ANTICÓDIGOS PARA A CONSTRUÇÃO DE CÓDIGOS LINEARES

Marcia M. Campello de Souza e Ricardo M. Campello de Souza

Deptº. de Eletrônica e Sistemas CT-UFPE, 50.741 Recife - PE

RESUMO

O problema de se encontrar um procedimento sistemático geral para a construção de códigos corretores-de-erro, ótimos ou quase-ótimos, à parte de casos isolados, continua sendo um desafio para os pesquisadores da área. Neste contexto, o conceito de anticódigos substancialmente simplifica e unifica a busca para tais códigos. Neste trabalho, um procedimento sistemático para obtenção de anticódigos é apresentado, através dos quais, removendo-os de uma classe de códigos ótima, códigos ótimos ou quase-ótimos, são obtidos. A abordagem apresentada aqui usa conceitos de Teoria de Grafo e é desenvolvida pela introdução do grafo-anticódigo.

Uma cota inferior sobre o número de palavras anticódigo é estabelecida, e todos os anticódigos construídos satisfazem-na com igualdade. ●

1. INTRODUÇÃO

Técnicas de construção para a geração de códigos com parâmetros ótimos tem sido a preocupação de muitas investigações. Neste contexto, o conceito de anticódigos tem mostrado ser um método muito interessante para a construção de classes de códigos ótimas [1-4]. Um anticódigo é definido como um arranjo de N linhas e m colunas com a propriedade de que a distância máxima de Hamming entre quaisquer par de linhas é menor ou igual a um certo valor δ. Se o anticódigo é linear e tem símbolos em GF(2), então ele tem $N=2^k$ palavras anticódigo, para um dado inteiro k, as quais formam um grupo. Um anticódigo é dito ser ótimo se ele tem a mínima distância máxima de Hamming, δ, para um dado valor de m, o comprimento da palavra anticódigo, e k. Se um anticódigo binário linear ótimo é removido de um código de sequência-m [5] com o mesmo parâmetro k, um código binário linear ótimo é obtido; isto é, o código tem a máxima distância mínima para seus parâmetros. Além do mais, para um dado valor de m, é somente necessário encontrar no máximo dois anticódigos ótimos para qualquer k possível. Portanto, um grande número de códigos ótimos ou quase-ótimos podem ser derivados destes dois anticódigos [4]. Embora muitos anticódigos ótimos tenham sido encontrados por exaustivas buscas em computador, um procedimento sistemático para geração de um anticódigo ótimo com qualquer conjunto de parâmetros desejado ainda não havia sido apresentado. A abordagem baseada na teoria de grafo introduzida aqui, estabelece tal procedimento.

2. A CONSTRUÇÃO DO GRAFO-ANTICÓDIGO

O problema de se construir anticódigos lineares ótimos pode alternativamente ser visto como o problema de se gerar um subconjunto de V_m com certos atributos, onde V_m é o espaço vetorial de todas as m-uplas binárias. Uma vez que a teoria de grafo lida com o desenvolvimento de algorítmos que, em essencia, selecionam um conjunto de vértices com certas propriedades definidas de um grafo, é então adequado investigar o problema mencionado acima do ponto de vista de teoria de grafo. Mais precisamente, o problema pode ser desenvolvido pela introdução do grafo-anticódigo.

Definição 1:

O grafo-anticódigo com parâmetros m (comprimento) e δ (distância máxima), AG(m,δ), é definido como sendo o grafo com um vértice para cada um dos 2^m vetores m-dimensionais de V_m e existe um ramo entre dois vértices se e somente se a distância entre eles é maior que δ. Um anticódigo neste grafo é representado por um conjunto independente do grafo. O exemplo a seguir mostra o grafo-anticódigo, AG(4,2).

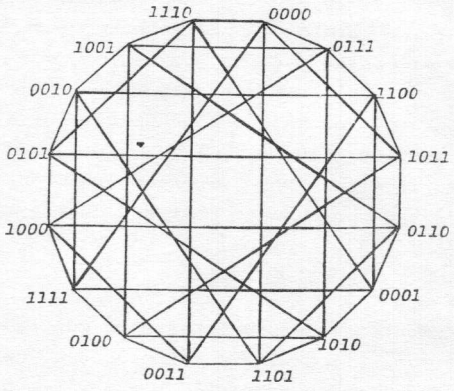

Fig. 1 AG(4,2)

Para valores de m e δ de interesse o tamanho dos grafos sob discussão será excessivamente grande e os algorítmos existentes na teoria de grafo para computar conjuntos independentes tornam-se inadequados [6-8]. Na tentativa de vencer estas dificuldades, muitas propriedades estruturais deste grafo foram investigadas. Algumas delas são brevemente descritas abaixo [9].

