Revista de Engenharia e Pesquisa Aplicada, Volume 2, Número 1, 2016

Códigos Corretores de Erros Baseados nas Transformadas Trigonométricas de Corpo Finito

E. W. Almeida
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil

F. Nery,
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil

J. B. Lima
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 – Recife, Brasil

D. C. Cunha
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil

Resumo Neste trabalho, códigos de bloco lineares construídos a partir de transformadas trigonométricas de corpo finito são examinados. A ideia básica consiste em interpretar o cálculo de uma transformada como um produto entre um vetor e uma matriz de transformação específica. Os autovetores da referida matriz são, então, tomados como as palavras do código a ser construído. Os parâmetros do código têm relação com o comprimento da transformada e com as multiplicidades dos *autovalores da respectiva matriz.*

Palavras-Chave: *Códigos de bloco lineare, transformadas trigonométricas de corpo finito, autovalores, autovetores.*

1 Introdução

As transformadas de corpo finito têm desempenhado um importante papel em diversos cenários de aplicação. Em processamento digital de sinais, essas transformadas são utilizadas, por exemplo, no cálculo rápido de convoluções, por permitirem implementações com baixo custo computacional e dispensarem arredondamentos [1], [2], [3], [4]; no contexto de códigos corretores de erros, transformadas de corpo finito são usadas para descrição de códigos no domínio da frequência [5].

A transformada de corpo finito mais conhecida ´e a de Fourier (FFFT, *finite field Fourier transform*), introduzida em 1972 e redefinida em diversos trabalhos posteriores. Além da FFFT, transformadas como a de wavelet e a de Hartley de corpo finito foram definidas. Suas aplicações incluem criptografia, codificação convolucional e sequências para espalhamento espectral [6], [7], [8].

Mais recentemente, foi introduzida a família das transformadas trigonométricas de corpo finito (FFTT, *finite field trigonometric transforms*), que inclui oito transformadas do cosseno (FFCT, *finite field cosine transform*) e oito do seno (FFST, *finite field sine transform*), classificadas conforme crit´erios de simetria específicos utilizados em sua construção [9], [10]. São exemplos de aplicações dessas transformadas a filtragem e a ocultação de informação em imagens digitais, o projeto de esquemas de comunicação multiusuário e a formatação de distribuições de probabilidade sobre os inteiros [11], [12], [13], [14].

Em [15], foram propostos códigos de bloco lineares construídos a partir da transformada do cosseno de corpo finito do tipo 4 par (FFCT-4e). Alguns dos códigos obtidos apresentaram máxima distância mínima, o que estimulou a investigação, no presente trabalho, de códigos com comprimentos maiores, que são mais interessantes do ponto de vista prático, e de códigos construídos a partir de outros tipos de FFTT. Os tópicos estudados são organizados da seguinte forma: na Seção II, são apresentadas as autoestruturas das matrizes de transformação de alguns tipos de FFTT e descritos os passos necessários `a construção de um código de bloco baseado nessas transformadas; na Seção III, são apresentados exemplos e resultados de simulações preliminares realizadas ao longo do período de iniciação científica; na Seção IV, são discutidas as principais conclusões deste trabalho e as perspectivas para trabalhos futuros.

2 Códigos Corretores de Erros Baseados na FFTT

2.1 Autoestrutura das FFTT

De forma geral, o cálculo de uma transformada trigonométrica de corpo finito de um vetor x = (xi), i = 0, . . . ,N−1, com componentes em GF(p), p ≅ 3 (mod4), pode ser escrito como

$$X_k = \sum_{i=0}^{N-1} x_i M_{i,k}. \qquad (1)$$

O vetor X = (Xk), k = 0, . . . ,N − 1, que corresponde à transformada de x, sob determinadas condições, também possui componentes apenas em GF(p); M = (Mi,k), i, k = 0, . . . ,N − 1, corresponde ao núcleo da transformada, que ´e definido em termos de cossenos ou senos de corpo finito, conforme o tipo de transformada sendo implementado. A Equação (1) equivale à equação matricial

$$\mathbf{X} = \mathbf{x} \cdot \mathbf{M}, \qquad (2)$$

em que M é a matriz de transformação da FFTT.

