A Transformada Discreta do Seno em um Corpo Finito

R. M. Campello de Souza **M. M. Campello de Souza**
H. M. de Oliveira **M. M. Vasconcelos**

Depto de Eletrônica e Sistemas, CTG, UFPE.

50670-901, Recife, PE

E-mails: (ricardo,hmo,marciam)@ufpe.br, mmv@ee.ufpe.br

Resumo

Uma nova transformada, a transformada discreta do seno sobre um corpo finito (TDSCF) é introduzida. O núcleo da TDSCF é a função trigonométrica seno definida sobre um corpo finito. A TDSCF tem comprimentos que são divisores de $(p+1)/2$. Um caso especial é a TDSCF de Mersenne, definida quando p é um primo de Mersenne. Essa classe de TDSCFs tem comprimentos que são potências de 2 e podem ser computadas por algoritmos FFT de base 2.

1 Introdução

Transformadas discretas definidas sobre estruturas finitas ou infinitas tem muitas aplicações em Engenharia. Dentre as várias transformadas discretas definidas sobre os reais ou complexos, a transformada discreta de Fourier (TDF) e as transformadas discretas do cosseno (TDC) e do seno (TDS) tem desempenhado um papel importante em Engenharia Elétrica. A TDC e a TDS tem recebido muita atenção devido ao seu uso em sistemas de codificação por transformadas. Em particular, a DST é o fundamento da técnica de codificação de bloco recursiva e tem sido usada na implementação rápida de transformadas ortogonais para codificação [1, 2]. Embora discretizadas no domínio da variável independente, estas transformadas tem coeficientes que pertencem a um estrutura infinita. Portanto, elas podem ser vistas como um tipo de "transformada analógica". Por outro lado, transformadas definidas sobre estruturas finitas, 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 tratar sinais definidos sobre corpos finitos, por meio da transformada de Fourier de corpo finito (TFCF), introduzida por Pollard e aplicada para computar convoluções discretas usando aritmética modular [3]. Uma versão de corpo finito da transformada discreta de Hartley, a transformada de Hartley de corpo finito (THCF), foi introduzida em [4]. Aplicações da THCF incluem o projeto de sistemas de multiplexação digital, de sistemas de acesso múltiplo e de seqüências multiníveis para espalhamento espectral [5, 6]. Recentemente, a versão de corpo finito da TDC, foi introduzida [8]. Essas transformadas são exemplos de transformadas digitais.

Neste trabalho, uma nova transformada digital, a transformada discreta do seno em um corpo finito (TDSCF), é introduzida. A partir de uma trigonometria para corpos finitos introduzida recentemente [4], a função trigonométrica seno sobre um corpo finito é usada para construir a TDSCF. Na seção 2 alguns fundamentos matemáticos são apresentados, que incluem a função seno e a construção de números complexos em um corpo finito. Uma nova propriedade dessas funções é introduzida, a qual leva à definição da TDSCF na seção 3. A existência da TDSCF inversa é demonstrada e alguns exemplos são apresentados. A seção 4 contém as conclusões do trabalho.

2 Fundamentos Matemáticos

2.1 O Corpo Finito dos Números Complexos

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

Da definição acima, todo elemento de $\mathrm{GI}(p)$ pode ser representado na forma $a+jb$ e é denominado número complexo de corpo finito.

Definição 2 *O conjunto unimodular de* $\mathrm{GI}(p)$ *é o conjunto de elementos* $\zeta = (a+jb) \in \mathrm{GI}(p)$*, 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 $p+1$ [9].

2.2 Trigonometria em Corpos Finitos

Esta seção introduz algumas funções trigonométricas sobre corpos finitos, as quais tem propriedades semelhantes àquelas das funções trigonométricas definidas sobre os reais [10].

Definição 3 *Seja ζ um elemento não nulo de* GI(p), $p \equiv 3 \pmod 4$. *As funções k-trigonométricas* k-cos *e* k-sen *de* $\angle(\zeta^i)$ *(o arco do elemento* ζ^i*) sobre* GI(p)*, são*

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

e

$$\mathrm{sen}_k(\angle\zeta^i) = \frac{1}{j2}(\zeta^{ki} - \zeta^{-ki}),$$

i, $k = 0, 1, ..., N-1$, *onde* ζ *tem ordem* N *e* $N|(p^2-1)$.