3. PROPRIEDADES DO GRAFO-ANTICÓDIGO

3.1. Regularidade

O grafo-anticódigo é regular e o grau de cada vér

tice é dado por

$$D = \sum_{i=\delta+1}^{m} \binom{m}{i} \quad \text{se } m \neq \delta \qquad (3.1)$$

onde $\binom{m}{i} = \frac{m!}{(m-i)!\,i!}$

e D é chamado o grau do grafo.

3.2. O Tamanho do "GIRTH" G (AG)

O tamanho do "girth" [10] de AG (m,δ) é dado por:

(i) $g(m,\delta)=3$ se $m \geq \delta+1+\lceil(\delta+1)/2\rceil$, $\delta \geq 1$ (3.2)

(ii) $g(m,\delta)=4$ se $\delta+2 \leq m < \delta+1+\lceil(\delta+1)/2\rceil$, $\delta>1$ (3.3)

(iii) $g(m,\delta)=\infty$ se $m<\delta+2$ (3.4)

onde $\lceil x\rceil$ é o menor inteiro $\geq x$

3.3. O Grafo Hamiltoniano

Pode ser mostrado que todo grafo-anticódigo que satisfaz a condição de exsitência de um ciclo é Hamiltoniano, isto é, ele tem um ciclo Hamiltoniano [9] . Se um conjunto de vetores base b_j de V_m é escolhido de tal forma que o peso de cada vetor é maior que δ, então existe um arranjo $x_1, x_2 \ldots x_{2^m}$ de elementos de V_m onde $x_i = x_{i-1} + b_j$ para $i=1,2\ldots 2^m$ tal que dois vetores sucessivos na sequência são adjacentes no grafo-anticódigo, assim gerando um Ciclo Hamiltoniano [9]. O exemplo dado na Fig. 1 mostra um Ciclo Hamiltoniano com respeito à base {0111, 1011, 1101, 1110}.

3.4. Coloração dos Vértices

A coloração de todos os vértices de um grafo tal que nenhum vértice adjacente tenha a mesma cor é chamada a coloração do grafo e usualmente um grafo pode ser colorido de diversas maneiras. Um grafo G que requer não menos que γ cores diferentes para sua coloração é chamado um grafo γ-cromático e o número $\gamma(G)$ é chamado o número cromático de G.

Uma cota inferior sobre γ para o grafo-anticódigo pode ser derivada e pode ser mostrado que se ele satisfaz a expressão (3.2) então:

$$\gamma(m,\delta) \geq 3 \qquad (3.5)$$

O estabelecimento de outras cotas será mostrado na seção 5. A partição, induzida pela coloração do grafo, produz conjuntos independentes. Um algorítmo para coloração de vértices do grafo-anticódigo, que usa os princípios de contração, é desenvolvido na próxima seção para a construção de anticódigos.

4. O ALGORÍTMO DE CONTRAÇÃO

Um algorítmo eficiente para a geração de conjuntos independentes do grafo-anticódigo foi desenvolvido. Isto é um algorítmo de contração [10-11] e é descrito abaixo.

Os vértices do grafo são ordenados em um ciclo Hamiltoniano (seção 3.3) com o vetor todo zero na metade à direita. Um vértice arbitrário, β_1, não adjacente ao vetor todo zero e portanto com peso $\leq\delta$, na metade à esquerda, é selecionado. Então os vetores x no lado direito são grupados com os vetores $x \oplus \beta_1$ no lado esquerdo, onde $\oplus$ indica adição módulo-2. Isto contrai o grafo à metade do número de seus vértices e cada vértice no grafo contraído tem um par de vetores associado a ele. O novo grafo é agora dividido ao meio e outro vértice, β_2, não adjacente ao vértice que contém o vetor todo zero, é selecionado. O processo é repetido até que um grafo completo seja obtido. Cada conjunto de vetores associado aos vértices do grafo completo é um anticódigo (m,δ); o conjunto contendo o vetor todo zero é um anticódigo linear. Para ilustrar o algorítmo descrito acima um exemplo é dado. Aqui vamos usar a notação $G_i(v,e)$, onde v é o número de vértices de G_i, e é o grau de cada vértice em G_i e i é o número de interações, para representar o grafo contraído em cada estágio do processo. O exemplo a seguir ilustra o procedimento.

Exemplo : Construir o anticódigo (3,2). O grafo-anticódigo AG(3,2) é representado na Fig. 2.

