Transformadas em Corpos Finitos Para Codificação de Canal

Ricardo M. Campello de Souza

Este artigo apresenta uma descrição geral da teoria dos códigos de bloco lineares através da transformada de Fourier de corpo finito. Nesta abordagem, não apenas os conceitos fundamentais da área são apresentados em um contexto diferente, como também várias formulações alternativas de famílias importantes de códigos corretores de erro são estabelecidas, o que leva a novas soluções para alguns problemas clássicos em codificação de canal.

1. Introdução

Embora a teoria da codificação de canal tenha percorrido um longo caminho para atingir seu avançado estado de desenvolvimento atual e códigos para controle de erros tenham inúmeras aplicações práticas, alguns problemas importantes (e.g., a determinação da distância mínima dos códigos cíclicos) ainda desafiam os esforços dos pesquisadores da área. Este artigo apresenta uma abordagem do assunto, baseada em transformadas definidas em corpos finitos. Tipicamente, uma transformação é usada como uma ferramenta matemática para modificar um dado problema em outro que possa ser melhor compreendido e resolvido de modo mais eficiente. Neste trabalho, o problema da codificação para controle de erros em sistemas de comunicação digital, é analisado sob o prisma da Transformada de Galois (GFT), uma transformada análoga à de Fourier, porém definida apropriadamente como um mapeamento relacionando vetores com componentes em um corpo finito. Nesse contexto, a teoria básica dos códigos de bloco lineares é vista sob uma nova perspectiva através da qual novas formulações e resultados são obtidos. Nesta abordagem, as questões essenciais da área, a saber, codificação, decodificação e limites de desempenho são beneficiadas e soluções alternativas para muitos problemas, quer de caráter teórico, quer prático, são obtidas.

Na Seção 2, os principais fatos referentes à GFT são estabelecidos de maneira introdutória e servem de referência às demais partes deste artigo. O material apresentado posteriormente está dividido em três partes: (i) descrição da teoria básica dos códigos de bloco lineares via GFT (Seção 3); (ii) descrição de famí-

O autor é Professor do Departamento de Eletrônica e Sistemas da Universidade Federal de Pernambuco, 50741, Recife, PE.

lias importantes de códigos de bloco lineares via GFT (Seção 4); e (iii) decodificação no domínio da transformada (Seção 5). As conclusões relativas ao material discutido são apresentadas na Seção 6.

2. A Transformada de Galois

O uso de transformadas representa uma abordagem matemática que unifica o estudo de vários ramos da Engenharia Elétrica. Transformações lineares, particularmente as de Fourier e Laplace, são fontes bem estabelecidas de técnicas para solução de problemas em sistemas lineares sendo, tradicionalmente, mapeamentos entre corpos infinitos (e.g., R, C). A principal distinção das transformadas consideradas aqui é que as mesmas são mapeamentos entre corpos finitos (campos de Galois). Tais transformadas foram introduzidas inicialmente no contexto de processamento digital de sinais, para implementar algoritmos rápidos para cálculo de convoluções discretas [**1**]-[**6**], tendo sido aplicadas posteriormente na área de codificação de canal, na construção de algoritmos eficientes para codificação e decodificação de várias classes de códigos [**7**]-[**17**]. O estudo da teoria da codificação de canal através da GFT é atualmente um assunto bastante extenso e, embora a aplicação de transformadas definidas em corpos finitos a esta área tenha sido introduzida em 1961 na forma do polinômio de Mattson-Solomon [**18**], esta abordagem somente em 1983 tornou-se parte da literatura estabelecida no assunto [**19**]. A seguir são apresentados alguns conceitos básicos sobre a GFT.

O vetor $\{a_j\}$, formado por n elementos de um corpo GF(q) de característica p, e o vetor $\{A_j\}$, formado por n elementos de $GF(q^m)$, formam um par GFT, aqui denotado por $\{a_j\} \longleftrightarrow \{A_j\}$, se

$$A_j = \sum_{i=0}^{n-1} a_i \alpha^{ji} \qquad (1)$$

e

$$a_j = \frac{1}{n(\text{mod } p)} \sum_{j=0}^{n-1} A_j \alpha^{-ji} \qquad (2)$$

onde α é um elemento de ordem n de $GF(q^m)$. Por analogia com a transformada clássica de Fourier, $\mathbf{a} = \{a_j\}$ é dito ser um vetor no domínio do tempo cujo espectro é $\mathbf{A} = \{A_j\}$. Sem perda de generalidade, será considerado o caso em que α é um elemento primitivo de $GF(q^m)$. A definição do par GFT acima é inteiramente análoga àquela de um par da transformada discreta de Fourier (DFT) [**20**], onde o núcleo de transformação $e^{-j2\pi/n}$ é substituído por α. uma raiz n-ésima da uniade em $GF(q^m)$.

