Uma Introdução a Anticódigos

Marcia M. Campello de Souza

Neste trabalho, os conceitos fundamentais de anticódigos são apresentados. Um anticódigo, com símbolos em GF(q), é um arranjo de N linhas e m colunas tal que a distância máxima de Hamming entre qualquer par de linhas é menor ou igual a δ. Como é mostrado, um anticódigo apresenta propriedades opostas àquelas de um código. Assim, um anticódigo ótimo tem um valor máximo de m para N e δ dados, ou um valor mínimo de δ para m e n dados. Procedimentos para geração de códigos corretores de erro, baseados no conceito de anticódigos, são investigados. Como resultado, diversos códigos com parâmetros ótimos são obtidos, a partir da remoção de um anticódigo de seu código de seqüência-m.

1. Introdução

Embora a teoria da codificação seja uma área já bem estabelecida [**1**]-[**5**] e tenha uma importância fundamental no presente estado da arte das comunicações, o problema de se encontrar um procedimento sistemático para gerar códigos corretores de erro ótimos, à parte de casos isolados, continua sendo um desafio para os pesquisadores da área. Neste contexto, o conceito de anticódigos tem mostrado ser um método importante como uma maneira de simplificar e unificar a busca para tais códigos. Neste trabalho, os conceitos fundamentais de anticódigos lineares são apresentados. Técnicas de construção para encontrar códigos corretores de erro baseadas no conceito de anticódigos são investigadas e códigos gerados por este método são mostrados.

Inicialmente, procedimentos de perfuração são analisados, e os anticódigos são definidos e descritos em termos das matrizes geradora e de paridade. Em seguida, a distância máxima de um anticódigo é introduzida e cotas sobre seus parâmetros são analisadas. Métodos de construção de anticódigos lineares binários são apresentados e podem, então, ser usados para produzir códigos lineares binários sem colunas repetidas e com comprimento de bloco n satisfazendo a condição $k \leq n \leq 2^k-1$, onde k é o número de dígitos de informação no bloco.

A autora é Professora do Departamento de Eletrônica e Sistemas da Universidade Federal de Pernambuco, 50741, Recife, PE.

2. Descrição do Conceito de Perfuração

Um código de bloco corretor de erro pode ser descrito por uma matriz Nxn, que é o dicionário do código. As N linhas do dicionário do código são as palavras código; as n colunas são também importantes e são chamadas de colunas código. Para um código linear sobre GF(q), o dicionário do código consiste de $N = q^k$ palavras código, onde q é uma potência de um número primo e cada palavra código é constituída de k dígitos de informação e n-k dígitos de redundância. O dicionário do código tem, portanto, k colunas de informação e n-k de redundância. Se for considerada a forma sistemática do código, as k primeiras colunas são as colunas de informação e as últimas n-k são as colunas de redundância.

Códigos de bloco lineares com parâmetros $n=q^k-1$, k e distância mínima $d = (q-1)q^{k-1}$ são descritos na literatura [**1**] e têm grande importância no estudo de anticódigos. Esses são os códigos simplex, também chamados códigos de seqüência-m. Solomon e Stiffler [**6**] estabeleceram a importância dos códigos de seqüência-m, mostrando que todos os códigos lineares (n, k, d), ótimos ou não, sem colunas repetidas, podem ser gerados removendo-se algumas colunas de um código de seqüência-m. Aqui, o termo código ótimo será usado no sentido de que, para um dado par de valores n e k, o valor de d é o maior possível. Um método para a construção de tais códigos foi também estalecido [*7*].

A idéia de suprimir certas colunas de um código de seqüência-m pode ser estendida pela introdução do conceito de anticódigos, e foi inicialmente apresentada por Farrell [**8**] e [**2**]. O uso da teoria de anticódigos produz uma vasta classe de códigos perfurados [**9**], os quais são ótimos ou quase ótimos e incluem a família dos códigos Solomon-Stiffler.

