NOVAS FERRAMENTAS PARA PROCESSAMENTO DE SINAIS EM CORPOS FINITOS

A. J. A. Paschoal
H. M. de Oliveira
R. M. Campello de Souza

CODEC - GRUPO DE PESQUISA EM COMUNICAÇÕES
DEPARTAMENTO DE ELETRÔNICA E SISTEMAS
UNIVERSIDADE FEDERAL DE PERNAMBUCO
Caixa Postal 7800, 50732-970, Recife/PE

RESUMO

Neste artigo, o conceito de anel galoisiano é introduzido com o objetivo de desenvolver novas ferramentas para o processamento de sinais definidos em corpos finitos. Assim, definem-se as funções k-trigonométricas seno e cosseno sobre o corpo finito $GF(p^m)$ e exploram-se algumas de suas propriedades. Algumas sugestões de aplicações empregando tais ferramentas são apresentadas.

ABSTRACT

In this paper, the concept of Galoisian Ring is introduced aiming at the development of new tools for the processing of signals defined over finite fields. The notions of k-trigonometric functions over the finite field $GF(p^m)$ are defined, and a few of its properties are investigated. Some applications of the new tools are suggested.

I. INTRODUÇÃO

A Transformada Aritmética de Fourier (AFT) consiste num algoritmo para calcular os coeficientes da série de Fourier de um sinal que emprega a fórmula de inversão de Möbius. Tal algoritmo possui as seguintes vantagens: (i) baixa complexidade computacional, medida pelo numero de adições e multiplicações necessárias e (ii) possibilidade de implementação usando processamento paralelo. A AFT originalmente definida por D. Tufts e G. Sadasiv em 1988 [1], possuia a desvantagem de ser apenas aplicável a sinais periódicos reais e pares. Posteriormente, ela foi estendida por I. Reed *et al.* [2] para computar os coeficientes de qualquer sinal periódico complexo. De fato, a AFT compete com os algoritmos rápidos (transformadas rápidas de Fourier - FFT) clássicos empregados para computar a transformada discreta de Fourier (DFT) no que diz respeito a precisão, complexidade computacional e velocidade. De especial interesse no contexto das áreas de Processamento Digital de Sinais e de Teoria da Informação é a DFT definida sobre um corpo finito (GFT - Galois Field Transform) [3,4]. Este artigo objetiva introduzir novas ferramentas para o processamento de sinais definidos sobre corpos finitos, visando dentre outras aplicações estabelecer condições que permitam o desenvolvimento de um algoritmo similar à AFT para o cálculo da GFT. Entretanto, tal como na AFT, o desenvolvimento deste algoritmo deve ser essencialmente baseado em representações trigonométricas, porém sobre corpos finitos. O presente trabalho introduz esta teoria, o que per si constitui um resultado interessante, estendendo a trigonometria à matemática discreta e abrindo possibilidades para o desenvolvimento de novos algoritmos.

II. ANÉIS GALOISIANOS

Antes de introduzir uma trigonometria sobre corpos finitos, alguns resultados preliminares são apresentados. Particularmente, introduz-se uma estrutura cujos elementos, denominados galoisianos, são do tipo $\gamma = \alpha + j\beta$, onde $\alpha, \beta \in GF(p^m)$, sendo p um primo ímpar, e $j = \sqrt{-1}$. Este números correspondem a complexos definidos em um corpo finito.

Definição 1 : Um Anel Galoisiano $GR(p^m)$ é uma estrutura matemática $<G, \oplus, \odot>$ contendo duas operações, definidas respectivamente por

$$\gamma_1 \oplus \gamma_2 = (\alpha_1 + j\beta_1) \oplus (\alpha_2 + j\beta_2) = (\alpha_1 + \alpha_2) + j(\beta_1 + \beta_2),$$

$$\gamma_1 \odot \gamma_2 = (\alpha_1 + j\beta_1) \odot (\alpha_2 + j\beta_2) = (\alpha_1\alpha_2 - \beta_1\beta_2) + j(\alpha_1\beta_2 + \alpha_2\beta_1)$$

onde os elementos do conjunto G são galoisianos sobre o corpo finito $GF(p^m)$ e verificam às seguintes propriedades:

(i) (Fechamento) Dados $\gamma_1, \gamma_2 \in GR(p^m)$, então,

$$\gamma_1 \oplus \gamma_2 \quad e \quad \gamma_1 \odot \gamma_2 \in GR(p^m).$$

(ii) (Associatividade) Dados $\gamma_1, \gamma_2, \gamma_3 \in GR(p^m)$, então,

$$\gamma_1 \oplus (\gamma_2 \oplus \gamma_3) = (\gamma_1 \oplus \gamma_2) \oplus \gamma_3 = \gamma_1 \oplus \gamma_2 \oplus \gamma_3$$

$$\gamma_1 \odot (\gamma_2 \odot \gamma_3) = (\gamma_1 \odot \gamma_2) \odot \gamma_3 = \gamma_1 \odot \gamma_2 \odot \gamma_3$$