Usando a representação polinomial dos vetores **a** e **A**, isto é,

$$a(x) = \sum_{i=o}^{n-1} a_i x^i$$

e

$$A(z) = \sum_{j=o}^{n-1} A_j z^j$$

é possível estabelecer a seguinte relação entre um polinômio no domínio do tempo e seu espectro [**15**].

Teorema 1

(i) O polinômio no domínio do tempo a(x) tem α^j como uma raiz, em GF(q^m), se é só se $A_j = 0$.
(ii) O polinômio no domínio da freqüência A(z) tem α^{-i} como uma raiz, em GF(q^m), se e só se $a_i = 0$.

A prova deste resultado é imediata e decorre do fato de que

$$\text{(i) } a(\alpha^j) = \sum_{i=o}^{n-1} a_i \alpha^{ji} = A_j$$

$$\text{(ii) } A(\alpha^{-i}) = \sum_{j=o}^{n-1} A_j \alpha^{-ji} = a_i \; n(\text{mod } p)$$

Portanto, observa-se que raízes e coeficientes desempenham papéis semelhantes em cada domínio. Isto mostra que alguns problemas no domínio do tempo tais como, por exemplo, a determinação da distribuição de peso e a questão da decodificação, são traduzidos para o domínio da freqüência como problemas de determinação de raízes de uma certa classe de polinômios A(z) definida sobre GF(q^m). O teorema a seguir elucida uma importante característica destes polinômios [**19**].

Teorema 2

Se $\{a_i\} \longleftrightarrow \{A_j\}$, então, $a_i \in GF(q)$ se e só se

$$A_j^q = A_{((jq))}$$

onde ((x)) denota x(mod n), ou seja, se o polinômio

$$A(z) = \sum_{j=o}^{n-1} A_j z^j$$

operações de soma e multiplicação módulo (z^n-1)).

Deste teorema, decorre que se a componente espectral A_j é especificada, então as componentes cujos índices pertencem à classe de inteiros da forma jq (mod n) são potências de A_j, de modo que apenas um elemento de cada classe precisa ser diretamente calculado via (**1**). Na Seção 4 este fato é usado na construção de códigos cíclicos binários. Neste caso (q = 2), diz-se simplesmente que o espectro A(z) é um idempotente.

A DFT tem muitas propriedades que se aplicam diretamente no caso da GFT. Estas são de especial interesse na análise e projeto de sistemas codificados e desempenham um papel relevante no desenvolvimento da área de códigos corretores de erro sob o prisma do domínio da freqüência. As provas destas propriedades seguem linhas semelhantes àquelas da DFT e não serão apresentadas aqui [**2**]. A seguir é mostrado um exemplo ilustrativo de aplicação dos teoremas 1 e 2.

Exemplo 1

Sejam q = 2, m = 4, n = q^m - 1 = 15 e considere a GFT de GF(2) para GF(16) (operação em GF(16) é módulo o polinômio primtivo $\pi(x) = x^4 + x + 1$). A transformada do vetor binário

a = (1 0 0 0 1 0 0 1 0 0 1 0 1 1 0)

é o vetor de componentes em GF(16)

A = (0 α^6 α^{12} α^8 α^9 0 α α^5 α^3 α^4 0 α^{10} α^2 α^5 α^{10})

onde α é um elemento primitivo de GF(16). Nesse par GFT pode ser verificado pelo cálculo direto que:

(i) 1, α^5 e α^{10} são raízes de a(x) desde que $A_0 = A_5 = A_{10} = 0$;

(ii) α, α^4, α^6, α^7, α^9, α^{10}, α^{12}, α^{13} e α^{14} são raízes de A(z) desde que

$a_1 = a_2 = a_3 = a_5 = a_6 = a_8 = a_9 = a_9\, a_{11} = a_{14} = 0$;

(iii) $A_0^2 = A_0$;

$A_2 = A_1^2$, $A_4 = A_2^2 = A_1^4$, $A_8 = A_4^2 = A_1^8$;

$A_6 = A_3^2$, $A_{12} = A_6^2 = A_3^4$, $A_9 = A_{12}^2 = A_3^8$;

$A_{10} = A_5^2$;

$A_{14} = A_7^2$, $A_{13} = A_{14}^2 = A_7^4$, $A_{11} = A_{13}^2 = A_7^8$.

Observa-se então que apenas as componentes espectrais A_0, A_1, A_3, A_5 e A_7 precisam ser computadas via (**1**). As demais ficam determinadas por (**3**).

