hamming extendidos. Devido à sua importância prática, os códigos referidos a seguir serão sempre binários, salvo indicação contrária. A notação (n,k,d) será usada para representar um código de comprimento n, contendo k dígitos de informação e distância mínima d.

2. CÓDIGOS DE REPETIÇÃO

Os códigos de repetição (CR) tem seus blocos formados com um único dígito de informação, o qual é repetido n vezes. A distância mínima é portanto igual a n e o alfabeto consiste de apenas duas palavras, que são respectivamente as énuplas toda 1 e toda zero. Na recepção, a decodificação é feita por lógica de maioria da seguinte forma. Efetua-se a contagem do número de 1's da énupla recebida, compara-se o resultado com n/2 e decide-se pela palavra toda 1 caso a contagem exceda n/2, em caso contrário decide-se pela énupla toda zero. Quando n for par e ocorrer um empate na contagem dos 1's e zeros da énupla recebida, apenas deteta-se a ocorrência de n/2 erros. Os parâmetros dos códigos de repetição são, portanto:

Comprimento	:	n
Número de dígitos de informação	:	k = 1
Distância mínima	:	d = n

3. CÓDIGOS DE UM ÚNICO DÍGITO DE VERIFICAÇÃO DE PARIDADE

Estes códigos, referidos daqui por diante pela forma abreviada (UDP), tem cada uma de suas palavras composta por n-1 dígitos de informação e um único dígito de verificação de paridade. Este dígito de verificação de paridade é calculado como a soma modulo 2 dos dígitos de informação. O código resultante tem distância mínima dois, portanto apenas deteta a ocorrência de um número ímpar de erros.

Os parâmetros dos códigos UDP são os seguintes :

Comprimento : n

Número de dígitos de informação : k = n-1

Distância mínima : d = 2

4. CÓDIGOS DE HAMMING

Os códigos de Hamming corrigem um erro por palavra e são caracterizados pelos seguintes parâmetros :

Comprimento : $n=2^m-1$, $m>1$

Número de dígitos de informação : $k=2^m-1-m$

Distância mínima : $d=3$

Uma maneira simples de especificar um código de Hamming é através de sua matriz de verificação de paridade [H] . A matriz [H] destes códigos tem m linhas e $n = 2^m - 1$ colunas, sendo cada uma das n colunas representada por uma m-upla não-nula e distinta das demais [1]. Os códigos de Hamming são perfeitos [1] e são por demais conhecidos. Quando na forma cíclica, admitem procedimentos extremamente simples de geração e de decodificação.

5. CÓDIGOS REED-MULLER

Um código Reed-Muller (RM) de ordem r tem os seguintes parâmetros :

Comprimento : $n = 2^m$

Número de dígitos de informação : $k = 1 + \sum_{i=1}^{r} C_m^i$

Distância mínima : $d = 2^{n-r}$

Um código RM é usualmente denotado por R(r,m).

A teoria dos códigos RM é bem desenvolvida e encontra-se disponível na literatura especializada [1], [2].

A construção destes códigos é a seguir descrita, em termos da matriz geradora [G]. As linhas de [G] são formadas a partir de vetores v_i, $0 \leq i \leq m$, de comprimento $n = 2^m$, escolhidos do seguinte modo. O vetor v_0 é a énupla toda 1. Os demais vetores v_i, $1 \leq i \leq m$, são as linhas de uma matriz cujas colunas são todas as possíveis m-uplas binárias. A matriz [G] é então formada, tendo como linhas os vetores v_i, $0 \leq i \leq m$, juntamente com seus produtos dois a dois, três a três, etc.,... , m a m. O produto de vetores, acima referido, é definido do seguinte modo :

$a = (a_1, a_2, a_3, \ldots\ldots, a_n)$

$b = (b_1, b_2, b_3, \ldots\ldots, b_n)$

$ab = (a_1b_1, a_2b_2, \ldots\ldots, a_nb_n)$

Os códigos RM são não-sistemáticos e podem ser decodificados por um método clássico, conhecido por algorítmo de Reed [1]. Recentemente um outro procedimento de decodificação para estes códigos foi introduzido [3].

Uma propriedade importante dos códigos RM é a que permite gerá-los de forma recursiva [2] conforme indicado a seguir :

$$R(r+1,m+1) = \{u|u+v : u\varepsilon R(r+1,m),\ v\varepsilon R(r,m)\} \qquad (1)$$

Fazendo r = m-2 em R(r,m), o código R(m-2,m) resultante é equivalente a um código de Hamming com um dígito de verificação de paridade adicional. Os códigos R(m-1,m) obtidos fazendo-se r = m-1 em R(r,m), possuem um único dígito de verificação de paridade.

Os códigos de Hamming extendidos podem ser gerados recursivamente, bastando para tanto fazer r = m - 2 em (1). Dessa forma é obtida a seguinte expressão de recorrência :

$$R(m-1,m+1) = \{u|u+v : u\varepsilon R(m-1,m),\ v\varepsilon R(m-2,m)\} \qquad (2)$$

6. GERAÇÃO RECURSIVA DOS CÓDIGOS DE HAMMING

A notação H(s) e UDP(s) será usada a seguir para indicar, respectivamente, os códigos de Hamming e de um único dígito de verificação de paridade, ambos de comprimento 2^s-1, enquanto que I(s) indicará a simples presença de 2^s-1 dígitos de informação.

