Códigos Corretores de Erros Baseados na Transformada do Cosseno de Corpo Finito

E. S. V. Freire, R. M. Campello de Souza e J. B. Lima

***Resumo*— Uma nova família de códigos corretores de erros, criados a partir de transformadas trigonométricas sobre corpos finitos, é apresentada. A matriz de paridade do código, a dimensão e a distância mínima são obtidas a partir da autoestrutura da transformada do cosseno de corpo finito unitária. Observa-se que alguns códigos obtidos são códigos de máxima distância mínima.**

***Palavras-Chave*— Transformadas do cosseno de corpo finito, transformadas trigonométricas, autossequências, códigos de bloco lineares, códigos MDS.**

***Abstract*— A new family of error-correcting codes, created from trigonometric transforms over finite fields, is introduced. The code parity-check matrix, dimension and the minimum distance are obtained from the eigenstructure of the unitary finite field cosine transform. Our results show that some codes constructed are maximum distance separable, MDS codes.**

***Keywords*— Finite field cosine transform, trigonometric transforms, eigensequences, linear block codes.**

I. INTRODUÇÃO

Transformadas em corpos finitos são ferramentas que tem sido muito usadas em áreas como processamento digital de sinais e códigos corretores de erros [1], [2], [3], [4], [5], [6], [7]. Nesse cenário, estão as transformadas trigonométricas sobre corpos finitos (FFTTs, do inglês *finite field trigonometric transforms*), que têm diversas aplicações, como por exemplo, em marca d'água digital, filtragem de imagens e separação de sequências na comunicação multiusuário [8], [9], [10], [11].

Neste artigo, uma das transformadas trigonométricas digitais, a transformada do cosseno de corpo finito (FFCT, *finite field cosine transform*) [12], é usada para a construção de novos códigos de bloco lineares não-binários. Em geral, a FFCT é um mapeamento relacionando vetores do campo de Galois GF(q) com o conjunto de inteiros gaussianos GI$(p) = \{a + bj, a, b \in \text{GF}(p)\}$.

Os códigos apresentados neste artigo são baseados na autoestrutura da FFCT unitária do tipo 4 par, FFCT-4$\mathfrak{p}$ [11]. A definição das autossequências da FFCT-4$\mathfrak{p}$ fornece os elementos necessários para determinar a matriz de paridade, $\mathbf{H}$, do código, a partir da qual os parâmetros do código, n (comprimento do bloco), k (dimensão) e d (distância mínima de Hamming), são obtidos. Um fato interessante de ser observado é que alguns códigos encontrados são códigos de máxima distância mínima (MDS, do inglês *maximum distance separable*).

A existência de transformadas rápidas sobre corpos finitos é um fator decisivo para a implementação desses códigos, podendo facilitar bastante a sua decodificação, como pode ser visto em [13].

O restante deste artigo é organizado da seguinte forma: Na próxima seção, a autoestrutura da FFCT-4$\mathfrak{p}$ unitária é revista. Na Seção III, os códigos baseados na autoestrutura dessas transformadas trigonométricas são apresentados. O comprimento de bloco e a dimensão do código são obtidos. Além disso, alguns valores para a distância mínima são indicados, em que se pode observar, para alguns códigos, a igualdade $d = n - k + 1$. O artigo é finalizado com algumas conclusões na Seção IV.

II. AUTOSSEQUÊNCIAS DA FFCT-4$\mathfrak{p}$ UNITÁRIA

No que segue, a forma unitária da FFCT-4$\mathfrak{p}$ é considerada.

Definição 1: As sequências $\mathbf{x} = (x_0, x_1, \ldots, x_{N-1})$, em que $x_i \in$ GF(p), e $\mathbf{X} = (X_0, X_1, \ldots, X_{N-1})$, em que $X_k \in$ GI(p), formam um par da FFCT-4$\mathfrak{p}$ unitária quando

$$X_k = \sqrt{\frac{2}{N}} (\text{mod } p) \sum_{n=0}^{N-1} x_n \cos_\zeta((k + 1/2)(n + 1/2))$$

e

$$x_n = \sqrt{\frac{2}{N}} (\text{mod } p) \sum_{k=0}^{N-1} X_k \cos_\zeta((k + 1/2)(n + 1/2)),$$