3. Anticódigos

Considere-se o dicionário do código de seqüência-m com $n=q^k - 1$ colunas e $N = q^k$ linhas. Se m colunas são removidas deste dicionário então outro código é obtido com o mesmo número de linhas, q^k, e $q^k - 1 - m$ colunas. O código de seqüência-m é equidistante, isto é, todas as linhas têm peso de Hamming (ou simplesmente peso) igual a $(q - 1)q^{k-1}$, exceto a linha nula. Se as m colunas suprimidas têm pelo menos uma linha com δ símbolos diferentes de zero e todas as outras contêm δ ou menos símbolos diferentes de zero, então o novo código gerado tem pelo menos uma linha que contém uma quantidade de símbolos diferentes de zero igual a $(q - 1)\, q^{k-1} - \delta$ e nenhuma outra linha, exceto a linha nula, tem peso menor. Por outro lado, removendo-se um arranjo

com parâmetros (m, k, δ) de um código (n, k, d) de seqüência-m, um novo código com parâmetros (n_1, k, d_1) é produzido. Esse arranjo assim construído tem propriedades opostas àquelas de um código, e por essa razão é chamado de anticódigo. Mais formalmente, um anticódigo AC (m, k, δ) com símbolos em GF(q) é um arranjo de m colunas e $N = q^k$ linhas com a propriedade de que a distância máxima de Hamming entre qualquer par de linhas é menor ou igual a um certo valor δ. O valor δ é chamado a distância máxima do anticódigo. Um anticódigo AC (m, k, δ) suprimido de seu código de seqüência-m, é chamado um anticódigo linear. As q^k linhas do anticódigo são as palavras anticódigo e suas m colunas são as colunas anticódigo. A **Fig. 1** representa de forma simbólica o relacionamento entre código de seqüência-m, código perfurado e anticódigo.

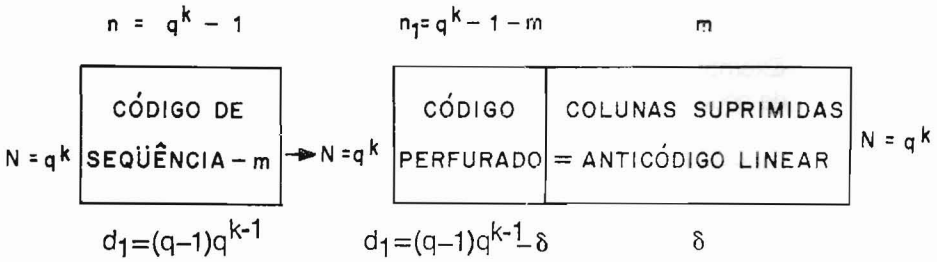


Figura 1. Relacionamento entre código de seqüência-m, código perfurado e anticódigo.

Em geral, um anticódigo pode ser definido como uma matriz com N linhas e m colunas, de elementos de GF(q), cuja distância máxima de Hamming entre qualquer par de linhas é igual a ou menor que um certo valor δ.

Anticódigos lineares com símbolos binários são usados para construir códigos lineares binários. Para gerar um código linear binário com parâmetros (n_1, k, d_1), como mostrado simbolicamente na **Fig. 1**, um anticódigo linear binário (m, k, δ) é removido de seu código de seqüência-m ($2^k - 1$, k, 2^{k-1}), onde $m = 2^k - 1 - n_1$, $\delta = 2^{k-1} - d_1$. Por exemplo, considere o código de seqüência-m (7, 3, 4), cujo dicionário é dado na **Fig. 2.** Os códigos perfurados obtidos são (n_1, k, d_1) = (6, 3, 3), (4, 3, 2) e (3, 3, 1) para os anticódigos (m, k, δ) = (1, 3, 1), (3, 3, 2) e (4, 3, 3), respectivamente.

				4	3		1	m
n			3	4		6	7	
	0	0	0	0	0	0	0	
	0	0	1	1	0	1	1	
	0	1	0	1	1	0	1	
	0	1	1	0	1	1	0	
	1	0	0	1	1	1	0	k=3
	1	0	1	0	1	0	1	
	1	1	0	0	0	1	1	
	1	1	1	1	0	0	0	
d			1	2		3	4	
				3	2		1	δ

Figura 2. Exemplo da obtenção de códigos perfurados a partir de um código de seqüência-m.