3. Códigos de Bloco Lineares

Do Teorema 1 fica claro que a noção de peso de Hamming de um vetor a(x) no domínio do tempo (GF(q)) é traduzida para o domínio da freqüência (GF(q^m)) como o número de elementos distintos $\alpha^i \in GF(q^m)$, que não são raízes do espectro A(z). Portanto um código de bloco linear C(n, k, d) sobre GF(q) pode ser descrito, nesse domínio, como um subespaço de dimensão k de polinômios q-idempotentes sobre GF(q^m), onde $n \mid (q^m - 1)$, tal que nenhum polinômio, excetuando-se o polinômio nulo, tem mais que n-d raízes em GF(q^m). Como a GFT é uma transformação linear, o código é então visto como um subespaço do espaço vetorial de todas as n-uplas de GF(q^m) sobre o corpo GF(q). Nesse contexto, C é denotado por C_T.

Muitas das definições básicas estabelecidas para um código no domínio do tempo têm o mesmo significado no domínio da freqüência, e.g., as noções de dicionário, comprimento e dimensão do código. Além disso, uma descrição matricial é também possível através da matriz $\mathbf{G}_T$, k x n, cuja i-ésima linha é a GFT da i-ésima linha da matriz geradora **G**.

Exemplo 2

As matrizes geradoras **G** e $\mathbf{G}_T$ de um código binário C(7, 3, 4) são mostradas a seguir (operação em GF(8) é módulo o polinômio $p(x) = x^3 + x + 1$):

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \longleftrightarrow \mathbf{G}_T = \begin{bmatrix} 0 & 1 & 1 & \alpha^2 & 1 & \alpha & \alpha \\ 0 & \alpha^3 & \alpha^6 & \alpha^3 & \alpha^5 & \alpha^5 & \alpha^6 \\ 0 & 0 & 0 & \alpha^4 & 0 & \alpha^2 & \alpha \end{bmatrix}$$

As palavras código em ambos os domínios são:

0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	0	1	0	1	1	α^2	1	α	α^4
0	1	0	1	0	1	1	0	α^3	α^6	α^3	α^5	α^5	α^6
0	0	1	0	1	1	1	0	0	0	α^4	0	α^2	α
1	1	0	0	1	1	0	0	α	α^2	α^5	α^4	α^6	α^3
1	0	1	1	0	1	0	0	1	1	α	1	α^4	α^2
0	1	1	1	1	0	0	0	α^3	α^6	α^6	α^5	α^3	α^5
1	1	1	0	0	0	1	0	α	α^2	1	α^4	1	1

(palavras no domínio do tempo) (palavras no domínio da freqüência)

A matriz $\mathbf{G}_T$ pode ter uma coluna com todos os elementos iguais a zero, como é o caso no exemplo acima. Em geral, para códigos cujas palavras têm todas o mesmo peso d, com símbolos em um corpo GF(q), de característica p, a primeira coluna de $\mathbf{G}_T$ é $(x\ x\ x \ldots\ x)^T$, onde $x \equiv d \pmod p$ [**21**].

É possível também definir a matriz $\mathbf{H}_T$, correspondente à matriz de paridade do código. Para cada palavra código $\{a_i\} \in C$ e para cada uma das n-k linhas $\{v_i\}$ da matriz **H** de C, sabe-se que

$$\sum_{i=0}^{n-1} v_i a_i = 0$$

Aplicando-se o teorema do produto [**21**] ao vetor $\{b_i\}$ obtido da multiplicação, componente a componente, dos vetores $\{v_i\}$ e $\{a_i\}$, chega-se a

$$\{b_i\} = \{v_i\} \cdot \{a_i\} \longleftrightarrow \{B_j\} = \frac{1}{n(\text{mod } p)} \{V_j\} * \{A_j\}$$

onde * denota convolução cíclica. Usando-se o teorema de Parseval, (**4**) torna-se

$$\sum_{l=0}^{n-1} V_l A_{n-1} = 0 \qquad (5)$$

e as componentes do espectro código $\{A_j\}$ satisfazem um conjunto de n-k equações independentes, que são as equações de paridade em $GF(q^m)$. Além disso, as linhas $\{V_j\}$ formam a matriz $\mathbf{H}_T$ [**21**].

O teorema de Parseval pode também ser aplicado para caracterizar a condição de dualidade entre dois códigos. É sabido que C e C_d são códigos duais se e só se, para quaisquer palavras código $\{a_i\} \in C$ e $\{b_i\} \in C_d$, é verdadeira a relação.

$$\sum_{i=0}^{n-1} a_i b_i = 0$$

No domínio da GFT isto é equivalente a

$$\sum_{j=0}^{n-1} A_j B_{n-j} = 0$$

que é a condição de dualidade em $GF(q^m)$. Se $C \equiv C_d$, então o código é dito ser autodual e, para qualquer $\{a_i\} \in C$, tem-se

$$\sum_{j=0}^{n-1} A_j A_{n-j} = 0$$

Como n é par para tais códigos, deve-se ter necessariamente, neste caso, $A_o = 0$ para corpos de características $p = 2$ [**21**].