(iii) Dado $\gamma \in GR(p^m)$, existe $e_{\otimes} \in GR(p^m)$, tal que $\gamma \otimes e_{\otimes} = e_{\otimes} \otimes \gamma = \gamma$. O elemento $e_{\otimes}$ é chamado identidade multiplicativa e corresponde ao galoisiano 1 + j0, onde 0 e 1 são, respectivamente, as identidades aditiva e multiplicativa no corpo $GF(p^m)$. Além disso, existe $e_{\oplus} \in GR(p^m)$ tal que $\gamma \oplus e_{\oplus} = e_{\oplus} \oplus \gamma = \gamma$. O elemento $e_{\oplus}$ é chamado identidade aditiva, que claramente corresponde ao galoisiano 0 + j0.

(iv) Dado $\gamma \in GR(p^m)$, existe $\gamma^{-1} \in GR(p^m)$, tal que $\gamma \oplus \gamma^{-1} = \gamma^{-1} \oplus \gamma = e_{\oplus}$. O elemento γ^{-1} é chamado o inverso aditivo de γ

Dado um elemento $a \in GR(p^m)$, se existir $a^{-1} \in GR(p^m)$, tal que $a \otimes a^{-1} = a^{-1} \otimes a = e_{\otimes}$, então tal elemento é chamado de inverso multiplicativo de a.

O módulo quadrado e o conjugado complexo de um galoisiano $\gamma = \alpha + j\beta$ são expressos por $|\gamma|^2 = \alpha^2 + \beta^2$ e $\gamma^* = \alpha - j\beta$, respectivamente.

Lema 1 : Um galoisiano γ é não-inversivel se e somente se $|\gamma|^2 \equiv 0 \pmod p$.

Prova : Dado um galoisiano $\gamma_1 = \alpha_1 + j\beta_1$, seja $\gamma_2 = \alpha_2 + j\beta_2$ o seu inverso multiplicativo. Então, deve-se ter

$$\gamma_1 \otimes \gamma_2 = (\alpha_1 + j\beta_1) \otimes (\alpha_2 + j\beta_2) = 1 + j0.$$

Assim,

$$\alpha_1\alpha_2 - \beta_1\beta_2 = 1,$$

$$\alpha_1\beta_2 + \alpha_2\beta_1 = 0.$$

Ou, equivalentemente,

$$\begin{bmatrix} \alpha_1 & -\beta_1 \\ \beta_1 & \alpha_1 \end{bmatrix} \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

O sistema acima não tem solução para $|\gamma_1|^2 \equiv 0 \pmod p$.

Q.E.D

No caso de γ_1 ser um Galoisiano inversível, seu inverso γ_2 será expresso por

$$\gamma_2 = \frac{1}{\alpha_1^2 + \beta_1^2}(\alpha_1 - j\beta_1) = \frac{\gamma_1^*}{|\gamma_1|^2}.$$

ficando implícita a condição de se ter, neste caso, $\alpha_1^2 + \beta_1^2 \equiv 0 \pmod p$.

III. RELAÇÕES TRIGONOMÉTRICAS SOBRE CORPOS FINITOS

Definição 2 : Dado um elemento $\alpha^i \in GF(p^m)$, α primitivo, definem-se as funções k-trigonométricas pelas relações :

$$\cos_k(i) = \frac{\alpha^{ik} + \alpha^{-ik}}{2},$$

$$\operatorname{sen}_k(i) = \frac{\alpha^{ik} - \alpha^{-ik}}{2j},$$

$k = 0, 1, \ldots, p^m - 2$, $i = 0, 1, \ldots, p^m - 2$.

É interessante observar que as expressões acima são bem definidas sobre $GR(p^m)$ e que resultam em galoisianos e, em contraste com as funções trigonométricas usuais, não apresentam noção de ordem. Ademais, a restrição $p \neq 2$ garante a incongruência entre as operações de adição e subtração.

III.1 **Propriedades** (As provas podem ser obtidas a partir da definição 2 e não são apresentadas aqui [5].)

Em GF(p), as operações são feitas reduzindo-se mod p. Sobre o corpo de extensão $GF(p^m)$, as operações são feitas modulo $\pi(x)$, o polinômio primitivo usado para gerar o corpo.

