Auto-seqüências da Transformada Numérica de Fourier

H. M. Cavalcanti, R. M. Campello de Souza

***Resumo*— Sinais cujas formas não variam quando submetidos à Transformada Numérica de Fourier (TNF) e que geram uma classe de autofunções do operador unitário TNF são apresentados. A utilização de tais seqüências invariantes como assinaturas de usuários em um sistema de comunicação multiusuário através do Canal Somador Real (t-RAC) é sugerida.**

***Palavras-Chave*— Transformadas numéricas, comunicação multiusuário, canal somador real, transformada de Fourier de corpo finito.**

***Abstract*— shape-invariant signals under the Number Theoretic Fourier Transform (NTFT) are investigated, leading to a class of eigenfunctions for the unitary NTFT operator. Such invariant sequences (eigensequences) are suggested as user signatures over the real adder channel (t-RAC) for a multiuser communication system.**

***Keywords*— Number theoretic transforms, multiuser communication, real adder channel, finite field Fourier transform.**

I. INTRODUÇÃO

Este trabalho investiga as auto-seqüências do operador Transformada Numérica de Fourier (TNF). Uma seqüência cuja forma não é alterada pelo operador TNF é uma seqüência invariante à TNF (SITNF). Tais seqüências são importantes em aplicações envolvendo análise de espectro, já que a complexidade computacional de suas TNFs é linear. Por ser uma transformada de corpo finito, a TNF oferece ainda uma vantagem a mais em relação à Transformada Discreta de Fourier (DFT), que é o fato de só se trabalhar com números inteiros, evitando assim problemas com arredondamento e truncamento, comuns em aplicações que trabalham no domínio dos números reais [1].

II. AUTO-SEQÜÊNCIAS DA TRANSFORMADA NUMÉRICA DE FOURIER

A seguir, a forma unitária do operador TNF é definida [2].

Definição 1. A transformada numérica de Fourier unitária de x[n], uma seqüência de comprimento N de componentes em GF(p), é a seqüência X[k], $k = 0, 1, \ldots, N-1$, de elementos em GF(p) dados por

$$X[k] \triangleq (\sqrt{N})^{-1}(mod\ p)\sum_{n=0}^{N-1} x[n]\alpha^{kn}\ , \tag{1}$$

onde $N^{\frac{p-1}{2}} \equiv 1(mod\ p)$ e $\alpha \in GF(p)$ tem ordem N.

H. M. Cavalcanti, R. M. Campello de Souza¸ Departamento de Eletrônica e Sistemas, Grupo de Processamento de Sinais, Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, PE, E-mails: herciliomc@gmail.com, ricardo@ufpe.br.

A transformada inversa de X[k] é

$$x[n] = (\sqrt{N})^{-1}(mod\ p)\sum_{k=0}^{N-1} X[k]\alpha^{-kn}. \tag{2}$$

O par transformado da TNF é denotado por

$$x[n] \leftrightarrow X[k]. \tag{3}$$

Algumas propriedades úteis são listadas abaixo.
P1. X[n]$\leftrightarrow$x[-k].
P2. E(x[n])$\leftrightarrow$ E(X[k]).
P3. O(x[n])$\leftrightarrow$ O(X[k]),
onde E(x[n]) e O(x[n]) denotam, respectivamente, as partes par e ímpar de x[n].
O presente trabalho investiga seqüências x[n] cuja TNF X[k] tem a forma

$$X[k] = \lambda x[k], \tag{4}$$

$\lambda\in$GF(p) ou, em forma de operador, Γ(x[n])=λx[n], onde Γ denota o operador TNF unitário. Tais seqüências são então auto-sequências da TNF com autovalor associado λ e são denotadas por λN-SITNF. Os valores de λ satisfazendo (4) são dados pelo Teorema 1.

Teorema 1: Os autovalores do operador TNF unitário são as raízes de ordem quatro da unidade ($\pm$1,$\pm j$) , onde

$$j^2 \equiv -1(mod\ p). \tag{5}$$

Demonstração: Aplicando quatro vezes o operador TNF a x[n] e considerando a propriedade P1, obtém-se

$$\Gamma^{(4)}(x[n]) = \lambda^4 x[k] = x[k], \tag{6}$$

portanto λ^4=1 e o resultado segue.

■

É possível provar que [3], se p=4k+3 então j$\in$GF(p^2), k inteiro, e se p=4k+1, então

$$j = (\frac{p-1}{2})!(mod\ p). \tag{7}$$

O teorema a seguir ilustra um pouco da natureza de uma λN-SITNF.

Teorema 2: Se x[n] é uma λN-SITNF, então x[n] é ímpar se λ =$\pm$j ou par se λ=$\pm$1.

Demonstração: Se x[n]$\leftrightarrow$X[k] é uma λN-SITNF, então utilizando-se a propriedade P1, o par transformado resultante é λx[n]$\leftrightarrow$x[-k]. Logo λ^2x[k]=x[-k], de modo que se λ=$\pm$1 então x[n]=x[-n] e, se λ=$\pm$j , x[n]=-x[-n] e a prova está completa.

■

Seqüências ímpares e pares podem ser usadas para gerar λN-SITNFs de acordo com os teoremas 3 e 4 a seguir.

Teorema 3: Se x[n] é uma seqüência de comprimento N, então a seqüência y[n]=E(x[n])$\pm$E(X[n]) é uma λN-SITNF com autovalor associado λ=$\pm$1.