Como foi mencionado anteriormente, o problema de se encontrar o peso de uma palavra código a(x) requer a determinação do número de elementos distintos $\alpha^l \in GF(q^m)$, para os quais o espectro correspondente A(z) satisfaz $A(\alpha^l) \neq 0$. Assim, se n_r denota o número de raízes distintas de A(z), em $GF(q^m)$, para se achar a distância mínima d do código, é preciso encontrar o espectro não nulo com o número máximo N_r de raízes distintas. Isto é

$$N_r = \underset{A(z) \in C}{MAX} \; n_r$$

e

$$d = n - N_r$$

Em alguns casos específicos importantes (e. g., códigos BCH, Bose-Chaudhuri-Hocquenghem) esta busca do espectro com N_r raízes distintas pode ser executada de modo eficiente e, de fato, valores novos de d têm sido determinados por este método [**22**].

Com os conceitos apresentados até esse ponto, é possível caracterizar, via GFT, algumas famílias de códigos de bloco simples. Estas famílias representam exemplos de casos em que é possível estabelecer diretamente a estrutura das raízes de A(z).

(i) A(z) Constante

A(z) não tem raízes, ou seja, toda palavra a(x) tem peso n e existem q palavras. São os códigos de repetição C(n, 1, n).

(ii) $A_0 = 0$
Todas as palavras têm peso par e sendo zero uma das raízes de A(z), $N_r = n-2$. São os códigos de um dígito de paridade, C(n, n-1, 2).

(iii) A(z) Envolve Apenas a Classe $C_1 = \{1, p, p^2, ..., p^{m-1}\}$

Nesse caso

$$A(z) = A_1(z) = \sum_{j \epsilon C_1} A_j z^j$$

ou seja,

$$A(z) = T_m(A_j z^j)$$

onde

$$T_m(x) = \sum_{i=0}^{m-1} x^{p^i}$$

é a função traço de $x \epsilon GF(q^m)$ [23]. Como exatamente q^{m-1} elementos de $GF(q^m)$ têm traço nulo, A(z) tem $q^{m-1}-1$ raízes distintas não nulas. Além disso, A_j pode ser qualquer elemento de $GF(q^m)$, de modo que fica caracterizada uma família com parâmetros $n = q^m-1$, $k = m$ e $d = q^m-q^{m-1}$. Percebe-se ainda que, como n_r é o mesmo para qualquer A(z), as palavras código têm todas o mesmo peso. Esta é portanto a família dos códigos simplex (ou de seqüência-m) [23].

4. Códigos Cíclicos

4.1, Introdução

Códigos definidos em função das raízes de um polinômio gerador podem ser descritos, no domínio da freqüência, com o auxílio do Teorema 1. Dessa forma, um código linear C(n, k, d) sobre GF(q) é dito ser cíclico se e só se ele consiste de todas as ênuplas de GF(q) cujas transformadas são nulas em um conjunto

de n-k componentes especificadas através das n-k raízes, em GF(q^m), do polinômio gerador do código. Estas componentes nulas são denominadas freqüências de paridade, sendo determinadas pelo polinômio gerador g(x) do código. Assim considerando, sem perda de generalidade, que g(x) tem n-k raízes distintas em GF(q^m), as freqüências de paridade correspondem àqueles valores de j ($0 \leq j \leq n-1$) satisfazendo $A_j = g(\alpha^j) = 0$ [15].

Exemplo 3

Em GF(8), as raízes de $g(x) = x^3 + x^2 + 1$ são α^2, α^5 e α^6. O código cíclico gerado por g(x) tem o seguinte deicionário (operação em GF(8) é módulo o polinômio primitivo $\pi(x) = x^3 + x + 1$):

a_0	a_1	a_2	a_3	a_4	a_5	a_6
0	0	0	0	0	0	0
1	1	1	0	1	0	0
0	1	1	1	0	1	0
0	0	1	1	1	0	1
1	0	0	1	1	1	0
0	1	0	0	1	1	1
1	0	1	0	0	1	1
1	1	0	1	0	0	1
0	0	0	1	0	1	1
1	0	0	0	1	0	1
1	1	0	0	0	1	0
0	1	1	0	0	0	1
1	0	1	1	0	0	0
0	1	0	1	1	0	0
0	0	1	0	1	1	0
1	1	1	1	1	1	1

(palavras de C)