4. Distância Máxima de Hamming

A distância máxima de um anticódigo AC é o valor máximo da distância entre qualquer par de palavras anticódigo distintas, isto é,

$$\delta = \max (d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in AC, \mathbf{u} \neq \mathbf{v}) \qquad (1)$$

A diferença módulo-q de duas palavras anticódigo de um anticódigo linear é uma outra palavra anticódigo. Portanto, segue-se que a distância máxima de um anticódigo linear AC sobre GF(q) é igual ao peso da palavra anticódigo de maior peso, isto é.

$$\delta = \max \{ w(\mathbf{u}-\mathbf{v}) : \mathbf{v}, \mathbf{u} \in AC, \mathbf{v} \neq \mathbf{u}\} =$$

$$= \max \{ w(\mathbf{x}) : \mathbf{x} \in AC, \mathbf{x} \neq \mathbf{0} \} \qquad (2)$$

onde w(.) representa o peso da palavra entre parênteses.

Dados os parâmetros m, k de um anticódigo, a distância máxima deve ter o valor menor possível, desde que seu mínimo leva a um valor máximo da distância mínima d_1 do código perfurado. Esta propriedade desejada da distância máxima de um anticódigo é oposta à da distância mínima de um código, onde um valor maior possível deve ser encontrado.

Um anticódigo linear ótimo tem a mínima distância máxima δ para k e m fixados. Então, se um anticódigo AC (m, k, δ) é removido de seu código de seqüência-m (n, k, d) e o código perfurado é ótimo, no sentido de que tem a distância mínima d maior possível para k e n dados, então o anticódigo será ótimo no sentido definido acima.

5. Descrição Matricial de um Anticódigo

5.1. Matriz Geradora de um Anticódigo

Considere uma matriz **G**, k x m, com elementos de GF(q). Se o peso de qualquer das q^k combinações lineares de suas linhas é no máximo δ, então as combinações formam as palavras anticódigo de um anticódigo de comprimento m e distância máxima δ. Se **G** tem posto i, onde $1 \leq i \leq k$, então cada palavra anticódigo ocorre q^{k-i} vezes [**9**].

Exemplo 1

Seja a matriz

$$\mathbf{G}_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Para q = 2 obtém-se o anticódigo

```
0  0  0
0  1  1
1  0  1
1  1  0
---------
1  1  0
1  0  1
0  1  1
0  0  0
```

com m=3, 2^3 palavras anticódigo, $\delta = 2$, e cada palavra anticódigo ocorre duas vezes, isto é, $2^{k-1} = 2$ e, dessa forma, o posto de G_1 e i = 2.

Assim, um anticódigo linear (m, k, δ) pode alternativamente ser descrito por meio de uma matriz geradora **G**, como mostrado acima. Considerando-se a matriz geradora G_b, consistindo do conjunto de vetores linearmente independentes da matriz **G**, isto é, os i vetores linearmente independentes, então G_b produz um anticódigo sem linhas repetidas. Tal anticódigo é chamado de anticódigo linear básico (BAC). Além disso, o espaço linha de G_b é um subespaço de V_m de dimensão i, onde V_m é o espaço vetorial de dimensão m sobre GF(q). A matriz geradora **G** de um anticódigo pode ou não estar na forma escalonada padrão (EP), mas é sempre possível transformá-la para esta forma por apropriadas operações de linha e permutações de coluna [1]. Se o anticódigo tem palavras repetidas, isto é, se i < k, então a matriz geradora EP contém k-1 linhas nulas e uma submatriz identidade ixi.

Exemplo 2

Convertendo G_1 para a forma EP a seguinte matriz é obtida

$$G_2 = \left[\begin{array}{cc:c} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hdashline 0 & 0 & 0 \end{array}\right]$$

Neste caso i=2 e assim uma submatriz identidade 2 x 2 e uma linha nula são obtidas.

A matriz geradora G_b, i x m, de um anticódigo linear básico, consistindo de i vetores linearmente independentes, pode também ser transformada na forma EP e tem uma forma similar àquela da matriz geradora de um código. Assim, G_b na forma EP tem a seguinte forma

$$G_b = \left[\begin{array}{c:c} I_i & B \end{array}\right] \qquad (3)$$

onde I_i é uma matriz identidade i x i e **B** é uma matriz arbitrária i x (m-i).

