A Transformada Discreta do Cosseno em um Corpo Finito

M.M. Campello de Souza, H.M. de Oliveira, R.M Campello de Souza, M. Müller Vasconcelos

Resumo - Uma nova transformada digital, a transformada discreta do cosseno sobre um corpo finito (a TDCCF) é introduzida. O núcleo da TDCCF é a função trigonométrica cosseno definida sobre um corpo finito (k-cossenos). Relações entre os k-cossenos são estabelecidas, através das quais uma fórmula de inversão para a transformada é encontrada.

***Palavras-Chave*—Transformadas digitais, corpos finitos, transformada discreta do cosseno.**

Abstract - A new digital transform, the discrete cosine transform in a finite field (FFDCT) is introduced. The kernel of the FFDCT is the trigonometric function cosine defined over a finite field (k-cosines). A new property of such functions is established, through wich na inversion formula for the FFDCT is derived.

***Index Terms*—Digital transforms, finite fields, discrete cosine transform.**

I. INTRODUÇÃO

As muitas aplicações de transformadas discretas sobre corpos finitos e infinitos são bem conhecidas. A transformada discreta de Fourier (TDF) tem desempenhado um papel importante em Engenharia Elétrica. Uma outra transformada discreta importante é a transformada discreta do cosseno (TDC), a qual tornou-se a ferramenta padrão usada para compressão de imagens. Sistemas de codificação por transformadas [1], normalmente usam transformadas tais como Walsh-Hadamard (WHT), Karhunen-Loève (KLT) e a TDC. Embora discretizadas no domínio da variável independente, estas transformadas tem coeficientes que pertencem a um corpo infinito. Portanto, elas podem ser vistas como um tipo de "transformadas analógicas". Em contraste, as transformadas definidas sobre corpos finitos, além de discretizadas no domínio da variável independente, tem seus coeficientes definidos sobre um alfabeto finito e podem ser vistas como "transformadas digitais".

A análise de Fourier pode ser aplicada para analisar sinais sobre corpos finitos, por meio da transformada de Fourier de corpo finito (TFCF), introduzida por Pollard em 1971 [2] e aplicada para computar convoluções discretas usando aritmética modular. Desde então várias aplicações da TFCF foram encontradas, em diversas áreas, tais como Processamento Digital de Sinais e Imagem, Codificação de Canal e Criptografia [3-5]. Uma versão de corpo finito da transformada discreta de Hartley, a transformada de Hartley de corpo finito (THCF), foi introduzida recentemente por Campello de Souza et al. [6]. Aplicações da THCF incluem o projeto de sistemas de multiplexação digital, de sistemas de acesso múltiplo e de seqüências multiníveis para espalhamento espectral [7-9]. A TFCF e a THCF são exemplos de transformadas digitais.

Nesse trabalho, uma nova transformada digital, a transformada discreta do cosseno em um corpo finito (TDCCF) é introduzida. Uma trigonometria para corpos finitos foi proposta recentemente por Campello de Souza *et al.* [6], a partir de onde a função trigonométrica cosseno é extraída e usada para construir a TDCCF. Na seção 2 alguns preliminares matemáticos são apresentados, que incluem a função cosseno e a construção de números complexos em um corpo finito. Uma nova propriedade dessas funções é introduzida, a qual leva à definição da TDCCF na seção 3. A existência da TDCCF inversa é demonstrada e alguns exemplos são apresentados. A seção 4 contém as conclusões do trabalho.

Os autores são do CODEC - Grupo de Pesquisas em Comunicações, Departamento de Eletrônica e Sistemas - CTG - UFPE, C.P. 7800, 50711 - 970, Recife - PE, Brasil. E-mail: (ricardo, hmo, marciam)@ufpe.br, fuzz@terra.com.br.