Suprimindo-se uma coluna de dígitos de verificação de paridade do dicionário do código RM indicado em (2), obtém-se um código de Hamming com a seguinte fórmula de recorrência, onde $m \geq 2$

$$H(m) = \{u+h|v : h\varepsilon H(m-1),\ u\varepsilon I(m-1),\ v\varepsilon UDP(m-1)\} \qquad (3)$$

Com relação ao código R(m-1,m+1), o código H(m) dado por (3) tem o mesmo número de dígitos de informação, porém uma distância mínima de 3, como consequência da supressão de uma coluna. Portanto, H(m) é de fato um código de Hamming ordinário, expresso numa forma não-sistemática.

O exemplo apresentado a seguir ilustra a geração do código de Hamming (7,4,3) empregando (3).

EXEMPLO 1

Para m = 2 o código de Hamming obtido tem parâmetros (3,1,3), ou seja, é equivalente a um código de repetição. Para m = 3, o código (7,4,3) resultante não evidencia uma relação óbvia com os códigos CR e UDP. Sejam k_1, k_2, k_3 e k_4 os dígitos de informação do código (7,4,3). A codificação das palavras é feita do seguinte modo. Inicialmente forma-se o vetor $(k_1, k_1, k_1, 0, 0, 0, 0)$ cujas três primeiras posições constituem uma palavra do código de repetição (3,1,3). Em seguida é formado o vetor $(k_2, k_3, k_4, k_2, k_3, k_4, c)$ onde $c = k_2+k_3+k_4$ representa o dígito de paridade do código (4,3,2), cujas posições de informação são ocupadas por k_2, k_3 e k_4. Somando os dois vetores obtém-se como resultado uma palavra do código (7,4,3).

7. DECODIFICAÇÃO

Supondo que uma palavra b do código H(m) é transmitida, mostra-se a seguir como proceder para detetar e corrigir um erro que eventualmente venha a atingí-la.

a) Recalcular o dígito de verificação de paridade do segmento v da énupla recebida e compará-lo com o seu correspondente recebido. Caso ambos coincidam, os u dígitos de informação de v são declarados livres de erro e são entregues ao destinatário. Em caso contrário, há um erro entre os referidos dígitos do segmento v.

b) Adicionar modulo 2, bit a bit, os dígitos nas posições de informação de v às correspondentes posições do segmento representado por u+h. Esta operação permite prosseguir com a decodificação trabalhando agora sobre o código H(m-1).

c) Aplicam-se os procedimentos descritos em a) e b) ao código H(m-1), reduzindo o problema à decodificação do código H(m-2) e assim sucessivamente até a obtenção do código (3,1,3). O código (3,1,3) é do tipo CR e é decodificado por voto de maioria, dando como resultado o valor de k_1.

d) Caso tenha ocorrido um erro, somar modulo 2, às três primeiras posições da énupla recebida, o valor de k_1 obtido em c). Desta forma remove-se o efeito de k_1 sobre o código (7,4,3). A correção de k_2, k_3 e k_4 é feita por comparação das posições que se correspondem no código C(3), onde :

$C(3) = \{u|v : u \in CR(2), v \in UDP(2)\}$

Para o par de dígitos que discordar, o dígito de verificação de paridade indica qual dos dois é o errado. Este procedimento vai sendo repetido, nas demais etapas intermediárias, aos códigos H(m-i), $m \leq i \leq m-2$, até completar a decodificação.

EXEMPLO 2

Neste exemplo é considerada a decodificação do código (7,4,3) do exemplo 1. A decodificação obedece a seguinte sequência :

a) Recalcula-se c na palavra recebida. Caso ocorra c = 0, então k_2, k_3 e k_4 estão livres de erro e são entregues ao destinatário. Caso ocorra c = 1, então há um erro em um dos quatro dígitos situados mais à direita na palavra recebida.

b) Soma-se modulo 2 as posições 1 e 4, 2 e 5, 3 e 6, eliminando-se o efeito de k_2, k_3 e k_4 sobre a palavra recebida. Toma-se para k_1 o valor assumido pela maioria das três somas indicadas.

c) Remove-se o efeito de k_1 nas três primeiras posições da palavra recebida somando-o modulo 2 a cada uma delas.

d) Finalmente, obtém-se k_2, k_3 e k_4 por comparação das posições de 1 e 4, 2 e 5, 3 e 6.

8. COMENTÁRIOS

O procedimento de codificação descrito dá origem a um código parcialmente sistemático. Como consequência, com um único dígito de verificação de paridade de codifica-se a maioria dos dígitos de informação, exceto em cerca de metade das vezes em que ocorre erro. Em sistemas codificados adaptativos, o procedimento aqui introduzido proporciona a flexibilidade necessária para a mudança de códigos e a correspondente alteração do decodificador.

9. AGRADECIMENTOS

Este trabalho recebeu apoio parcial do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

10. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Peterson, W.W. & Weldon, E.J., (1972). Error Correcting Codes, MIT Press, segunda edição, capítulo 5.

[2] MacWilliams, F.J. & Sloane, N.J.A., (1977). The Theory of Error-Correcting Codes, North-Holland, capítulo 13.

[3] Tokiwa, K. et alii, (1982). "New Decoding Algorithm for Reed-Muller Codes, IEEE Trans. IT, vol. IT-28, Nº 5, setembro, pp. 779-787.