5.2. Matriz de Paridade de um Anticódigo

Associada à matriz geradora G_b de um BAC (m, i, δ), existe uma matriz H_b com m - i linhas linearmente independentes, onde o espaço linha de H_b é o espaço nulo de G_b, isto é,

$$G_b H_b^T = 0 \qquad (4)$$

onde H_b^T denota a transposta de H_b. A matriz H_b é a matriz de paridade do anticódigo linear básico.

O seguinte teorema descreve a relação existente entre os pesos das palavras de um anticódigo linear básico e sua matriz de paridade.

Teorema 1

Seja BAC (m, i, δ) um anticódigo linear básico sobre GF(q) com matriz de paridade H_b. Então, existe uma palavra anticódigo de peso j se e somente se existe uma combinação linear de j colunas de H_b, que resulta igual a zero.

Prova

(a) Considere a matriz de paridade H_b na seguinte forma

$$H_b = [\, h_1, h_2, \ldots\ldots, h_m \,]$$

onde h_i representa a i-ésima coluna de H_b. Seja **u** uma palavra anticódigo de peso j. Então, desde que **u** é uma palavra anticódigo, obtém-se de (4) que

$$u\ H_b^T = 0$$

Portanto, correspondendo aos j símbolos não nulos de **u**, uma combinação linear dessas j colunas de H_b produz um resultado igual a zero.

(b) Agora, suponha que $h_{e_1}, h_{e_2}, \ldots, h_{e_j}$ são as colunas de H_b para as quais

$$a_1 h_{e_1} + a_2 h_{e_2} + \ldots a_j h_{e_j} = 0 \qquad (5)$$

Então,

$$u H_b^T = 0$$

onde **u** é um vetor de peso j. Assim **u** é uma palavra anticódigo de peso j em AC.

Do teorema acima, obtém-se o seguinte corolário.

Corolário 1

Seja BAC um anticódigo linear básico com matriz de paridade H_b. O peso máximo (ou distância máxima) de BAC é igual ao maior número de colunas de H_b cuja combinação linear é zero.

6. Anticódigos Equivalentes

Considere a matriz geradora de um anticódigo linear AC (m,k,δ). Algumas operações elementares de linha na matriz **G** dão origem a um anticódigo equivalente, isto é, um anticódigo com colunas diferentes daquelas do anticódigo gerado pela matriz **G**, mas com as mesmas palavras anticódigo. O exemplo a seguir mostra que, a partir do anticódigo equivalente AC', é possível produzir um código perfurado equivalente àquele produzido por AC.

Exemplo 3

Considere o anticódigo derivado da matriz geradora **G**:

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

gera o anticódigo AC (3,3,2)

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{matrix}$$

Operações elementares em **G** produzem o seguinte anticódigo equivalente:

$$\mathbf{G} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

gera o anticódigo AC'(3,3,2), equivalente ao AC(3,3,2)

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{matrix}$$

Ambos geram o código perfurado (4,3,2).

Observa-se que permutando colunas da matriz **G** mencionada acima, o mesmo anticódigo é gerado, isto é, as colunas do anticódigo produzido por **G** são as mesmas e, dessa forma, o código perfurado é o mesmo.

7. Anticódigos Duais

A matriz de paridade $\mathbf{H}_b$ de um BAC(m,k,δ) (esta notação implica k=i) consiste de (m-k) linhas linearmente independentes. O espaço linha gerado por $\mathbf{H}_b$ é o anticódigo linear básico (m, m-k, δ). Este anticódigo, denotado por BAC_d, é o espaço nulo de BAC(m,k,δ) e é chamado de anticódigo dual do BAC.

Seja $\mathbf{H}_b$ a matriz de paridade de um BAC (m, k, δ). Decorre do Corolário 1, que $\mathbf{H}_b$ tem a propriedade de que (δ + 1) ou mais de suas colunas não são linearmente dependentes. Desde que $\mathbf{H}_b$ é a matriz geradora (m-k) x m do BAC_d, então pode-se supor, sem perda de generalidade, que a primeira linha de $\mathbf{H}_b$ tem peso δ', o qual é a distância máxima do BAC_d. Se δ' colunas, correspondendo às δ' posições não nulas na primeira linha, bem como a linha nula, são removidas de $\mathbf{H}_b$, o resultado é uma matriz $\mathbf{H'}_b$ (m-k-1)x(m-δ). Essa matriz tem a propriedade de que (δ + 1) ou mais de duas colunas não são linearmente dependentes. Então, $\mathbf{H'}_b$ é a matriz de paridade de um anticódigo básico com parâmetros m-δ', k-δ' + 1 e distância máxima no máximo δ. Isto pode ser resumido por intermédio do teorema que se segue.