II. PRELIMINARES MATEMÁTICOS

II.1 O Corpo Finito dos Números Complexos

Definição 1: GI(p) := {$a + jb$, $a, b \in$ GF(p)}, p um primo ímpar tal que $j^2 \equiv -1 \pmod{p}$ não é um resíduo quadrático em GF(p) (i.e., $p \equiv 3$ (*mod* 4), os chamados primos de Hartley), é o conjunto dos inteiros gaussianos sobre GF(p) ❑

O corpo de extensão GF(p^2) é isomórfico à estrutura "complexa" GI(p), os inteiros gaussianos sobre GF(p) [10]. Da definição acima, todo elemento de GI(p) pode ser representado na forma $a + jb$ e é denominado número complexo de corpo finito.

Definição 2: O módulo de um elemento de GF(p), p=4k+3, é dado por

$$|a| = \begin{cases} a, & se \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ -a, & se \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \end{cases}$$

Proposição 1: O módulo de um elemento de GF(p) é sempre um resíduo quadrático módulo p [11]. ❑

Definição 3: O módulo de um elemento $\zeta = (a+jb) \in GI(p)$, onde $p=4k+3$, é definido por $|a+jb| = \left|\sqrt{|a^2+b^2|}\right|$. ❑

O módulo de ζ é sempre um resíduo quadrático módulo p.

Definição 4: O conjunto unimodular de GI(p) é o conjunto de elementos $\zeta = (a+jb) \in GI(p)$, tais que $a^2+b^2 \equiv 1 \pmod p$. Os elementos ζ são denominados elementos unimodulares. ❑

Esse conjunto é um grupo cíclico de ordem $p+1$ [11]. É possível estender o grupo unimodular de GI(p) anexando elementos complexos $(a+jb)$ que satisfazem $a^2 + b^2 \equiv -1 \pmod p$.

Definição 5: O conjunto negaunimodular de GI(p) é o conjunto de elementos $\zeta = (a+jb) \in GI(p)$, tais que $a^2+b^2 \equiv -1 \pmod p$. Os elementos ζ são denominados elementos negaunimodulares. ❑

Definição 6: O conjunto supraunimodular de GI(p) é o conjunto de elementos $\zeta = a + jb \in GI(p)$ tais que $(a^2 + b^2)^2 \equiv 1 \pmod p$. ❑

Esse conjunto é um grupo cíclico de ordem $2(p+1)$ e todos os seus elementos tem módulo igual a um [11]. Alguns arquivos Matlab® .m para lidar com elementos unimodulares e negaunimodulares, podem ser encontrados na URL http://www.ee.ufpe.br/codec/Fftools.html (tabela 1).

Tabela 1 - Rotinas Matlab® disponíveis para examinar grupos especiais de inteiros gaussianos sobre o corpo finito GF(p).

Arquivo .m	I. FINALIDADE
Unimod(p)	Lista os $p+1$ elementos unimodulares de GI(p)
Negaunimod(p)	Lista os $2(p+1)$ elementos supraunimodulares de GI(p)
Unigen(p)	Encontra um gerador do grupo unimodular de GI(p)
Negagen(p)	Encontra um gerador do grupo supraunimodular de GI(p)

II.2 Trigonometria em Corpos Finitos

Esta sessão introduz algumas funções trigonométricas sobre corpos finitos, as quais tem propriedades semelhantes àquelas das funções trigonométricas usuais definidas sobre os reais [12].

Definição 7. Seja ζ um elemento não nulo de GI(p), onde p é um primo de Hartley. As funções k-trigonométricas (k-*cos* e k-*sen*) de $\angle(\zeta^i)$ (o arco do elemento ζ^i) sobre GI(p), são

$$\cos_k(\angle\zeta^i) = \tfrac{1}{2}(\zeta^{ki} + \zeta^{-ki})$$

e

$$\mathrm{sen}_k(\angle\zeta^i) = \tfrac{1}{2j}(\zeta^{ki} - \zeta^{-ki}),$$

onde ζ tem ordem N, $N \mid (p^2-1)$ e $i,k = 0, 1, \ldots, N-1$. ❑

Numa notação mais simples, considerando ζ fixo, escreve-se $cos_k(i)$ e $sen_k(i)$ para representar as funções k-trigonométricas. Essas definições fazem sentido apenas se GI(p) é um corpo, razão porque p precisa ser um primo de Hartley. Uma dificuldade para se definir uma TDC com a função k-cos como núcleo, está no fato de que essas funções são apenas *quase ortogonais*, como indicado na proposição 2 a seguir [12].