A_0	A_1	A_2	A_3	A_4	A_5	A_6
0	0	0	0	0	0	0
0	1	1	0	1	0	0
0	α	α^2	0	α^4	0	0
0	α^2	α^4	0	α	0	0
0	α^3	α^6	0	α^5	0	0
0	α^4	α	0	α^2	0	0
0	α^5	α^3	0	α^6	0	0
0	α^6	α^5	0	α^3	0	0
1	1	1	0	1	0	0
1	α	α^2	0	α^4	0	0
1	α^2	α^4	0	α	0	0
1	α^3	α^6	0	α^5	0	0
1	α^4	α	0	α^2	0	0
1	α^5	α^3	0	α^6	0	0
1	α^6	α^5	0	α^3	0	0
1	0	0	0	0	0	0

(palavras de C_T)

As freqüências de paridade são j = 3, 5 e 6 e, em cada espectro, $A_3 = A_5 = A_6 = 0$. Das demais freqüências apenas A_0 e A_1 são independentes, as outras sendo restritas pelo Teorema 2.

A propriedade de que um código cíclico é preservado pela permutação cíclica que mapeia i em (i+1)(mod n) pode ser examinada através da propriedade de deslocamento no tempo da GFT. Assim, se $(a_j) \longleftrightarrow \{A_j\}$, então, para i_0 constante,

$$\{a_{i-i_0}\} \longleftrightarrow \{\alpha^{ji_0} A_j\}$$

Portanto, $\{A_j\} \in C_T \leftrightarrow \{\alpha^j A_j\} \in C_T$ e a multiplicação de a(x) por x (mod x^n-1) corresponde à multiplicação de A_j por α^j (mod z^n-1).

4.2. Códigos BCH

O estudo de códigos corretores de erro no domínio da freqüência é particularmente útil para a importante classe de códigos BCH. Nesse caso, vários resultados podem ser formulados de modo mais simples e procedimentos de decodificação alternativos eficientes podem ser estabelecidos [**19**] e [**21**]. Um exemplo típico é a determinação da chamada cota BCH [**15**], cuja determinação via GFT é mostrada a seguir.

Teorema 3

A distância mínima de um código BCH sobre GF(q) é pelo menos igual à sua distância projetada δ.

Prova

Seja a(x) um polinômio código de peso menor do que δ-1 e sejam $i_1, i_2, ..., i_w$, $w \leq \delta - 1$, as posições de suas componentes não nulas. Associado a a(x), define-se seu polinômio localizador

$$L(z) = \sum_{j=0}^{n-1} L_j z^j = \prod_{l=1}^{w} (1 - \alpha^{i_l} z) \qquad (6)$$

cujas raízes α^{-i_l}, $l = 1, 2, ..., w$, indicam as posições não nulas de a(x). Do Teorema 1 pode-se afirmar que $\{I_j\}$, a transformada inversa de $\{L_j\}$. é zero sempre que $\{a_j\}$ não o é, ou seja, $a_i I_i = 0$, para todo i. Do teorema do produto [**21**], obtém-se

$$\sum_{k=0}^{n-1} L_k A_{j-k} = 0 \qquad (7)$$

Como $L_0 = 1$ e $L_k = 0$ para $k > w$, (7) resulta em

$$A_j = - \sum_{k=1}^{w} L_k A_{j-k} \qquad (8)$$

Esta expressão é a relação de recorrência obtida de um registrador a deslocamento com realimentação linear, com conexões definidas pelos L_k. Como a distância projetada é δ, existem δ-1 componentes consecutivas A_j nulas; usando-as como estado inicial, chega-se a $A_j = 0$ para todo j e a(x) é o polinômio nulo; ou seja, a única palavra do código que possui peso menor do que δ, é a palavra de peso zero.

A técnica empregada na prova do Teorema 3 pode ser aplicada para se explorar a estrutura de peso de outras classes de códigos cíclicos [24]. Além disso, através da GFT é possível uniformizar a dedução de outras cotas baseadas na existência de conjuntos de raízes consecutivas de g(x) [25].

Uma definição alternativa pode ser estabelecida para os códigos BCH de maneira análoga à feita para os códigos cíclicos, isto é, baseada nas raízes do polinômio gerador. Assim, um código BCH com distância projetada δ é o conjunto de todas as ênuplas de $GF(q^m)$ que têm δ-1 componentes consecutivas nulas especificadas e cujas GFTs inversas pertencem a GF(q). Para os códigos Reed-Solomon a restrição sobre a transformada inversa pode ser removida, uma vez que nesse caso tem-se m = 1 e a GFT mapeia GF(q) em GF(q). Ademais, o número de componentes consecutivas nulas é n-k [21].

Além dos códigos considerados aqui, outras famílias importantes de códigos algébricos, tais como os códigos alternantes, podem ser descritos via GFT [21].