em que $\zeta \in$ GI(p) tem ordem multiplicativa $2N$, e $\cos_\zeta(x)$ é dado por

$$\cos_\zeta(x) = 2^{-1} (\text{mod } p)(\zeta^x + \zeta^{-x}).$$

Na definição acima, $\sqrt{2/N} (\text{mod } p)$ indica a raiz quadrada de 2 vezes o inverso multiplicativo de N módulo p. O par FFCT-4$\mathfrak{p}$ é denotado por $\mathbf{x} \leftrightarrow \mathbf{X}$ ou $\mathbf{X} = \mathbf{FC}_{4\mathfrak{p}} \cdot \mathbf{x}$, em que $\mathbf{FC}_{4\mathfrak{p}}$ é a matriz de transformação.

Neste trabalho, utiliza-se apenas os elementos $\zeta = (a + bj) \in$ GI(p) unimodulares, ou seja, elementos que obedecem à relação $a^2 + b^2 \equiv 1 (\text{mod } p)$. Além disso, vale ressaltar que $j := \sqrt{-1}$ é um resíduo não-quadrático em GF(p). Considerando as restrições mencionadas, pode-se enunciar o lema a seguir [14].

Lema 1: Se $\zeta = (a + bj) \in$ GI(p) é unimodular,
i) $\cos_\zeta(ki) = \Re(\zeta^{ki})$.

E. S. V. Freire e R. M. Campello de Souza, Departamento de Eletrônica e Sistemas, Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, Brasil, E-mails: eduarda_freire@yahoo.com.br, ricardo@ufpe.br.

J. B. Lima, Departamento de Engenharia Elétrica, Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, Brasil, E-mail: juliano.bandeira@upe.poli.br.

ii) a ordem de ζ divide $p+1$.

Assim, se $\zeta \in \mathrm{GI}(p)$ for unimodular, a FFCT-4$\mathfrak{p}$ possuirá apenas componentes "reais", ou seja, pertencentes a $\mathrm{GF}(p)$.

É importante observar que a FFCT-4$\mathfrak{p}$ requer elementos ζ' de ordem multiplicativa $8N$ (devido à presença dos dois termos $1/2$ que indicam a necessidade de se obter a raiz quarta de ζ). Além disso, é necessário que $\sqrt{2/N} (\mathrm{mod}\ p)$ exista.

Definição 2: Uma sequência $\mathbf{x}$ é dita ser uma autossequência da FFCT-4$\mathfrak{p}$, com autovalor associado $\lambda \in \mathrm{GI}(p)$, quando satisfaz $\mathbf{X} = \lambda \mathbf{x}$.

A autoestrutura das FFCT-4$\mathfrak{p}$ está diretamente relacionada com a autoestrutura da transformada de Fourier de corpo finito generalizada (GFFFT, do inglês *generalized finite field Fourier transform*, cuja matriz de transformação é dada por [11]

$$\mathbf{FF}_{2N,G} = (\sqrt{2N})^{-1} \alpha^{(n+\frac{1}{2})(n+\frac{1}{2})},\ n,k = 0,1,\ldots,2N-1,$$

em que α é um elemento com ordem multiplicativa $2N$ em $\mathrm{GF}(p)$ e $p \equiv 3 (\mathrm{mod}\ 4)$.

Lema 2: As seguintes assertivas são válidas:

i) Se $\mathbf{x} = (x_0, \ldots, x_{N-1}, -x_{N-1}, \ldots, -x_0)$ for um autovetor da matriz GFFFT de comprimento $2N$, ou seja, $\mathbf{FF}_{2N,G}\tilde{\mathbf{x}}^T = \lambda \tilde{\mathbf{x}}^T$, $(\lambda = 1, -1)$, então $\tilde{\mathbf{x}} = (x_0, \ldots, x_{N-1})$ é um autovetor da matriz $\mathbf{FC}_{4\mathfrak{p}}$ de ordem N, ou seja, $\mathbf{FC}_{4\mathfrak{p}}\tilde{\mathbf{x}}^T = \lambda \tilde{\mathbf{x}}^T$, $(\lambda = 1, -1)$. Dessa forma, a partir de autovetores da GFFFT, é possível construir autovetores da FFCT-4$\mathfrak{p}$.

ii) Os únicos autovalores da matriz de transformação FFCT-4$\mathfrak{p}$ são 1 e -1.