Proposição 2: Se $\zeta \in GF(p)$ tem ordem multiplicativa N, então

$$\sum_{k=0}^{N-1} \cos_k(r)\cos_k(s) = \begin{cases} N, & \text{se } r \equiv \pm s \pmod p \\ 0, & \text{caso contrário} \end{cases}$$

❑

Portanto as funções k-cos não podem ser usadas diretamente para definir uma TDC sobre um corpo finito. De fato, a TDC usual (sobre os reais) na sua forma mais comumente utilizada, é construída por um processo que envolve a duplicação da seqüência x[n] de comprimento N, cuja TDC se quer definir, seguida pela computação da transformada discreta de Fourier (TDF) dessa seqüência de comprimento $2N$, o que requer que se use um núcleo de ordem $2N$. A TDC é então obtida a partir dessa TDF, resultando no par (existem outros pares TDC semelhantes, sendo na verdade possível definir 8 versões da mesma, em função de como se constrói uma extensão periódica *suave* da seqüência $x[n]$. A exigência de *suavidade* está relacionada com as propriedadees de compactação de energia da TDC [13]):

$$C[k] := \sum_{n=0}^{N-1} x[n]\cos\left(\frac{(2n+1)k\pi}{2N}\right),$$

$$x[n] = \sum_{k=0}^{N-1} \beta[k]C[k]\cos\left(\frac{(2n+1)k\pi}{2N}\right)$$

onde $\beta[k] = \begin{cases} \frac{1}{2}, & \text{se } k = 0 \\ 1, & \text{se } k = 1 \end{cases}$.

Nessa discussão, o ponto chave é que o comprimento da transformada não é igual à ordem de seu núcleo. Seja $f = (f_i)$ um vetor de comprimento N sobre GF(p). Para definir uma transformada discreta do cosseno de comprimento N sobre um corpo finito usando k-cossenos, de forma análoga à definida acima para os reais, o seguinte lema se faz necessário:

Lema 1: Se $\zeta \in GI(p)$ tem ordem multiplicativa $2N$, então

$$A = \sum_{k=1}^{N-1} \cos_k(i) = \begin{cases} N-1, & \text{se } i = 0 \\ -1, & \text{se } i \text{ é par } (\neq 0) \\ 0, & \text{se } i \text{ é ímpar} \end{cases}$$

Prova: Por definição

$$A = \sum_{k=1}^{N-1} \cos_k(i) = \tfrac{1}{2}\sum_{k=1}^{N-1}(\zeta^{ki} + \zeta^{-ki}),$$

de modo que, claramente, $A = N-1$ se $i = 0$. Caso contrário, tem-se

$$A = \tfrac{1}{2}[\frac{\zeta^i(\zeta^{i(N-1)}-1)}{\zeta^i-1} + \frac{\zeta^{-i}(\zeta^{-i(N-1)}-1)}{\zeta^{-i}-1}].$$

Como ζ tem ordem 2*N*, então $\zeta^N = -1$. Multiplicando a segunda parcela por $-\zeta^i$, obtém-se

$$A = \tfrac{1}{2}[\frac{(-1)^i-\zeta^i)}{\zeta^i-1} + \frac{1-(-1)^i\zeta^i}{\zeta^{-i}-1}],$$

de modo que, para *i* par,

$$A = \tfrac{1}{2}[\frac{1-\zeta^i+1-\zeta^i}{\zeta^i-1}] = -1$$

e, para *i* ímpar,

$$A = \tfrac{1}{2}[\frac{-1-\zeta^i+1+\zeta^i}{\zeta^i-1}] = 0.$$

❑

III. A TRANSFORMADA DISCRETA DO COSSENO EM UM CORPO FINITO

Baseado no lema 1, é possível se estabelecer uma nova transformada digital, análoga à transformada discreta do cosseno definida sobre os reais, a chamada transformada discreta do cosseno em um corpo finito (TDCCF), como apresentado na definição 8 a seguir

.