5. Decodificação Algébrica

Uma das áreas que mais se beneficia da abordagem apresentada neste trabalho é a da decodificação de códigos cíclicos. Procedimentos alternativos eficientes têm sido propostos para a decodificação de tais códigos, envolvendo não apenas a decodificação algébrica [15], como também decodificação por tabelas de síndrome, por permutação e com decisão suave [26]-[30]. Aqui é considerada apenas a decodificação algébrica de códigos BCH, denominada na literatura decodificação via transformada ("transform decoding").

No que se segue, a(x) denota uma palavra código de um código BCH, com distância projetada $\delta = 2t+1$, transmitida por um canal de comunicação. O polinômio recebido, r(x), representa uma versão, possivelmente corrompida, de a(x) e é dado por r(x) = a(x) + e(x), onde e(x) é a representação polinomial do erro introduzido durante a transmissão. O vetor erro tem peso ν e suas componentes não nulas ocupam as posições $i_1, i_2, ..., i_\nu$. Um decodificador no domínio do tempo (DDT) executa os seguintes passos para decodificar o vetor recebido r(x) [31]:

(i) Cálculo da síndrome de r(x), isto é,

$$S_j = r(\alpha^j) = e(\alpha^j)$$

onde α^j, j = 1, 2, ..., 2t, são as 2t raízes consecutivas do polinômio gerador do código.

(ii) Determinação do polinômio localizador de erros (PLE) L(z), a partir da síndrome.

(iii) Cálculo das raízes de L(z), as quais indicam as posições de r(x) em erro.

(iv) Cálculo da amplitude do erro (para códigos multiníveis).

Da definição da GFT entretanto, é visível que a síndrome é um vetor no domínio da freqüência tendo 2t componentes da GFT E(z) do polinômio erro, isto é,

$$S_j = e(\alpha^j) = E_j \quad , \qquad j = 1, 2, \ldots 2t$$

Portanto, analisar a questão da decodificação sob o ponto de vista da GFT é inteiramente natural e a tarefa do decodificador pode ser considerada como aquela de encontrar o espectro do vetor erro a partir do conhecimento de 2t de suas componentes, sabendo que o q-idempotente E(z) tem pelo menos n-t raízes distintas em $GF(q^m)$. Esta descrição do problema é análoga a uma situação bem conhecida em processamento digital de sinais (o teorema da amostragem) e coloca a questão da decodificação de códigos cíclicos no contexto dessa área [**32**].

Um decodificador no domínio da freqüência (DDF) executa os seguintes passos para decodificar r(x) [**31**]:

(i) Cálculo de 2t componentes consecutivos do espectro do erro através de

$$E_j = r(\alpha^j) \quad , \qquad j = 1, 2, \ldots, 2t$$

(ii) Determinação, de maneira análoga a um DDT, do PLE

$$L(z) = \prod_{k=1}^{\nu} (1 - \alpha^{i_k} z) = \sum_{j=0}^{\nu} L_j z^j$$

onde $L_0=1$ e $\nu \leq t$. L(z) é, de fato, um polinômio definido no domínio da freqüência, construído convenientemente de modo que sua transformada inversa

$\{l_j\}$ é zero sempre que $\{e_j\}$ não o é. Assim, o produto componente a componente dos dois vetores é nulo, ou seja, $\{l_j\}.\{e_j\} = 0$ e assim $\{L_j\} * \{E_j\} = 0$, onde * denota convolução cíclica, e portanto

$$\sum_{k=0}^{n-1} L_k E_{j-k} = 0 \qquad (10)$$

Note-se que (**10**) é a equação chave no domínio da freqüência. Desde que 2t componentes de E_j são conhecidas, (**10**) pode ser usada para se obter ν equações em ν coeficientes desconhecidos L_k (note que $L_k = 0$ para $k > \nu$). Estas equações são lineares e podem ser resolvidas por técnicas de inversão matricial, pelo algoritmo de Euclides ou pelo algoritmo de Berlekamp [**31**].

(iii) Uma vez que L(z) é encontrado, as n-2t componentes por determinar de $\{E_j\}$ podem ser computadas por uma relação recursiva derivada de (**10**). Isolando-se o termo correspondente a $k = 0$ em (**10**), obtém-se

$$E = -\sum_{k=1}^{n-1} L_k E_{j-k} \qquad (11)$$

(iv) Finalmente, é preciso computar a GFT inversa de E(z) e então $a(x) = r(x) - e(x)$ é a palavra transmitida estimada.