III. Construção do Código FFCT-4$\mathfrak{p}$

A partir da Definição 1, a matriz $\mathbf{FC}_{4\mathfrak{p}}$ é dada pela Equação (1), em que $\zeta \in \mathrm{GI}(p)$ tem ordem $2N$. Para ζ unimodular, a Equação (1) se reduz à Equação (2).

Se $\mathbf{x} \leftrightarrow \mathbf{X}$ é uma autossequência da transformada linear $\mathbf{FC}_{4\mathfrak{p}}$, então seu espectro satisfaz $(\mathbf{FC}_{4\mathfrak{p}})\mathbf{x} = \lambda \mathbf{x}$, tal que $(\mathbf{FC}_{4\mathfrak{p}} - \lambda \mathbf{I})\mathbf{x} = 0$. Como resultado, a matriz $(\mathbf{FC}_{4\mathfrak{p}} - \lambda \mathbf{I})$ desempenha um papel semelhante ao da matriz de paridade de um código de bloco linear com comprimento $n = N$ e dimensão k, em que $n - k = posto(\mathbf{FC}_{4\mathfrak{p}} - \lambda \mathbf{I})$. No que se segue, a forma escalonada padrão das matrizes de paridade e geradora são usadas, i.e., $\mathbf{H} = [\mathbf{I}_{n-k}|\mathbf{P}]$ e $\mathbf{G} = [-\mathbf{P}^T|\mathbf{I}_k]$. Dois códigos de bloco sobre $\mathrm{GF}(p)$ podem ser gerados, um para cada autovalor λ. Os possíveis valores para p e N são determinados a partir das restrições implícitas na Definição 1, a saber, $\sqrt{2/N} (\mathrm{mod}\ p)$ e a raiz quarta de ζ devem existir. Além disso, utilizaremos apenas ζ tais que suas raízes quartas sejam unimodulares, de forma que os elementos da matriz FFCT-4$\mathfrak{p}$ pertençam sempre a $\mathrm{GF}(p)$. A partir do item (ii) do Lema 1, observa-se também que, para um código de comprimento N, deve-se procurar por um elemento ζ unimodular tal que $2N | p+1$.

Exemplo 1: Construção de códigos de bloco lineares a partir da FFCT-4$\mathfrak{p}$ unitária de comprimento $N = 5$, sobre $\mathrm{GF}(79)$. Considere o elemento $\zeta = 15 + 31j$, que é unimodular e possui ordem $10 = 2N$, sobre $\mathrm{GF}(79)$. A partir da matriz de transformação $\mathbf{FC}_{4\mathfrak{p}}$, obtém-se

$$\mathbf{FC}_{4\mathfrak{p}} - \lambda\mathbf{I} = \begin{pmatrix} 26-\lambda & 65 & 4 & 28 & 15 \\ 65 & 15-\lambda & 75 & 53 & 51 \\ 4 & 75 & 75-\lambda & 4 & 4 \\ 28 & 53 & 4 & 15-\lambda & 14 \\ 15 & 51 & 4 & 14 & 26-\lambda \end{pmatrix}.$$

Após algumas operações elementares de linhas, as matrizes de paridade, na forma escalonada padrão, associadas com os dois autovalores $\lambda = \pm 1$, são, respectivamente

$$\mathbf{H}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 72 & 6 \\ 0 & 1 & 0 & 6 & 74 \\ 0 & 0 & 1 & 52 & 8 \end{pmatrix}$$

e

$$\mathbf{H}^{(-1)} = \begin{pmatrix} 1 & 0 & 71 & 74 & 73 \\ 0 & 1 & 52 & 73 & 72 \end{pmatrix},$$

que geram os seguintes Códigos $\mathbf{FC}_{4\mathfrak{p}}(n,k)$ com matrizes geradoras $\mathbf{G}^{\lambda}$

$$\mathbf{FC}_{4\mathfrak{p}}(5,2), \quad \mathbf{G}_5^{(-1)} = \begin{pmatrix} 1 & 0 & 71 & 74 & 73 \\ 0 & 1 & 52 & 73 & 72 \end{pmatrix}$$

e

$$\mathbf{FC}_{4\mathfrak{p}}(5,2), \quad \mathbf{G}_5^{(-1)} = \begin{pmatrix} 8 & 27 & 1 & 0 & 0 \\ 5 & 6 & 0 & 1 & 0 \\ 6 & 7 & 0 & 0 & 1 \end{pmatrix}.$$