Definição 8: Se $\zeta \in$ GI(*p*) tem ordem multiplicativa 2*N*, então a transformada discreta do cosseno de corpo finito da seqüência de comprimento *N*, $f = (f_i)$, i = 0,1,... *N* -1, de elementos de GF(*p*), é a seqüência $C = (C_k)$, $k = 0,1,...N$ -1, de comprimento *N*, de elementos de GI(*p*) dados por

$$C_k := \sum_{i=0}^{N-1} 2 f_i \cos_k(\tfrac{2i+1}{2}).$$

Exemplo 1: Considerando *p* = 7, o elemento ζ = (2+*j*2) ∈ GI(7) tem ordem *p*+1= 8 e é um elemento gerador do grupo unimodular de GI(7). A TDCCF de comprimento (*p*+1)/2 = 4 da seqüência *f* = (1, 2, 3, 4) é a seqüência *C* = (6, 6*j*, 0, *j*). A matriz de transformação $\{2\cos_k(\frac{2i+1}{2})\}$, *i, k* = 0, 1, 2, 3 é

$$M_{k,i} = \begin{bmatrix} 2 & 2 & 2 & 2 \\ 6j & 4j & 3j & j \\ 4 & 3 & 3 & 4 \\ 4j & j & 6j & 3j \end{bmatrix}.$$

❑

Usando-se o lema 1, a inversa da TDCCF pode ser determinada, como mostrado pelo teorema 1 a seguir.

Teorema 1 (A fórmula de inversão): A transformada discreta do cosseno de corpo finito inversa, da seqüência $C = (C_k)$, $k = 0,1,..N$ -1, de elementos de GI(*p*), é a seqüência $f = (f_i)$, $i = 0,1,..N$ -1, de elementos de GF(*p*), dados por

$$f_i = \tfrac{1}{N}\sum_{k=0}^{N-1} \beta_k C_k \cos_k(\tfrac{2i+1}{2}),$$

onde

$$\beta_k = \begin{cases} 1/2, & \text{se } k = 0 \\ 1, & \text{se } k \neq 0 \end{cases}.$$

Prova: O que se quer é provar que $g_i = f_i$, $i = 0,1,... N$ -1, onde

$$g_i := \tfrac{1}{N}\sum_{k=0}^{N-1} \beta_k C_k \cos_k(\tfrac{2i+1}{2}).$$

Da definição 8, pode-se escrever,

$$g_i = \tfrac{1}{N}\sum_{k=0}^{N-1} \beta_k [\sum_{r=0}^{N-1} 2 f_r \cos_k(\tfrac{2r+1}{2})]\cos_k(\tfrac{2i+1}{2}).$$

Invertendo a ordem dos somatórios,

$$g_i = \tfrac{2}{N}\sum_{r=0}^{N-1} f_r [\sum_{k=0}^{N-1} \beta_k \cos_k(\tfrac{2r+1}{2})\cos_k(\tfrac{2i+1}{2})].$$

Considerando a identidade $\cos_k(a \pm b) = \cos_k(a)\cos_k(b) \mp sen_k(a)\,\mathrm{sen}_k(b)$, obtém-se

$$g_i = \tfrac{2}{N}\sum_{r=0}^{N-1} f_r [\tfrac{1}{2} + \tfrac{1}{2}\sum_{k=1}^{N-1}[\cos_k(r+i+1)] + \tfrac{1}{2}\sum_{k=1}^{N-1}\cos_k(r-i)]].$$