A decodificação algébrica, efetuada em qualquer domínio, é a técnica mais eficiente para decodificar os códigos BCH com parâmetros $n \geq 100$ e $t \geq 10$. Sobre a mesma é importante salientar os seguintes pontos, como forma de comparação entre os procedimentos executados nos dois domínios.

a) Ambas as técnicas estão limitadas pela distância projetada δ, isto é, o decodificador é capaz de corrigir até t erros por bloco, onde $\delta = 2t+1$.

b) Embora estas técnicas requeiram essencialmente os mesmos passos, existem dois pontos importantes a destacar. Um DDF não exige a computação da amplitude do erro, necessária em um DDT para códigos multiníveis, tais como os códigos Reed-Solomon. Além disso, o procedimento exaustivo de busca para computar as raízes de L(z) em um DDT, conhecido como busca de Chien, é substituído pela computação de uma GFT inversa em um DDF. Vantagens computacionais podem ser obtidas nesse ponto, pelo emprego de algoritmos rápidos, como a FFT, para o cálculo dessa GFT.

c) O dispositivo que calcula a síndrome é efetivamente um computador de transformadas e portanto pode ser empregado para calcular qualquer outra GFT em um DDF, diminuindo assim o custo total do sistema codificado [**21**].

6. Conclusões

Neste trabalho foi apresentada uma descrição da teoria básica dos códigos de bloco lineares através da transformada de corpo finito (GFT), uma transformada como a de Fourier, porém apropriadamente definida como um mapeamento relacionando vetores de componentes em corpos finitos. Nesta abordagem, os conceitos básicos são introduzidos à luz da GFT e novas formulações e resultados são apresentados. Nesse contexto, a formulação da classe de códigos cíclicos é particularmente atraente, destacando-se em especial a decodificação de tais códigos. Especificamente, a importante questão da decodificação algébrica de códigos BCH é mais adequadamente descrita sob o ponto de vista da GFT. Assim, não apenas a síndrome e o polinômio localizador de erros são entidades pertencentes ao domínio da freqüência, mas também a relação entre estes elementos, que leva à equação fundamental do processo, surge de modo bastante natural se argumentos baseados na GFT são considerados. Esta formulação alternativa é muito útil, tanto prática quanto teoricamente, levando a novas opções para o projetista de sistemas codificados. De fato, várias implementações híbridas têm sido concebidas onde técnicas de ambos os domínios são empregadas [**19**]e[**21**].

Em função do desenvolvimento da descrição freqüencial, a separação existente entre as duas abordagens (tempo e freqüência) tornou-se inteiramente artificial, e a área de codificação de canal pode assim ser colocada no contexto mais amplo de processamento digital de sinais. Dessa forma, o assunto fica ao alcance de uma audiência mais ampla e abrem-se novas e interessantes possibilidades para a análise, síntese e implementação de códigos corretores de erro.

Agradecimentos

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

Referências

[**1**] J.M. Pollard, "The Fast Fourier Transform in a Finite Field", Mathematics of Computation, vol. 25, Abril 1971, pp. 365-374.

[**2**] C.M. Rader, "Discrete Convolutions Via Mersenne Transforms", IEEE Transactions on Circuits, vol. C-21, Dezembro 1972, pp. 1269-1273.

[3] I.S. Reed e T.K. Truong, "The Use of Finite Fields to Compute Convolutions", IEEE Transactions on Information Theory, vol. IT-21, no. 2, Março 1975, pp. 208-213.

[4] R.C. Agarwal e C.S. Burrus, "Number-Theoretic Transforms to Implement Fast Digital Convolution", Proceedings of the IEEE, vol. 63, no. 4, Abril 1975, pp. 550-560.

[5] I.S. Reed e T.K. Truong, "Complex Integer Convolutions Over a Direct Sum of Galois Fields", IEEE Transactions on Information Theory, vol. IT-21, no. 6, Novembro 1975, pp. 657-661.

[6] S.W. Golomb, I.S. Reed e T.K. Truong, "Integer Convolutions Over the Finite Field GF(3.2^n + 1)", SIAM Journal on Applied Mathematics, vol. 32, Março 1977, pp. 356-365.

[7] W.C. Gore, "Transmitting Binary Symbols With Reed-Solomon Codes", Princeton Conference on Information Sciences and Systems Proceedings, 1973, pp. 495-497.

[8] V.B. Afanasyev, "Time Saving Reed-Solomon Coding and Error Detection", IEEE International Symposium on Information Theory, Tallin, USSR, 1973.

[9] A. Michelson, "A New Decoder for the Reed-Solomon Codes Using a Fast Transform Technique", Systems Engineering Technical Memorandum no. 52, Electronic Systems Group, Eastern Division GTE Sylvania, Waltham, Massachusetts, Agosto 1975.