A. Os parâmetros do código

De uma forma mais apropriada, considere o código $\mathbf{FC}_{4\mathfrak{p}}^{\lambda}(n,k,d)$. O comprimento de bloco n do código é a ordem N da matriz FFCT-4$\mathfrak{p}$ unitária. A dimensão do código k é a multiplicidade do autovalor associado λ, já que essa é a dimensão do subespaço gerado pelas autossequências associadas com λ [15]. As multiplicidades dos dois autovalores são mostradas na Tabela I [11]. Devido ao fator $\sqrt{2/N} (\mathrm{mod}\ p)$ na Definição 1, a multiplicidade de λ depende do valor de $\sqrt{2/N} \equiv \pm b (\mathrm{mod}\ p)$ usado. Isso significa que, na Tabela I, as colunas correspondentes aos autovalores 1 e -1 são trocadas, dependendo do valor considerado (b ou ($p-b$)). Pode ser observado também que os códigos baseados na FFCT-4$\mathfrak{p}$, assintoticamente, tem taxa igual a $1/2$.

A Tabela II mostra os valores de n, k e d para alguns códigos baseados na FFCT-4$\mathfrak{p}$. Podemos observar que, para valores de $n \leq 7$, tais códigos são MDS, ou seja, $d_{\min} = n - k + 1$. Para obtenção dos parâmetros dos códigos e de suas matrizes de paridade e geradora, utilizou-se o programa MATLAB, no qual foram implementadas funções para lidar com corpos finitos.

TABELA I

Multiplicidade dos Autovalores da Matriz FFCT-4$\mathfrak{p}$.

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

$$\mathbf{FC}_{4\mathfrak{p}} = \sqrt{\frac{2}{N}}(\text{mod } p) \begin{pmatrix} \cos_\zeta\left(\frac{1}{2}\cdot\frac{1}{2}\right) & \cos_\zeta\left(\frac{1}{2}\cdot\frac{3}{2}\right) & \dots & \cos_\zeta\left(\frac{1}{2}\cdot\frac{2N-1}{2}\right) \\ \cos_\zeta\left(\frac{3}{2}\cdot\frac{1}{2}\right) & \cos_\zeta\left(\frac{3}{2}\cdot\frac{3}{2}\right) & \dots & \cos_\zeta\left(\frac{3}{2}\cdot\frac{2N-1}{2}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \cos_\zeta\left(\frac{2N-1}{2}\cdot\frac{1}{2}\right) & \cos_\zeta\left(\frac{2N-1}{2}\cdot\frac{3}{2}\right) & \dots & \cos_\zeta\left(\frac{2N-1}{2}\cdot\frac{2N-1}{2}\right) \end{pmatrix} \quad (1)$$

$$\mathbf{FC}_{4\mathfrak{p}} = \sqrt{\frac{2}{N}}(\text{mod } p) \begin{pmatrix} \Re\left(\zeta^{\frac{1}{2}\cdot\frac{1}{2}}\right) & \Re\left(\zeta^{\frac{1}{2}\cdot\frac{3}{2}}\right) & \dots & \Re\left(\zeta^{\frac{1}{2}\cdot\frac{2N-1}{2}}\right) \\ \Re\left(\zeta^{\frac{3}{2}\cdot\frac{1}{2}}\right) & \Re\left(\zeta^{\frac{3}{2}\cdot\frac{3}{2}}\right) & \dots & \Re\left(\zeta^{\frac{3}{2}\cdot\frac{2N-1}{2}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Re\left(\zeta^{\frac{2N-1}{2}\cdot\frac{1}{2}}\right) & \Re\left(\zeta^{\frac{2N-1}{2}\cdot\frac{3}{2}}\right) & \dots & \Re\left(\zeta^{\frac{2N-1}{2}\cdot\frac{2N-1}{2}}\right) \end{pmatrix} \quad (2)$$

TABELA II
PARÂMETROS DE ALGUNS CÓDIGOS BASEADOS NA FFCT-4$\mathfrak{p}$: $(N, p, \zeta, k^\lambda, d^\lambda)$ PARA $\lambda \equiv \pm 1(\text{mod } p)$.