Do lema 1 e observando que (*r*+*i*+1) é par sempre que (*r*-*i*) é ímpar e vice-versa, a expressão acima pode ser avaliada considerando-se três casos:

i) Quando *r*+*i*+1 = 0, ou *r* = -*i* –1, o que implica f_r = 0. Portanto, nesse caso, tem-se g_i = 0.
ii) Quando *r*-*i* = 0, ou *r* = *i*. Portanto, nesse caso, obtém-se

$$g_i = \tfrac{2}{N} f_i [\tfrac{1}{2} + \tfrac{1}{2}(0) + \tfrac{1}{2}(N-1)] = f_i.$$

iii) Quando ambos, *r*+*i*+1 e *r*-*i*, são diferentes de zero. Das paridades dessas expressões, resulta em

$$g_i = \tfrac{2}{N}\sum_{r=0}^{N-1} f_r [\tfrac{1}{2} + \tfrac{1}{2}(0) + \tfrac{1}{2}(-1)] = 0,$$

e, portanto, $g_i = f_i$, $i = 0,1,... N$ -1, e a prova está completa.

❑

Exemplo 2: A matriz de transformação inversa é dada por $\{\frac{\beta_k}{N}\cos_k(\frac{2i+1}{2})\}$, *i, k* = 0, 1, 2, 3. No caso da TDCCF do exemplo 1, a matriz de inversão é

$$M^{-1}{}_{k,i} = \begin{bmatrix} 1 & 6j & 4 & 4j \\ 1 & 4j & 3 & j \\ 1 & 3j & 3 & 6j \\ 1 & j & 4 & 3j \end{bmatrix}.$$

Observe que, devido à forma das expressões das transformadas direta e inversa, dada uma das matrizes da TDCCF, pode-se obter a outra diretamente por inspeção. No caso, tem-se $m^{-1}_{i,k} = \begin{cases} \frac{1}{2} m_{k,i}, & \text{se } k = 0 \\ m_{k,i}, & \text{se } k \neq 0 \end{cases}$. ❑

A TDCCF compreende uma importante subclasse de transformadas de corpo finito, as TDCCF de Mersenne, as quais são definidas sobre GF(p), quando p é um primo de Mersenne, isto é, $p = 2^s$-1. Nesse caso, o comprimento da transformada é $N = 2^{s-2}$, o que a torna uma ferramenta atrativa uma vez que algoritmos rápidos de base 2 podem ser usados na sua computação. A tabela 2 a seguir apresenta valores de parâmetros envolvidos na construção de algumas TDCCF.

Tabela 2 - Parâmetros da Transformada Discreta do Cosseno em alguns corpos finitos: p, comprimento N, elemento unimodular ζ usado na função k- *cos*(.) e sua ordem no campo de extensão GF(p^2).

p	***N***	**ζ**	**Ord(ζ)**
7*	4	2+j2	8
23	12	4+j10	24
31*	16	2+j11	32
47	24	4+j19	48
71	36	8+j24	72
79	40	2+j32	80
103	52	2+j10	103
127*	64	2+j39	128
151	76	2+j65	152
167	84	4+j73	168
191	96	6+j27	192
199	10	2+j14	200

* TDCCF de Mersenne.

Nos exemplos apresentados acima, o vetor transformado tem componentes em GF(p^2). Entretanto, como os elementos da matriz de transformação são obtidos por potências da raíz quadrada de um elemento unimodular, devido ao fator (1/2) na definição da função *k-cos* (razão pela qual a transformada de comprimento N emprega um elemento ζ de ordem $2N$), um tal elemento é sempre *real* ($\in$ GF(p)) ou *imaginário* (da forma jb). Portanto, a complexidade computacional envolvida no cálculo da transformada é essencialmente a mesma de uma transformada que assume valores apenas em GF(p). Entretanto, transformadas *reais* podem ser facilmente construídas, considerando-se a proposição 3 a seguir [14].

Proposição 3: Se $\zeta = a + jb$ é um elemento unimodular, então a função $cos_k(\zeta^i)$ assume valores apenas em GF(p), para quaisquer k, i. ❑

Portanto, se ζ é um elemento unimodular cuja raíz quadrada λ também é unimodular, então a matriz de transformação só terá elementos pertencentes a GF(p) e a TDCCF é real nesse caso. Entretanto, sendo λ um elemento gerador do grupo unimodular, sua ordem é (p+1), de modo que ζ terá ordem (p+1)/2, o que implica em uma TDCCF de comprimento N = (p+1)/4. Os parâmetros para essa transformada são semelhantes aos da tabela 2, porém seus comprimentos valem a metade daqueles indicados.