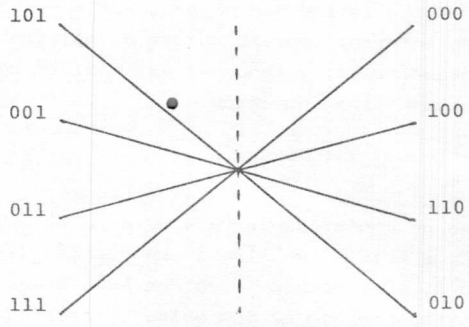

Fig. 2 $AG(3,2) \equiv G_0(8,1)$

O primeiro passo do processo produz o seguinte grafo contraído :

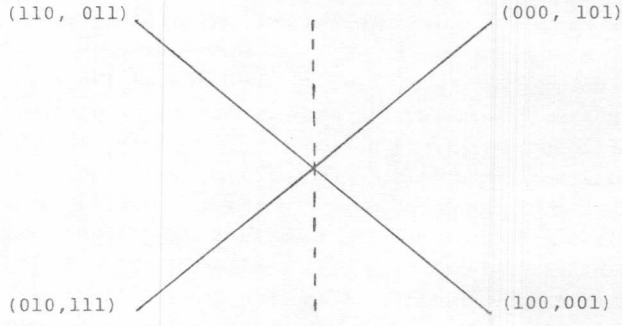

Fig. 3 $G_1(4,1)$

Uma segunda interação é necessária, resultando no seguinte grafo :

(100,001,010,111) ——————— (000,101,110,011)

Fig.4 $G_2(2,1)$

onde um grafo completo foi gerado. O conjunto com o vetor todo zero é o anticódigo linear (3,2).

5. COTAS

Um limite inferior sobre o número de palavras anticódigo foi estabelecido e é dado por

$$N \geq 2^m/p \qquad (5.1)$$

onde p é a maior potência de 2 menor ou igual a D+1, sendo D o grau do grafo.

O algorítmo de contração apresentado é também um algorítmo para coloração do grafo como mencionado na seção 3.4. Assim, um limite superior para o número cromático, $\gamma(m,\delta)$, do grafo-anticódigo foi derivado e temos

$$\gamma(m,\delta) \leq |V_m|/N \qquad (5.2)$$

6. RESULTADOS E CONCLUSÕES

O objetivo principal deste trabalho é fornecer um procedimento sistemático para obtenção de anticódigos ótimos e, consequentemente, códigos ótimos e quase-ótimos. O problema de se construir anticódigos é examinado do ponto de vista da Teoria de Grafo e esta abordagem é desenvolvida pela introdução de um grafo particular, o qual contém todas as informações necessárias para geração de anticódigos de um determinado comprimento m e distância máxima δ. Isto leva à criação do grafo-anticódigo $AG(m,\delta)$. O anticódigo linear (m,δ) é representado por um conjunto independente de $AG(m,\delta)$ o qual é também um subespaço de V_m.

Um procedimento sistemático para construção de anticódigos lineares ótimos é descrito na seção 4. A tabela 1 abaixo lista alguns dos anticódigos que foram obtidos pelo algorítmo descrito acima.

O grafo-anticódigo pode ser facilmente estendido para anticódigos multi-níveis e uma generalização do algorítmo de contração para o caso q-ário tem sido analisado. Anticódigos multi-níveis [12] são de interesse particular por causa da falta relativa de técnicas de construções sistemáticas para códigos multi-níveis comparados às do caso binário.

AGRADECIMENTOS

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

m	k ≥	δ
1	1	1
3	2	2
4	3	3
7	3	4
8	4	5
10	4	6
11	4	7
15	4	8
16	5	9
17	5	10
18	5	11
21	5	12
22	5	13
25	5	14
26	5	15
31	5	16
32	6	17
33	6	18
34	6	19
37	6	20
38	6	21
40	6	22

TABELA 1 - ANTICÓDIGOS BINÁRIOS LINEARES ÓTIMOS EM δ

REFERÊNCIAS

01. Farrell, P. G., "Linear Binary Anticodes", Electronic Letters, Vol. 6, Nº 13, June 1970.
02. Farrell, P. G. and Farrag, A., "Further Properties of Linear Binary Anticodes", Electronics Letters, Vol. 10, Nº 16, August 1974.
03. MacWilliams, F. J. and Sloane, N. J. A.,"The Theory of Error Correcting Codes", North-Holland, 1978.
04. Farrell, P. G., "An Introduction to Anticodes", Chapter 3 in "Algebraic Coding Theory and Applications", ed. G. Longo, Springer-Verlag, 1979.
05. Peterson, W. W. and Weldon, Jr. E. J., "Error-Correcting Codes", 2nd ed. MIT Press, 1972.
06. Christofides, N., "Graph Theory an Algorithmic Approach", Academic Press, 1975.
07. Matula, D. W. Marble, G. and Isaacson, J. D., "Graph Coloring Algorithms, in "Graph Theory and Computing" ed. R. C. Read, Academic Press, 1972.
08. Tarjan, R. E. and Trojanowski, A. E., "Finding a Maximum Independent Set", SIAM J. Comput. Vol.6 , Nº 3, September, 1977.
09. Campello de Souza, M. M., "A Graph-Theoretic Approach to Anticodes", Ph.D. Thesis, University of Manchester, Manchester, 1983.
10. Bollobás, B., "Extremal Graph Theory", Academic Press, 1978.
11. Berge, C., "Graphs and Hypergraphs", North Holland, 1979.
12. Farrag, A., "Anticodes and Optimum Error-Correcting Codes", Ph.D. Thesis University of Kent, Canterbury, 1976.