Em trabalhos anteriores, a autoestrutura (autovalores e autovetores) das matrizes de transformação das FFTT foram investigados [10], [13]. Tais estudos foram estimulados, particularmente, por investigações semelhantes, realizadas com matrizes de transformadas discretas como a de Fourier (DFT, *discrete Fourier transform*) e a do cosseno (DCT, *discrete cosine transform*), e que propiciaram a definição de transformadas discretas fracionais e a concepção de esquemas de comunicação multiusuário [16], [17], [18], [19]. Neste trabalho, são consideradas as autoestruturas da FFCT-1e e da FFCT-4e. As matrizes dessas transformadas possuem apenas dois autovalores distintos, {1,−1}, cujas multiplicidades são apresentadas na Tabela I; seus autovetores podem ser construídos por meio de procedimentos sistemáticos.

TABELA I
MULTIPLICIDADES DOS AUTOVALORES DA FFCT-1e E DA FFCT-4e.

N	Mult. de 1	Mult. de -1
ímpar	$\frac{N+1}{2}$	$\frac{N-1}{2}$
par	$\frac{N}{2}$	$\frac{N}{2}$

2.2 Construção de Código nas FFTT

Um vetor x é dito ser um autovetor, com autovalor associado λ, de uma FFTT específica, quando satisfaz X = λ x. Considerando esta condição e utilizando a Equação (2), pode-se realizar o desenvolvimento

$$\mathbf{M} \cdot \mathbf{x} = \lambda \mathbf{x}$$
$$(\mathbf{M} - \lambda \mathbf{I}) \cdot \mathbf{x} = 0,$$

em que I é uma matriz identidade com dimensões iguais às de M. Como resultado, a matriz (M− λ I) desempenha um papel semelhante ao da matriz de verificação de paridade de um código de bloco linear com comprimento n = N e dimensão k, em que n − k = posto(M− λ I); a dimensão do código k é a multiplicidade do autovalor associado λ, já que essa é a dimensão do subespaço gerado pelos autovetores associados a esse autovalor [15], [20].

Diferentes matrizes de transformação M são obtidas conforme o número primo p ≅ 3 (mod 4) escolhido, o comprimento N e outros critérios que precisam ser observados [10]. Para cada matriz M, relacionada a um dos tipos de FFTT considerados neste trabalho, é possível construir dois códigos, selecionando o autovalor _ = 1 ou λ = −1. O escalonamento da matriz (M− λI) produz a matriz de verificação de paridade na forma sistemática H = [In−k|P] e, consequentemente, permite a obtenção da matriz geradora do código G = [−PT |Ik].

3 Exemplos e Resultados de Simulações

A construção dos códigos descritos na Seção II foi realizada em duas etapas. Na primeira delas, utilizou-se o Matlab para (*i*) obter matrizes de transformação da FFCT-1e e da FFCT-4e; (*ii*) gerar as respectivas matrizes na forma (M − _I); e (*iii*) realizar um escalonamento e obter as matrizes H e G na forma sistemática. A seguir, são apresentados dois exemplos de códigos obtidos ao final desta primeira etapa.

Exemplo 1: Neste exemplo, considera-se um código construído a partir de uma FFCT-1e, com N = 9 e λ = 1 (k = 5), em GF(31). As matrizes de verificação de paridade e geradora obtidas são, respectivamente,

$$\mathbf{H}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 15 & 23 & 17 & 28 \\ 0 & 1 & 0 & 0 & 0 & 17 & 16 & 12 & 4 \\ 0 & 0 & 1 & 0 & 0 & 4 & 3 & 19 & 1 \\ 0 & 0 & 0 & 1 & 0 & 19 & 17 & 8 & 12 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 25 & 16 \end{pmatrix}$$

e

$$\mathbf{G}^{(1)} = \begin{pmatrix} 16 & 14 & 27 & 12 & 29 & 1 & 0 & 0 & 0 \\ 8 & 15 & 28 & 14 & 30 & 0 & 1 & 0 & 0 \\ 14 & 19 & 12 & 23 & 6 & 0 & 0 & 1 & 0 \\ 3 & 27 & 30 & 19 & 15 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Exemplo 2: Neste exemplo, considera-se um código construído a partir de uma FFCT-4e, com N = 5 e _ = −1 (k = 2), em GF(79). As matrizes de verificação de paridadee geradora obtidas são, respectivamente