Teorema 2

Se δ' é a distância máxima do anticódigo dual BAC_d de um anticódigo básico BAC (m,k,δ), então um anticódigo básico (m-δ', k-δ'+1, $\delta' \leq \delta$) existe.

8. Cotas para os Parâmetros de um Anticódigo

8.1. Cotas de Distância Máxima

Nesta sub-seção, uma cota superior e uma cota inferior para a distância máxima δ de um anticódigo são apresentadas.

8.1.1. Uma Cota Inferior para δ

Uma cota inferior para δ é estabelecida por intermédio do teorema que se segue.

Teorema 3

Se um anticódigo linear básico (m,k,δ) sobre GF(q) com ou sem colunas repetidas existe, então

$$\delta \geq \frac{m\,(q-1)\,q^{k-1}}{q^k - 1} \qquad (6)$$

Prova

A soma dos pesos de todas as palavras anticódigo de um anticódigo linear básico (m,k,δ) é $m(q-1)q^{k-1}$. Desde que existem $q^k - 1$ palavras anticódigo diferentes de zero e o peso máximo é no mínimo igual ao peso médio, então a desigualdade em (6) é obtida.

Esta cota foi apresentada por Farrell [10] e é análoga à cota de Plotkin para a distância mínima de um código [1].

8.1.2. Uma Cota Superior Para δ

Uma cota superior para δ pode ser obtida para anticódigos. A dedução é semelhante àquela da cota inferior de Gilbert-Varsharmov sobre d para códigos [2] e é apresentada aqui sem prova.

Teorema 4

Um anticódigo linear básico (m, k, δ) sobre GF(q) com distância máxima no máximo δ existe, se

$$\sum_{i=\delta+1}^{m-1} C_{m-1}^{i}\,(q-1)^i > q^r - 1 \qquad (7)$$

onde $r = m - k$.

8.2. Uma Cota Superior para o Comprimento de Bloco

A cota apresentada abaixo é análoga à cota de Griesmer para o comprimento de bloco de um código [2].

Teorema 5

O valor máximo de m para o qual é possível obter um anticódigo linear básico (m,k,δ_0) é dado por

$$m \leq \delta_0 + \delta_1 + \delta_2 + \ldots + \delta_i + 1 \qquad (8)$$

onde $\delta_i = \left\lfloor \delta_{i-1}/2 \right\rfloor$ e $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x.

Prova

Se um anticódigo linear básico com parâmetros (m,k,δ_0) existe, então ele terá pelo menos uma palavra com δ_0 símbolos diferentes de zero. Sem perda de generalidade, o anticódigo pode ser rearranjado conforme mostrado na **Fig. 3.**

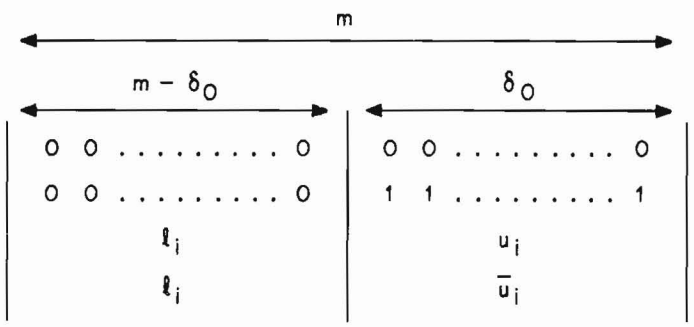


Figura 3. Possível rearranjo de um anticódigo linear básico (m,r,δ_0).

Desde que as primeiras δ_0 colunas (lado direito da **Fig. 3)** formam um grupo, então se algum elemento i deste grupo tem peso u_i seu complemento lógico também está no grupo. Seja o peso máximo da $(m-\delta_0)$-upla mais à esquerda que corresponde a linha i igual a l_i; assim,

$$l_i + u_i \leq \delta_0$$

e

$$l_i + \delta_0 - u_i \leq \delta_0$$

Então,

$$l_i \leq \frac{\delta_0}{2}$$

Dessa forma, as $(m - \delta_0)$ colunas mais à esquerda contêm um anticódigo básico com $m - \delta_0$ colunas e distância máxima no máximo $\delta_1 = \delta_0/2$. Usando este procedimento sucessivamente até $\delta_{i+1} = 1$, um anticódigo com $\delta = 1$ é encontrado e a desigualdade em (**8**) é obtida.