Numa notação mais simples, considerando ζ fixo, as funções k-trigonométricas são denotadas por $\cos_k(i)$ e $\mathrm{sen}_k(i)$. A proposição 1, indicada a seguir, decorre diretamente da definição 3.

Proposição 1 *A função* $\mathrm{sen}_k(i)$ *satisfaz:*

i) $\mathrm{sen}_N(\frac{2i+1}{2}) = (-1)^i$.

ii) $\mathrm{sen}_{N-k}(\frac{2i+1}{2}) = \mathrm{sen}_k(\frac{2i+1}{2})$.

A TDS usual é construída por um processo que envolve a duplicação da seqüência $f[n]$ de comprimento N, cuja TDS se quer definir, seguida pela computação da TDF dessa seqüência de comprimento $2N$, o que requer que se use um núcleo de ordem $2N$ [11].

3 A Transformada Discreta do Seno em um Corpo Finito

De forma análoga à transformada discreta do seno definida sobre os reais, a construção da TDSCF $S = (S_k)$ de uma seqüência $f = (f_i)$, $i = 0, ..., N-1$ de elementos de GF(p), faz uso da seqüência auxiliar $g = (g_i)$, $i = 0, ..., 2N-1$, de elementos $g_i \in$ GF(p), definidos por

$$g_i \triangleq f_i - f_{2N-1-i} = \begin{cases} f_i, & 0 \le i \le N-1 \\ -f_{2N-1-i}, & N \le i \le 2N-1 \end{cases}$$

Os coeficientes S_k da TDSCF são obtidos a partir da TFCF $G = (G_k)$ de g, conforme ilustrado a seguir e descrito nesta seção:

$$\begin{array}{ccccccc} {\scriptstyle N} & & {\scriptstyle 2N} & {\scriptstyle TFCF} & {\scriptstyle 2N} & & {\scriptstyle N} \\ (f_i) & \rightarrow & (g_i) & \longleftrightarrow & (G_k) & \rightarrow & (s_k) \end{array}$$

A seqüência g tem comprimento $2N$ e os coeficientes de sua TFCF são [3]:

$$G_k = \sum_{i=0}^{2N-1} g_i\zeta^{ki} = \sum_{i=0}^{N-1} f_i\zeta^{ki} - \sum_{i=N}^{2N-1} f_{2N-1-i}\zeta^{ki}, \quad (1)$$

$0 \le k \le 2N-1$, onde ζ é um elemento de ordem $2N$ de GI(p). Observe que, devido à anti-simetria usada na definição de g, o coeficiente G_o é nulo. Mudando, no segundo somatório, $2N-1-i$ por i, 1 torna-se

$$G_k = \sum_{i=0}^{N-1} f_i\zeta^{ki} - \sum_{i=0}^{N-1} f_i\zeta^{k(-1-i)},$$

ou seja,

$$G_k = \sum_{i=0}^{N-1} f_i[\zeta^{ki} - \zeta^{(-k-ki)}].$$

Evidenciando o termo $\zeta^{-k/2}$, tem-se

$$G_k = \sum_{i=0}^{N-1} f_i\zeta^{-k/2}[\zeta^{k/2}\zeta^{ki} - \zeta^{-k/2}\zeta^{-ki}],$$

ou

$$G_k = \zeta^{-k/2}\sum_{i=0}^{N-1} f_i[\zeta^{k(2i+1)/2} - \zeta^{-k(2i+1)/2}],$$

de modo que, da definição 3,

$$G_k = \zeta^{-k/2}\sum_{i=0}^{N-1} f_i 2j\mathrm{sen}_k[(2i+1)/2], \quad (2)$$

$0 \le k \le 2N-1$. Os N coeficientes S_k da TDSCF são extraídos da seqüência (G_k) de comprimento $2N$ e são definidos por

$$S_k = \begin{cases} -j\zeta^{k/2}G_k, & 1 \le k \le N, \\ 0, & \text{caso contrário} \end{cases}, \quad (3)$$

isto é,

$$S_k = \sum_{i=0}^{N-1} 2f_i\mathrm{sen}_k[(2i+1)/2], 1 \le k \le N. \quad (4)$$

A expressão acima define a TDSCF direta da seqüência f.

.

3.1 A TDSCF Inversa

Para inverter a expressão 4 e obter a TDSCF inversa, faz-se uso do lema 1 a seguir.