$$\mathbf{H}^{(1)} = \begin{pmatrix} 1 & 0 & 38 & 34 & 33 \\ 0 & 1 & 59 & 33 & 32 \end{pmatrix}$$

e

$$\mathbf{G}^{(1)} = \begin{pmatrix} 41 & 20 & 1 & 0 & 0 \\ 45 & 46 & 0 & 1 & 0 \\ 46 & 47 & 0 & 0 & 1 \end{pmatrix}.$$

Na segunda etapa, elaborou-se um programa, utilizando a linguagem Java, para determinar a distância mínima de alguns dos códigos construídos. Os resultados podem ser observados na Tabela II. Nesta tabela, além do comprimento do código (n = N), do número primo e do tipo de transformada utilizados, são apresentadas as distâncias mínimas obtidas pelo uso dos autovalores _ = 1 e λ = −1, denotadas respectivamente por $d_{(1)}$ e $d_{(-1)}$.

Para as FFCT-4e, a tabela contém alguns valores atualizados, em comparação com aqueles apresentados em [15]. Observa-se que, para essa transformada, obtém-se códigos de máxima distância mínima, isto é, que satisfazem d = n−k+1, para valores de n ≤ 7. Essa característica é importante no que diz respeito `a capacidade de correção de erros do código e representa um dos requisitos para que um código seja MDS (*maximum distance separable*). Considerando os códigos construídos a partir da FFCT-1e, que não haviam sido analisados em trabalhos anteriores, obtêm-se máxima distância mínima para valores de n ≤ 6.

E importante reafirmar que os resultados expostos foram obtidos unicamente a partir de simulações. Realizando o procedimento descrito na Seção II, ´e possível construir códigos com comprimentos maiores e que, talvez, apresentem máxima distância mínima. Entretanto, até o momento, a Tabela II não pode ser expandida em função da ausência

de um método analítico para determinar a distância mínima dos códigos das FFTT e da intensa carga computacional envolvida em simulações para valores de N grandes.

4 Conclusões e Trabalhos Futuros

Neste artigo, foram investigados, pelo uso de simulações computacionais, códigos de bloco lineares não-binários, baseados em alguns tipos de transformadas trigonométricas de corpo finito. Códigos construídos a partir da FFCT-4e foram revisitados e códigos baseados na FFCT-1e foram estudados. Os resultados obtidos impulsionam a continuidade dos estudos, para obtenção dos parâmetros de códigos com comprimentos maiores; também motivam a investigação de códigos relacionados a outras transformadas, como as FFTT do seno e aquelas baseadas em extensões simétricas ímpares, e as transformadas fracionais de corpo finito [10], [12], [21].

Como perspectiva de trabalhos futuros, deve-se estudar algoritmos de decodificação existentes que possam ser aplicados aos códigos construídos e avaliar a possibilidade de conceber algoritmos particularmente voltados `a decodificação de códigos de transformadas. A construção de novas transformadas a partir de códigos de bloco existentes, como o de

TABELA II
PARÂMETROS DE ALGUNS CÓDIGOS BASEADOS NAS FFTT.

N	p	FFCT	$d^{(1)}$	$d^{(-1)}$
3	7	$1e$	2	3
3	47	$4e$	2	3
4	23	$1e$	3	3
4	31	$4e$	3	3
5	7	$1e$	3	2
5	79	$4e$	3	4
6	79	$1e$	4	4
6	47	$4e$	4	4
7	23	$1e$	2	4
7	167	$4e$	4	5
8	127	$4e$	4	4
9	31	$1e$	4	3
9	71	$4e$	3	5
10	79	$4e$	5	5
13	23	$1e$	4	5

Hamming e o de Golay, também deve ser investigada. Neste sentido, pode-se contribuir para o esclarecimento da relação entre os códigos corretores de erros e as transformadas, de modo que vantagens oferecidas por um desses dois campos de estudo possam ser aproveitadas pelo outro.

Referências

[1] D. F. Elliott and K. R. Rao, *Fast Transforms - Algorithms, Analyses and Applications*, Academic Press, 1982.