9. Construção de Anticódigos Lineares

Nesta seção, algumas técnicas de construção de anticódigos lineares binários são investigadas.

9.1 Anticódigos de Seqüêencia-m

Existem $2^k - 1$ colunas diferentes que podem ser escolhidas na construção de um anticódigo. Se todas elas são usadas, sem repetição, então anticódigos ótimos com parâmetros $m = 2^k - 1$, $N = 2^k$ e $\delta = 2^{k-1}$ são obtidos. Eles são equidistantes e, dessa forma, satisfazem (**6**) com a igualdade. Esses parâmetros e propriedades são também aqueles dos códigos de seqüência-m. Assim, existem códigos e anticódigos de seqüência-m ótimos para os mesmos parâmetros. Esses anticódigos não têm palavras anticódigo repetidas. Então anticódigos ótimos $(7, k \geq 3, 4)$, $(15, k \geq 4, 8)$, $(31, k \geq 5, 16)$ existem.

Os códigos perfurados obtidos de tais anticódigos (para valores de k maiores que o mínimo indicado) são todos códigos ótimos [**11**]. A **Tabela 1** mostra alguns destes códigos perfurados (para valores de k iguais ao mínimo, os códigos perfurados produzidos são degenerados).

9.2 Empilhamento Simples

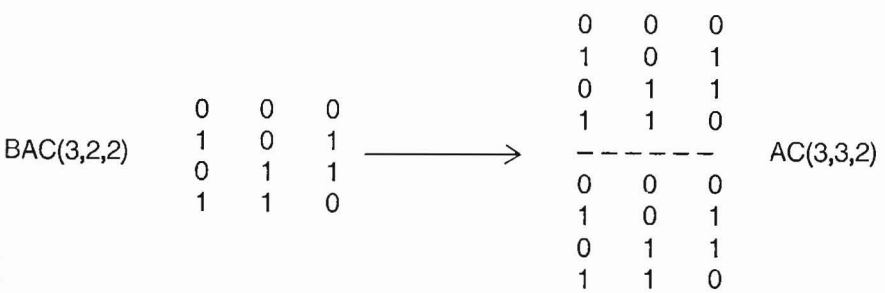
Como foi mencionado nas seções anteriores, um anticódigo pode ter linhas repetidas. Então, uma maneira de construir um anticódigo com m colunas e 2^{k+1} palavras é repetir (empilhar) o próprio anticódigo. Esse processo é chamado de empilhamento simples. De fato, o anticódigo pode ser repetido tantas vezes quantas forem requeridas.

ANTICÓDIGOS	SEQÜÊNCIA-m	CÓDIGOS PERFURADOS
m, k, δ	n, k, d	n_1, k, d_1
7, 4, 4	15, 4, 8	8, 4, 4
7, 5, 4	31, 5, 16	24, 5, 12
7, 6, 4	63, 6, 32	56, 6, 28
15, 5, 8	31, 5, 16	16, 5, 8
15, 6, 8	63, 6, 32	48, 6, 24
15, 7, 8	127, 7, 64	112 , 7, 56
31, 6, 16	63, 6, 32	32, 6, 16
31, 7, 16	127, 7, 64	96, 7, 48

Tabela 1. Códigos lineares binários ótimos obtidos a partir de anticódigos ótimos.

Exemplo 4

Considera-se aqui o seguinte empilhamento:



O anticódigo (3,3,2) é um empilhamento simples do anticódigo básico (3,2,2). Como mencionado na Seção 4, um anticódigo (m,k,δ) sem linhas e colunas re-

petidas é chamado um anticódigo básico e é usado como uma unidade para produzir novos anticódigos.

Se um anticódigo básico (m,k,δ) é obtido, então um empilhamento simples desse anticódigo pode ou não ser ótimo. O teorema seguinte relaciona um anticódigo de comprimento ótimo com o processo de empilhamento simples. Um anticódigo (m,k,δ) tem comprimento ótimo se possui o maior valor de m para valores de k e δ dados.