Lema 1 *Os coeficientes* G_k *em 2 satisfazem*

i) $G_k = -\zeta^k G_{2N-k}, 0 \le k \le 2N-1$.

ii) $G_k = j\zeta^{-k/2} S_{2N-k}, N \leq k \leq 2N-1$.

Prova:
i) Mudando k por $2N-k$ em 2 e usando a proposição 1 (ii) (note que como ζ tem ordem $2N$, então $\zeta^N = -1$), obtem-se:

$$G_{2N-k} = -\zeta^{k/2} \sum_{i=0}^{N-1} f_i 2j\text{sen}_k[(2i+1)/2].$$

Porém de 2, isso é o mesmo que

$$G_{2N-k} = -\zeta^{-k} G_k$$

e o resultado segue.
ii) Fazendo $2N-k = r$, o intervalo $N \leq k \leq 2N-1$ torna-se $1 \leq r \leq N$ e assim vale a expressão 3, isto é,

$$S_r = -j\zeta^{r/2} G_r,$$

de modo que

$$G_{2N-k} = j\zeta^{-(2N-k)/2} S_{2N-k}.$$

Usando o resultado (i) anterior, pode-se escrever

$$-\zeta^k G_k = -j\zeta^{k/2} S_{2N-k},$$

ou seja,

$$G_k = j\zeta^{-k/2} S_{2N-k},$$

e a prova está completa.

■

De posse do lema 1, é possível expressar f_i em função de S_k e obter a relação que corresponde à TDSCF inversa. Da TFCF inversa de G, tem-se

$$g_i = \frac{1}{2N} \sum_{k=0}^{2N-1} G_k \zeta^{-ki},$$

$0 \leq i \leq 2N-1$, sendo que

$$f_i = \begin{cases} g_i, & 0 \leq i \leq 2N-1 \\ 0, & \text{caso contrário} \end{cases}.$$

Expandindo o somatório acima, pode-se escrever

$$g_i = \frac{1}{2N}\Big[\sum_{k=0}^{N-1} G_k \zeta^{-ki} + \sum_{k=N}^{2N-1} G_k \zeta^{-ki}\Big].$$

Usando 3 e o lema 1, e considerando que $G_0 = 0$, tem-se

$$g_i = \frac{1}{2N}\Big[\sum_{k=1}^{N-1} j\zeta^{-k/2} S_k \zeta^{-ki} + \sum_{k=N}^{2N-1} j\zeta^{-k/2} S_{2N-k} \zeta^{-ki}\Big].$$

Mudando $2N-k$ por k no segundo somatório, leva a

$$g_i = \frac{j}{2N}\Big[\sum_{k=1}^{N-1} S_k \zeta^{-k(2i+1)/2} + \sum_{k=N}^{2N-1} S_k \zeta^{-(2N-k)/2} \zeta^{-(2N-k)i}\Big].$$

isto é,

$$g_i = \frac{j}{2N}\Big[-S_N j(-1)^i + \sum_{k=1}^{N-1} S_k (\zeta^{-k(2i+1)/2} - \zeta^{k(2i+1)/2})\Big].$$

Da definição 3, resulta

$$g_i = \frac{1}{N}\Big[(-1)^i \frac{S_N}{2} + \sum_{k=1}^{N-1} S_k \text{sen}_k\Big(\frac{2i+1}{2}\Big)\Big].$$

e portanto, da proposição 1 (i), os coeficientes f_i da TDSCF inversa de S são dados por

$$f_i = \frac{1}{N} \sum_{k=1}^{N-1} \rho_k S_k \text{sen}_k\Big(\frac{2i+1}{2}\Big), \qquad (5)$$

$0 \leq i \leq N-1$, onde $\rho_k = \begin{cases} \frac{1}{2}, & k = N \\ 1, & k \neq N \end{cases}$.
As expressões 4 e 5 definem o par transformado da TDSCF, denotado por

$$f = (f_i) \longleftrightarrow S = (S_k).$$

Exemplo 1: Considerando $p = 11$, o elemento $\zeta = (3 + j5) \in \text{GI}(11)$ tem ordem $p+1 = 12$ e é um elemento gerador do grupo unimodular de GI(7). Nessa estrutura, um par TDSCF de comprimento $(p+1)/2 = 6$ é