IV. CONCLUSÕES E SUGESTÕES

Nesse trabalho uma nova transformada digital foi introduzida, a transformada discreta do cosseno sobre GF(p) (a TDCCF), uma versão de corpo finito da bem conhecida transformada discreta do cosseno definida sobre o corpo dos números reais. Inicialmente, foram apresentados alguns fundamentos matemáticos que levam à construção de números *complexos* e das chamadas funções k-trigonométricas sobre um corpo finito. A função *k-cos* foi então usada como núcleo na definição da TDCCF, tendo sido apresentada a fórmula de inversão da transformada. A TDCCF apresenta comprimentos divisores de (p+1), onde p é um primo de Hartley, sendo possível a construção da TDCCF de Mersenne, que apresenta comprimentos do tipo potência de 2.

Considerando a existência de definições alternativas para a TDC usual, versões de corpo finito dessas alternativas devem ser investigadas. Além disso, versões digitais de outras transformadas discretas, tais como a transformada discreta do seno, precisam ser concebidas.

REFERÊNCIAS

[1] Transform Coding: Past, Present and Future, *IEEE Signal Processing Magazine Special Issue*, vol. 18, No. 5, Sep. 2001.

[2] J. M. Pollard, The Fast Fourier Transform in a Finite Field, *Math. Comput.*, vol. 25, No. 114, pp. 365-374, Apr. 1971.

[3] I. S. Reed, T. K. Truong, V. S. Kwoh and E. L. Hall, Image Processing by Transforms over a Finite Field, *IEEE Trans. Comput.*, vol.C-26, pp. 874-881, Sep. 1977.

[4] R. E. Blahut, Transform Techniques for Error-Control Codes, *IBM J. Res. Dev.*, vol. 23, pp. 299-315, May 1979.

[5] J. L. Massey, The Discrete Fourier Transform in Coding and Cryptography, 1998 IEEE Information Theory Workshop, ITW 98, San Diego, CA, Feb 9-11.

[6] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, Trigonometry in Finite Fields and a New Hartley Transform, *Proceedings of the 1998 IEEE International Symposium on Information Theory*, p. 293, Cambridge, MA, Aug. 1998.

[7] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, Efficient Multiplex for Band-Limited Channels, *Proceedings of the Workshop on Coding and Cryptography - WCC '99*, pp. 235 - 241, Paris, Jan. 1999.

[8] J. P. C. L. Miranda, H. M. de Oliveira, On Galois-Division Multiple Access Systems: Figures of Merit and Performance Evaluation,. *Anais do 19º Simpósio Brasileiro de Telecomunicações*, Fortaleza CE, 2001.

[9] H. M. de Oliveira, R. M. Campello de Souza, Orthogonal Multilevel Spreading Sequence Design, in *Coding, Communications and Broadcasting*, pp. 291-303, Eds. P. Farrell, M. Darnell and B. Honary, Research Studies Press / John Wiley, 2000.

[10] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison Wesley, 1985.

[11] D. Silva, R. M. Campello de Souza, H. M. de Oliveira, L. B. E. Palma and M.M.Campello de Souza, A Transformada Numérica de Hartley e Grupos de Inteiros Gaussianos, *Revista da Sociedade Brasileira de Telecomunicações*, Campinas, SP, v.17, No.1, pp. 48-57, 2002.

[12] A. N. Kauffman, A Transformada de Hartley em um Corpo Finito e Aplicações, *Dissertação de Mestrado*, Departamento de Eletrônica e Sistemas, UFPE, 1999.

[13] J. S. Lim, *Two-Dimensional Signal and Image Processing*, Prentice-Hall, 1990.

[14] R. M. Campello de Souza, H. M. de Oliveira, L.B. Espínola e M. M. Campello de Souza, Transformadas Numéricas de Hartley, *Anais do XVIII Simpósio Brasileiro de Telecomunicações*, pp. 357 - 366, Gramado, RS, setembro 2000.