Teorema 6

Seja $BAC(m,k,\delta)$ um anticódigo básico de comprimento ótimo. Suponha que o código perfurado obtido pela supressão de BAC de seu código de seqüência-m $(2^k-1,\ k,\ 2^{k-1})$ satisfaça à cota de Griesmer com igualdade. Então, o anticódigo AC produzido pela repetição de toda palavra anticódigo de BAC é também ótimo.

Prova

Desde que

$$(2^k - 1) - m = \sum_{i=0}^{k-1} \left\lceil \frac{2^{k-1} - \delta}{2^i} \right\rceil$$

por hipótese, e

$$\left\lceil \frac{2^{k-1} - \delta}{2^i} \right\rceil = 2^{k-1} - \left\lfloor \frac{\delta}{2^i} \right\rfloor \quad \text{para } i \leq k-1$$

obtém-se

$$(2^{k+1} - 1) - m = \sum_{i=0}^{k} \left\lceil \frac{2^k - \delta}{2^i} \right\rceil$$

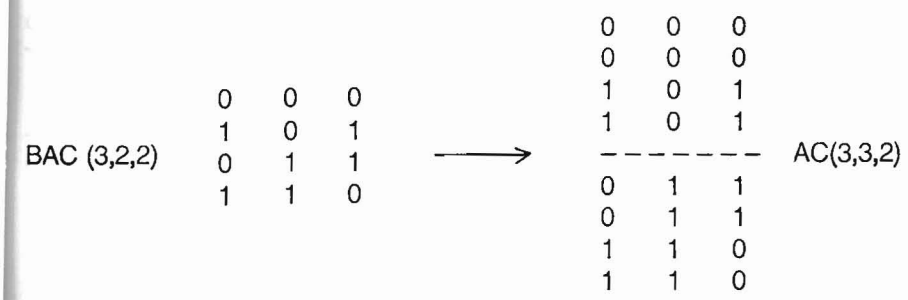
Dessa forma, o novo código perfurado obtido pela supressão de AC do seu código de seqüência-m $(2^{k+1} - 1,\ k + 1,\ 2^k)$ satisfaz a cota de Griesmer com igualdade e então AC é um anticódigo de comprimento ótimo.

9.3 Empilhamento Combinado

Construções alternativas para produzir palavras repetidas podem ser encontradas. O empilhamento mapeado é uma delas. Nesta formação cada palavra do anticódigo original é repetida tantas vezes quantas se desejar.

Exemplo 5

Considera-se neste exemplo o seguinte empilhamento:



Um outro método para se obter um anticódigo com um valor de k maior do que no anticódigo dado consiste em repetir o anticódigo original sobre uma versão invertida dele mesmo (empilhamento invertido). Esses processos, empilhamento simples, de mapeamento e de inversão, podem ser combinados de muitas formas para produzir anticódigos lineares [**12**]. Eles são, é claro, completamente descritos por sua matriz geradora.

Na tentativa de se desenvolver um procedimento alternativo e sistemático para construção de anticódigos ótimos e, conseqüentemente, códigos ótimos, um algoritmo que usa teoria de grafo foi estabelecido em [**9**] e [**13**]. A abordagem de teoria de grafos é um passo na direção de se obter uma solução para o problema de se encontrar um anticódigo linear ótimo sobre um campo de Galois de q elementos.

10. Conclusões

Neste trabalho são discutidos os conceitos fundamentais de anticódigos. Conforme mostrado, anticódigos têm propriedades opostas àquelas de um código. Assim, um anticódigo ótimo tem um valor máximo de m para N e δ dados, ou um valor mínimo de δ para m e N dados. São investigadas cotas sos parâmetros de um anticódigo e observa-se que suas deduções são semelhantes

àquelas correspondentes a códigos. Procedimentos para geração de código corretores de erro, baseados no conceito de anticódigos, são também investigados. Como resulado, diversos códigos com parâmetros ótimos são obtidos, a partir da remoção de um anticódigo de seu código de seqüência-m.