$$f = (1, 2, 3, 4, 5, 6) \longleftrightarrow S = (j4, 1, j10, 2, j6, 6)$$

As matrizes de transformação direta e inversa, são dadas por

$$M_{k,i} = \begin{bmatrix} j2 & j3 & j5 & j5 & j3 & j2 \\ 10 & 9 & 10 & 1 & 2 & 1 \\ j3 & j3 & j8 & j8 & j3 & j3 \\ 5 & 0 & 6 & 5 & 0 & 6 \\ j5 & j8 & j2 & j2 & j8 & j5 \\ 9 & 2 & 9 & 2 & 9 & 2 \end{bmatrix}$$

e

$$M_{k,i}^{-1} = \begin{bmatrix} j2 & 10 & j3 & 5 & j5 & 10 \\ j3 & 9 & j3 & 0 & j8 & 1 \\ j5 & 10 & j8 & 6 & j2 & 10 \\ j5 & 1 & j8 & 5 & j2 & 1 \\ j3 & 2 & j3 & 0 & j8 & 10 \\ j2 & 1 & j3 & 6 & j5 & 1 \end{bmatrix}$$

3.2 As Matrizes de Transformação

As expressões 4 e 5, repetidas a seguir, definem o par transformado da TDSCF $(f_i) \longleftrightarrow (S_k)$:

$$\begin{cases} S_k = \sum_{i=0}^{N-1} 2 f_i \mathrm{sen}_k(\frac{2i+1}{2}), & 1 \le k \le N, \\ f_i = \frac{1}{N} \sum_{k=1}^{N} \rho_k S_k \mathrm{sen}_k(\frac{2i+1}{2}), & 0 \le i \le N-1 \end{cases} \quad (6)$$

onde $\rho_k = \begin{cases} \frac{1}{2}, & k = N \\ 1, & k \neq N \end{cases}$. Devido à forma das expressões em 6, as matrizes de transformação direta e inversa, de elementos dados por $m_{k,i} = [2\mathrm{sen}_k(2i+1)/2]$ e $m^{-1}_{k,i} = [\frac{\rho_k}{N}\mathrm{sen}_k(2i+1)/2]$, respectivamente, apresentam uma relação simples e dada uma destas matrizes é possível obter a outra diretamente por inspeção. No exemplo, tem-se

$$m^{-1}_{k,i} = \begin{cases} 6m_{k,i}, & k = N \\ m_{k,i}, & k \neq N \end{cases} .$$

3.3 A TDSCF de Mersenne

Uma importante subclasse de transformadas derivadas da TDSCF, é a das TDSCF 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 N da transformada é um divisor de 2^{s-1}, o que a torna uma ferramenta atrativa uma vez que algoritmos rápidos de base 2 podem ser usados na sua computação. A tabela 1 a seguir apresenta valores de parâmetros envolvidos na construção de algumas TDSCF.

Tabela 1: Parâmetros da Transformada Discreta do Seno em alguns corpos finitos: p, comprimento N, elemento unimodular ζ usado na função k-sen(.) e a sua ordem no campo de extensão GF(p^2).

GF(p)	N	ζ	**Ord(ζ)**
7*	4	$2+j2$	8
11	6	$3+j5$	12
19	5	$17+j4$	10
23	12	$4+j10$	24
31*	8	$7+j13$	16
31*	16	$2+j11$	32
47	24	$4+j19$	48
71	36	$8+j24$	72
79	40	$2+j32$	80
103	52	$2+j10$	104
127*	64	$2+j39$	128
151	76	$2+j65$	152
167	84	$4+j73$	168
191	96	$6+j27$	192
199	100	$2+j14$	200

* TDSCF de Mersenne.

No exemplo 1, o vetor transformado tem componentes em GI(p). Entretanto, como os elementos da matriz de transformação são obtidos por potências da raíz quadrada de um elemento unimodular, devido ao fator $(1/j2)$ na definição da função k-sen, 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). Além disso, transformadas reais podem ser facilmente construídas, considerando-se a proposição 2 a seguir [12].

Proposição 2 *Se $\zeta = a+jb$ é um elemento unimodular, então a função* $\mathrm{sen}_k(i)$ *assume apenas valores em* GF(p)*, para quaisquer i, k.*

Portanto, se ζ é um elemento unimodular cuja raíz quadrada λ também é unimodular, então a matriz de transformação so terá elementos pertencentes a GF(p) e a TDSCF 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 TDSCF de comprimento $N = (p+1)/4$. Uma tal transformada é mostrada no exemplo 2 a seguir.