[2] S. Gudvangen and H. Buskerud, "Practical applications of number theoretic transforms," in *Norwegian Signal Processing Symposium, NORSIG'99*, 1999.

[3] H. Alaedine, E. H. Baghious, G Madre, and G. Burel, "Realization of block robust adaptive filters using generalized sliding Fermat number transform," in *14th European Signal Processing Conference, EUSIPCO'2006*, 2006.

[4] T. Toivonen and J. Heikkil¨a, "Video filtering with Fermat number theoretic transforms using residue number system," *IEEE Transactions on Circuits and Systems for Vide Technology*, vol. 16, no. 1, pp. 92–101, January 2006.

[5] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, 1985.

[6] K. S. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *IEEE Trans. on Signal Processing*, vol. 52, no. 10, pp. 2975–2991, October 2004.

[7] F. Fekri, M. W. Sartipi, R. M. Mersereau, and R. W. Schafer, "Convolutional codes using finite-field wavelets: Time-varying codes and more," *IEEE Trans. on Signal Processing*, vol. 53, no. 5, pp. 1881–1896, Maio 2005.

[8] H. M. de Oliveira and R. M. Campello de Souza, "Orthogonal multilevel spreading sequence design," in *Coding, Communications and Broadcasting*, P. G. Farnell, M. Darnell, and B. Honary, Eds., pp. 291–303. Research Studies Press, Jonh Wiley, Hertfordshire, 1st edition, 2000.

[9] M. M. C. de Souza, H. M. de Oliveira, R. M. Campello de Souza, and M. M. Vasconcelos, "The discrete cosine transform over prime finite fields," in *International Conference on Telecommunications*, J. N. de Souza, P. Dini, and P. Lorenz, Eds., Berlin, 2004, Lecture Notes in Computer Science, pp. 482–487, Springer.

[10] J. B. Lima, *Trigonometria sobre Corpos Finitos: Novas Definições e Cenários de aplicação*, Tese de Doutorado, Universidade Federal de Pernambuco, Setembro 2008.

[11] R. J. S. Cintra, V. S. Dimitrov, H. M. de Oliveira, and R. M. Campello de Souza, "Fragile watermar-

king using finite field trigonometrical transforms," *Signal Processing: Image Communication, Elsevier*, 2009.

[12] J. B. Lima and R. M. Campello de Souza, "New trigonometric transforms over prime finite fields for image filtering," in *Proceedings of the VI International Telecommunications Symposium, ITS'06*, 2006.

[13] J. B. Lima, R. M. Campello de Souza, and D. Panario, "Blind sequence separation based on the eigenstructure of finite field transforms," in *Anais do XXVI Simpósio Brasileiro de Telecomunicações, SBrT'08*, 2008.

[14] J. B. Lima, R. M. Campello de Souza, and H. M. de Oliveira, "Formatação de distribuições de probabilidade sobre os inteiros," in *Anais do XXV Simpósio Brasileiro de Telecomunicações, SBrT'07*, 2007.

[15] E. S. V. Freire, R. M. Campello de Souza, and J. B. Lima, "Códigos corretores de erros baseados na transformada do cosseno de corpos finitos," in *Anais do XXVII Simpósio Brasileiro de Telecomunicações, SBrT'09*, 2009.

[16] J. H. McClellan and T. W. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio and Electroacoustics*, vol. AU-20, no. 1, pp. 66–74, January 1972.

[17] C. Candan, M. Alper Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Prcess.*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[18] S.-C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Transactions on Signal Processing*, vol. 49, no. 6, pp. 1198–1207, June 2001.

[19] R. M. Campello de Souza and H. M. de Oliveira, "Eigensequences for multiuser communication over the real adder channel," in *Proceedings of the VI International Telecommunications Symposium, ITS'06*, 2006.

[20] J. H. McClellan and T. W. Parks, "Eigenvalue and eigenvector decomposition of the discrete fourier transform," *IEEE Trans. on Audio and Electroacoustics*, vol. AU-20, no. 1, pp. 66–74, March 1972.

[21] J. B. Lima and R. M. Campello de Souza, "The finite field fractional Fourier transform," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010, pp. 3670–3673.