Na tentativa de se obter um procedimento alternativo e sistemático para construção de anticódigos ótimos e, conseqüentemente, códigos ótimos, estudos foram desenvolvidos e um algoritmo que usa teoria de grafos foi estabelecido em [**9**] e [**13**]. Anticódigos com parâmetros ótimos foram obtidos a partir deste algoritmo em [**9**] e [**13**]. Este procedimento sistemático pode ser estendido para anticódigos multi-níveis e uma generalização do mesmo para o caso q-ário vem sendo investigada. Anticódigos multi-níveis são de interesse particular por causa da falta de técnicas de construção sistemática para códigos multi-níveis.

Recentemente, outras técnicas para contrução de anticódigos foram desenvolvidas em [**14**] e [**15**], resultando na obtenção de anticódigos ótimos. Foram também investigadas cotas mais precisas de distância máxima em [**14**] e [**15**]. Estas cotas podem levar a valores mais precisos de distância mínima de códigos, quando comparadas às atuais [**11**].

Agradecimento

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

Referências

[1] W.W. Peterson e E.J. Weldon, Jr., "Error Correcting Codes", MIT Press, 1972.

[2] F. J. MacWilliams e N.J.A. Sloane, "The Theory of Error Correcting Codes", North-Holland, 1986.

[3] S. Lin e D. J. Costello, Jr., "Error Control Coding: Fundamentals and Applications", Prentice Hall, 1983.

[4] R.E. Blahut, "Theory and Practice of Error Control Codes". Addison-Wesley, 1983.

[5] E.R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, 1968.

[6] G. Solomon e J.J. Stiffler, "Punctured Systematic Cyclic Codes", IEEE International Convention Record, vol. 12, 1964, pp. 128-129.

[7] G. Solomon e J.J. Stiffler, "Algebraically Punctured Cyclic Codes", Information and Control, vol. 8, 1965, pp. 170-179.

[8] P.G. Farrel, "Linear Binary Anticodes", Electronics Letters, vol. 6, 1970, pp. 419-421.

[9] M.M. Campello de Souza, "A Graph-Theoretic Approach to Anticodes", Ph. D. Thesis, Electrical Engineering Laboratories, University of Manchester, England, 1983.

[10] P.G. Farrel, "An Introduction to Anticodes", Capítulo 3 em "Algebraic Coding Theory and Applications", G. Longo (editor), Springer-Verlag, 1979.

[11] T. Verhoeff, "An Updated Table for Minimum-Distance Bounds for Binary Linear Codes", IEEE Transactions on Information Theory, vol. IT-33, no. 5, Setembro 1987, pp. 665-680.

[12] P.G. Farrel e A.A.M. Farrag, "Further Properties of Linear Binary Anticodes", Electronics Letters, vol. 10, no. 16, Agosto 1974, pp. 340-341.

[13] M.M. Campello de Souza e R.M. Campello de Souza, "Anticódigos para Construção de Códigos Lineares", Anais do VI Simpósio Brasileiro de Telecomunicações, Campina Grande, Setembro, 1988, pp. 93-95.

[14] V.C. Rocha Jr. e M. M. Campello de Souza, "Construção de Anticódigos e Cotas de Distância Máxima", Anais do VII Simpósio Brasileiro de Telecomunicações, Florianópolis, Setembro 1989, pp. 396-398.

[15] V.C. Rocha Jr. e M.M. Campello de Souza, "Anticode Construction and Bounds on Maximum Distance", IEEE International Symposium on Information Theory, Abstracts of Papers, San Diego, Estados Unidos, 1990, pp. 174.

MARCIA MAHON CAMPELLO DE SOUZA graduou-se pela Universidade Federal de Pernambuco e obteve o título de PhD pela University of Manchester, Manchester, Inglaterra, em 1976 e 1983 respectivamente, ambos em Engenharia Elétrica. De 1978 a 1987 foi Engenheira de Telecomunicações na Empresa Brasileira de Telecomunicações/EMBRATEL. Exerceu a função de Professor Visitante no Departamento de Eletrônica e Sistemas da UFPE e desde 1988, trabalha no mesmo Departamento como Professora

Adjunta. Suas áreas de interesse se concentram em Código Corretores de Erros,Teoria da Informação e Teoria dos Grafos. A Dra. Marcia Mahon é membro do IEEE e da London Mathemati cal Society.