Exemplo 2: Considerando $p = 31$, um primo de Mersenne, o elemento $\zeta = (7 + j13) \in$ GI(31) tem ordem $(p+1)/2 = 16$ e pode ser usado para definir uma TDSCF de Mersenne de comprimento $(p+1)/4 = 8$. Um par dessa transformada é

$$\begin{matrix} f \\ (1,2,3,4,5,6,7,8) \end{matrix} \quad \longleftrightarrow \quad \begin{matrix} S \\ (2,28,27,2,23,10,20,8) \end{matrix}$$

e suas matrizes de transformação reais são dadas por

$$M_{k,i} = \begin{bmatrix} 9 & 11 & 21 & 4 & 4 & 21 & 11 & 9 \\ 26 & 17 & 17 & 26 & 5 & 14 & 14 & 5 \\ 11 & 4 & 9 & 10 & 10 & 9 & 4 & 11 \\ 23 & 23 & 8 & 8 & 23 & 23 & 8 & 8 \\ 21 & 9 & 27 & 11 & 11 & 27 & 9 & 21 \\ 17 & 5 & 5 & 17 & 14 & 26 & 26 & 14 \\ 4 & 10 & 11 & 22 & 22 & 11 & 10 & 4 \\ 29 & 2 & 29 & 2 & 29 & 2 & 29 & 2 \end{bmatrix}$$

e

$$M^{-1}_{k,i} = \begin{bmatrix} 18 & 21 & 22 & 15 & 11 & 3 & 8 & 29 \\ 22 & 3 & 8 & 15 & 18 & 10 & 20 & 2 \\ 11 & 3 & 18 & 16 & 23 & 10 & 22 & 29 \\ 8 & 21 & 20 & 16 & 22 & 3 & 13 & 2 \\ 8 & 10 & 20 & 15 & 22 & 28 & 13 & 29 \\ 11 & 28 & 18 & 15 & 23 & 21 & 22 & 2 \\ 22 & 28 & 8 & 16 & 18 & 21 & 20 & 29 \\ 18 & 10 & 22 & 16 & 11 & 28 & 8 & 2 \end{bmatrix} .$$

4 Conclusões e Sugestões

Nesse trabalho uma nova transformada foi introduzida, a transformada discreta do seno sobre GF(p)

(a TDSCF), uma versão de corpo finito da bem conhecida transformada discreta do seno definida sobre o corpo dos números reais. Inicialmente, foram apresentados alguns fundamentos matemáticos que levam à construção das funções k-trigonométricas sobre um corpo finito. Para derivar a TDSCF da seqüência f de comprimento N, adotou-se, em um corpo finito, o procedimento clássico de relacionar f com uma nova seqüência, g, de comprimento $2N$. A TDSCF S de f foi então obtida da transformada de Fourier de corpo finito G de g. Por meio das relações estabelecidas entre G e S, estabeleceu-se a fórmula de inversão da transformada. A TDSCF tem comprimentos divisores de $(p+1)$, onde $p \equiv 3 \pmod 4$, sendo possível a construção da TDSCF de Mersenne, que apresenta comprimentos cujos valores são potências de 2.

A TDSCF introduzida nesse trabalho corresponde a versão anti-simétrica par. Sua versão bidimensional pode ser construída por um procedimento semelhante ao introduzido nesse trabalho.

Considerando a existência de definições alternativas para a TDS usual, versões de corpo finito dessas alternativas e possíveis aplicações para a transformada discreta do seno de corpo finito estão sendo investigadas.

Referências

[1] A. K. Jain, *Fundamentals of Digital Image Processing, Prentice-Hall*, 1989.

[2] H. S. Malvar, *Signal Processing with Lapped Transforms*, Artech, 1992.

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

[4] 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.

[5] 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.

[6] 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, agosto 2001.

[7] 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.

[8] M. M. Campello de Souza, H. M. de Oliveira, R. M. Campello de Souza e M. M. Vasconcelos, A Transformada Discreta do Cosseno em um Corpo Finito, *Anais do XX Simpósio Brasileiro de Telecomunicações*, Rio de Janeiro, RJ, outubro 2003.

[9] D. Silva, R. M. Campello de Souza, H. M. de Oliveira, L. B. E. Palma e 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, junho 2002.

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

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

[12] 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.