[10] J. Justesen, "On the Complexity of Decoding Reed-Solomon Codes", IEEE Transactions on Information Theory, vol.IT-22, no. 2, Março 1976, pp. 237-238.

[11] H. Murakami, I.S. Reed e L.R. Welch, "A Transform Decoder for Reed-Solomon Codes in Multiple-User Communication Systems", IEEE Transactions on Information Theory, vol. IT-23, no. 6, Novembro 1977, pp. 675-683.

[12] K.Y. Liu, I.S. Reed e T.K. Truong, "High-Radix Transforms for Reed-Solomon Codes Over Fermat Primes", IEEE Transactions on Information Theory, vol. IT-23, no. 6, Novembro 1977, pp. 776-778.

[13] I.S. Reed, R.A. Scholtz, T.K. Truong e L.R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions", IEEE Transactions on Information Theory, vol. IT-24, no. 1, Janeiro 1978, pp. 100-106.

[14] H. Murakami e I.S. Reed, "Multichannel Convolutional Coding Systems Over a Direct Sum of Galois Fields", IEEE Transactions on Information Theory, vol.IT-24, no. 2, Março 1978, pp. 205-212.

[15] R.E. Blahut, "Transform Techniques for Error Control Codes", IBM Journal of Research and Development, vol. 23, Maio 1979, pp. 299-315.

[16] R.L. Miller, T.K. Truong e I.S. Reed, "Fast Algorithm for Encoding the (255, 223) Reed-Solomon Coder Over GF(2^8)", Electronics Letters, vol. 16, Março 1980, pp. 222-223.

[17] I.S. Reed, T.K. Truong, R.L. Miller e J.P. Huang, "Fast Transforms for Decoding Reed-Solomon Codes", IEE Proceedings Part F, vol. 128, no. 1, Fevereiro 1981, pp.9-14.

[18] H.F. Mattson Jr. e G. Solomon, "A New Treatment of Bose-Chaudhuri Codes", SIAM Journal, vol. 9, 1961, pp. 654-669.

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

[20] R.N. Bracewell, "The Fourier Transform and its Applications", McGraw-Hill, 1978.

[21] R.M. Campello de Souza, "Transform Techniques for Channel Coding", PhD Thesis, Electrical Engineering Department, University of Manchester, 1983.

[22] R.M. Campello de Souza, "Cyclotomic Sequences and Cyclic Codes", IEEE International Symposium on Information Theory, Ann Arbor, Estados Unidos, 1986.

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

[24] V.C. Rocha Jr. e R.M. Campello de Souza, "Cyclic Codes for Random or Burst Error-Correction", IEEE International Symposium on Information Theory, St. Jovite, Canadá, 1983.

[25] T. Schaub e J.L. Massey, "Bounds on the Minimum Distance of Cyclic Codes Via Bounds on the Linear Complexity of Sequences", IEEE International Symposium on Information Theory, Ann Arbor, Estados Unidos, 1986.

[26] R.M. Campello de Souza, "Finite Field Transforms and Symmetry Groups", Journal of Discrete Mathematics, vol. 56, Outubro 1985, pp. 111-116.

[27] R.M. Campello de Souza, "Groups, Finite Transforms and the Decoding of Cyclic Codes", IEEE International Symposium on Information Theory, Ann Arbor, Estados Unidos, 1986.

[28] R.M. Campello de Souza, "Finite Transforms and the Decoding of Reed-Solomon Codes", International Symposium on Information and Coding Theory, Campinas, SP, 1987.

[29] V.C. Rocha Jr. e P.G. Farrell, "Algebraic Soft-Decision Techniques for Linear Block Codes", neste número pp.

[30] R.M. Campello de Souza, "A Transform Based Decoding Algorithm for Cyclic Codes Via Non-Preserving Permutations", IEEE International Symposium on Information Theory, San Diego, Estados Unidos, 1990.

[31] G.. Clark, Jr. e J.B. Cain, "Error-Correction Coding for Digital Communications", Plenum Press, 1981.

[32] R.M. Campello de Souza, "Algebraic Decoding and the Sampling Theorem", IEEE International Symposium on Information Theory, Kobe, Japão, 1988.

[33] R.E. Blahut, "Fast Algorithms for Digital Signal Processing", Addison-Wesley, 1985.

RICARDO MENEZES CAMPELLO DE SOUZA formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco em 1974, obteve o título de Mestre em Ciências pela mesma Universidade em 1979 e o título de PhD pela University of Manchester, Inglaterra, em 1983, ambos em Engenharia Elétrica. Desde 1979 é Professor do Departamento de Eletrônica e Sistemas da UFPE onde atualmente ocupa a posição de Chefe do Departamento. Seus interesses de pesquisa incluem teoria da codificação, criptografia e processamento digital de sinais.