N	p	ζ	k^{+1}	d^{+1}	k^{-1}	d^{-1}
3	47	$24+41j$	2	2	1	3
4	31	$4+27j$	2	3	2	3
5	79	$15+31j$	2	4	3	3
6	47	$6+23j$	3	4	3	4
7	167	$74+161j$	3	5	4	4
8	127	$21+103j$	4	4	4	4
9	71	$8+24j$	4	5	5	3
10	79	$18+25j$	5	5	5	5

IV. CONCLUSÕES

Nesse artigo uma nova família de códigos de bloco lineares não-binários, baseados nas transformadas do cosseno de corpo finito, tipo 4 par, unitárias, foi apresentada. As palavras-código de tais códigos $\mathbf{FC}^{\lambda}_{4\mathfrak{p}}(n,k,d)$ são as autossequências da transformada mencionada, associadas a um dado autovalor λ. A proposta descrita nesse artigo pode ser estendida para outras famílias de transformadas em corpos finitos, tais como a transformada numérica de Hartley [16], e outras transformadas trigonométricas [11]. Essas novas famílias de códigos podem ser construídas seguindo a mesma abordagem apresentada aqui e são membros de uma nova classe de códigos lineares multiníveis, que pode ser denominada de códigos de transformada. Para uma dada transformada em corpo finito de comprimento N, sua autoestrutura pode ser usada para construir um código de comprimento N e dimensão k, em que k é a multiplicidade dos autovalores da transformada. Diferentes multiplicidades irão gerar códigos com diferentes taxas. Nesse cenário, transformadas rápidas e propriedades da autoestrutura da transformada podem auxiliar na implementaçao do código.

Considerando transformadas discretas e utilizando a mesma abordagem empregada neste trabalho, códigos definidos sobre o corpo dos números reais também podem ser construídos.

As restrições dos parâmetros do código que resultam do uso de transformadas padrões, tanto sobre os corpos finitos como infinitos, podem ser removidas se transformadas lineares arbitrárias forem consideradas. Nesse caso, códigos com taxas sem restrições podem ser construídos.

REFERÊNCIAS

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

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

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

[4] 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.

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

[6] H. Tamori, N. Aoki, and T. Yamamoto, "A fragile digital watermarking technique by number theoretic transform," *IEICE Trans. Fundamentals*, vol. E85-A, no. 8, pp. 1902–1904, August 2002.

[7] G. Jerônimo da Silva Jr. and R. M. Campello de Souza, "Design method for two-channel cyclic filter banks over fields of characteristic two," *Electronics Letters*, vol. 45, no. 6, pp. 331–334, March 2009.

[8] R. J. S. Cintra, V. S. Dimitrov, H. M. de Oliveira, and R. M. Campello de Souza, "Fragile watermarking using finite field trigonometrical transforms," *Signal Processing: Image Communication, Elsevier*, 2009.

[9] 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.

[10] 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.

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

[12] 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.

[13] R. M. Campello de Souza, E. S. V. Freire, and H. M. de Oliveira, "Fourier codes," in *Tenth International Symposium on Communication Theory and Applications, ISCTA '09*, 2009.

[14] D. Silva, R. M. de Campello de Souza, H. M. de Oliveira, L. B. Espínola, and M. M. C. de Souza, "A transformada numérica de Hartley e grupos de inteiros gaussianos," *Revista da Sociedade Brasileira de Telecomunicações*, vol. 17, no. 1, pp. 48–57, Junho 2002.

[15] 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.

[16] R. M. Campello de Souza, H. M. de Oliveira, L. B. Espínola Palma, and M. M. Campello de Souza, "Hartley number theoretic transforms," in *Proc. IEEE Int. Symp. Information Theory*, Washington, DC, 2001, p. 210.