Demonstração: Das propriedades P1 e P2 pode-se obter o par E(x[n])$\pm$E(X[n])$\leftrightarrow$E(X[k])$\pm$E(x[-k]), logo E(x[n])$\pm$E(X[n])$\leftrightarrow\pm$(E(x[k])$\pm$E(X[k])) e o resultado segue. ■

Corolário: Toda seqüência x[n] par de comprimento N gera uma λN-SITNF y[n]=x[n]$\pm$X[n]. ■

Teorema 4: Se x[n] é uma seqüência de comprimento N, então a seqüência y[n]=O(x[n])$\mp$jO(X[n]) é uma λN-SITNF com autovalor associado λ=$\pm$j.

Demonstração: Das propriedades P1 e P3, obtém-se o par O(x[n])$\mp$jO(X[n])$\leftrightarrow$O(X[k])$\mp$jO(x[-k]) ou seja O(x[n])$\mp$jO(X[n])$\leftrightarrow\pm$j(O(x[k])$\mp$jO(X[k])) e a prova está completa. ■

Corolário: Toda seqüência x[n] ímpar de comprimento N gera uma λN-SITNF y[n]=x[n]$\mp$jX[n]. ■

III. Seqüências empregadas sobre o canal somador real

Os teoremas 3 e 4 ilustram um método simples de se obter λN-SITNFs. Há ainda um outro algoritmo que emprega trigonometria de corpos finitos para gerar famílias de λN-SITNFs para um dado primo da forma 4k+3 [1], [4]. No que se segue, SITNFs são usadas na concepção de um sistema de múltiplo acesso para o canal somador real.

A. Emprego de auto-seqüências da TNF sobre o canal somador real

Um modelo de canal de comunicação bem conhecido é o Canal Somador Real de t usuários (t-RAC). No presente trabalho, uma utilização das auto-seqüências da TNF como assinaturas de usuários sobre o 4-RAC é sugerida. No que se segue, $x_i[n]$ é a seqüência do usuário i. Essa seqüência deve ser uma λ_iN-SITNF, onde λ_1=1, λ_2=-1, λ_3=j e λ_4=-j.

A1. 4-RAC

Seja a seqüência y[n], enviada pelo canal, dada por

$$y[n] = x_1[n] + x_2[n] + x_3[n] + x_4[n]. \quad (8)$$

Se aplicarmos três vezes a TNF à ambos os membros da equação (8) podemos obter o seguinte sistema de equações,
x_1[n]+x_2[n]+x_3[n]+x_4[n]=y[n],
x_1[n]-x_2[n]+jx_3[n]-jx_4[n]=Γ(y[n]),
x_1[n]+x_2[n]-x_3[n]-x_4[n]=$\Gamma^{(2)}$(y[n]),
x_1[n]-x_2[n]-jx_3[n]+jx_4[n]=$\Gamma^{(3)}$(y[n]),
cuja solução leva às expressões de recuperação das seqüências dos usuários,
x_1[n]=$\frac{1}{2}$(E(y[n])+E(Y[n])),
x_2[n]=$\frac{1}{2}$(E(y[n])-E(Y[n])),
x_3[n]=$\frac{1}{2}$(O(y[n])-jO(Y[n])),
x_4[n]=$\frac{1}{2}$(O(y[n])+jO(Y[n])).

B. Exemplos de Auto-seqüências da Transformada Numérica de Fourier.

A tabela I apresenta exemplos de auto-seqüências da TNF para diversos valores de p e de λ.

TABELA I
AUTO-SEQÜÊNCIAS DA TRANSFORMADA NUMÉRICA DE FOURIER.

N	λ	p	seqüência
4	1	29	3,1,1,1
4	−1	17	15,2,2,2
4	j=12	29	0,28,0,1
7	j=12	29	0,3,9,12,17,20,26
7	−j=17	29	0,9,4,2,27,25,20
8	1	17	14,11,15,16,6,16,15,11
8	−1	17	9,16,7,16,4,16,7,16
12	1	13	5,5,4,9,1,1,6,1,1,9,4,5
12	−1	13	7,8,8,8,8,8,8,8,8,8,8,8
12	j=5	13	0,6,2,11,2,10,0,3,11,2,11,7
12	−j=8	13	0,0,4,5,11,11,0,2,2,8,9,0

É importante observar que na tabela acima foram considerados apenas primos da forma 4k+1, pois as TNFs obtidas a partir destes primos possuem autovalores reais e inteiros, o que não é possível para a DFT [1]. Esta é uma motivação adicional para a implementação de sistemas multiusuário como o 4-RAC sugerido no presente trabalho.

IV. Conclusões

Este trabalho investiga seqüências que são invariantes ao operador TNF unitário. Tais seqüências são de relevante interesse, pois o cálculo de suas TNFs é feito com uma complexidade computacional linear. Procedimentos sistemáticos para a obtenção de tais seqüências foram propostos. Um sistema de múltiplo acesso para o canal somador real com quatro usuários, utilizando as auto-seqüências da TNF como assinaturas, foi proposto. Expressões para a recuperação da informação dos usuários foram obtidas. O desempenho do esquema sugerido está sob investigação.

Agradecimentos

Os autores agradecem ao Prof. Dr. Hélio M. de Oliveira por suas valorosas sugestões ao presente trabalho.

Referências

[1] R. M. Campello de Souza, H. M. de Oliveira, "Eigensequences for Multiuser Communication over the Real Adder Channel", VI International Telecomunications Symposium (ITS´2006), Fortaleza, Sep. 2006.
[2] J. M. Pollard, "The Fast Fourier Transform in a Finite Field", Math. Comput., vol. 25, No. 114, pp. 365-374, Apr. 1971.
[3] D. M. Burton, "Elementary Number Theory", McGraw-Hill, 4ª ed., 1998.
[4] R.M. Campello De Souza, H.M. de Oliveira, A.N. Kauffman, A.J.A Paschoal, "Trigonometry in Finite Fields and a New Hartley Transform", Proceedings of the 1998 IEEE International Symposium on Information Theory, p. 293, Aug. 1998.