P1 (Círculo Unitário) :

$$\operatorname{sen}_k^2(i) + \cos_k^2(i) \equiv 1.$$

Embora a equação acima defina um circulo generalizado, este não apresenta as propriedades usuais de círculos definidos no espaço euclidiano.

P2 (Par/Impar) :

$$\cos_k(i) = \cos_k(-i),$$
$$\operatorname{sen}_k(i) = -\operatorname{sen}_k(-i),$$

P3 (Simetria) :

$$\cos_k(i) = \cos_i(k),$$
$$\operatorname{sen}_k(i) = \operatorname{sen}_i(k),$$

P4 (Fórmulas de Euler) :

$$\alpha^{ik} \equiv \cos_k(i) + j\operatorname{sen}_k(i),$$
$$\alpha^{-ik} \equiv \cos_k(i) - j\operatorname{sen}_k(i).$$

P5 (Adição de arcos) :

$$\cos_k(i \pm j) \equiv \cos_k(i)\cos_k(j) \mp \operatorname{sen}_k(i)\operatorname{sen}_k(j),$$

$$\operatorname{sen}_k(i \pm j) \equiv \operatorname{sen}_k(i)\cos_k(j) \pm \operatorname{sen}_k(j)\cos_k(i),$$

P6 (Arco duplo) :

$$\cos_k^2(i) - \mathrm{sen}_k^2(i) \equiv \cos_k(2i),$$

$$\cos_k^2(i) \equiv \frac{1 + \cos_k(2i)}{2},$$

$$\mathrm{sen}_k^2(i) \equiv \frac{1 - \cos_k(2i)}{2}.$$

P7 (Ortogonalidade) :

$$\text{(i)} \sum_{i=0}^{p^m-2} \cos_k(i)\,\mathrm{sen}_k(l) \equiv 0.$$

$$\text{(ii)} \sum_{i=0}^{p^m-2} \mathrm{sen}_k(i)\,\mathrm{sen}_k(l) = \begin{cases} (p^m-1)/2 & \text{se } i \equiv l \\ -(p^m-1)/2 & \text{se } i \equiv -l \\ 0 & \text{em caso contrário} \end{cases}$$

$$\text{(iii)} \sum_{i=0}^{p^m-2} \cos_k(i)\,\cos_k(l) = \begin{cases} (p^m-1)/2 & \text{se } i \equiv l \text{ ou } i \equiv -l \\ 0 & \text{em caso contrário} \end{cases}$$

Abaixo exibem-se exemplos ilustrativos apresentando funções k-trigonométricas definidas sobre GF(5) e GF(5^2). No primeiro caso (Tabela 1), considera-se o elemento primitivo $\alpha = 2$ e é assumido k = 1, enquanto que no segundo caso o polinômio gerador é $\pi(x) = x^2 + x + 2$.

p = 5, m = 1, $\alpha = 2$, k = 1.

i	$\cos_1(i)$	$\mathrm{sen}_1(i)$
0	1	0
1	0	j3
2	4	0
3	0	j2 = -j3

Tabela 1 - Funções k-trigonométricas sobre GF(5)

As propriedades apresentadas podem ser trivialmente verificadas, e.g.: $0 + (j3)^2 \equiv 1 \pmod 5$ **(P1)**; $\cos_1(2) = \cos_1(-2)$, $\mathrm{sen}_1(3) = -\mathrm{sen}_1(-3)$ **(P2)**; $2 = 0 + j(j3) \pmod 5$ **(P5)**; etc.

Em GF(5^2), com $\pi(x) = x^2 + x + 2$, tem-se

$\cos_1(9) = \alpha^{21}$ e $\mathrm{sen}_1(9) = -j\alpha^{15}$;

$\cos_1^2(9) + \mathrm{sen}_1^2(9) = \alpha^{18} - \alpha^6 = 1$ **(P1)**

$\alpha^9 = \alpha^{21} + j(-j\alpha^{15}) = 4 + 3\alpha$ **(P5)**, etc.

IV. A GUISA DE UMA ANÁLISE DE FOURIER

A análise espectral constitui uma das ferramentas de maior uso em Engenharia e, em particular, no domínio das telecomunicações. Noções de espectro e transformada são de uso largamente difundido e são bastante úteis em áreas como códigos corretores de erro e criptografia, as quais lidam com corpos finitos. Neste contexto, a GFT é a ferramenta adequada.

Por definição, o espectro do sinal discreto $\underline{f} = (f_0, f_1, \ldots, f_{N-1})$, com componentes $f_i \in GF(p)$, é o vetor $\underline{F} = (F_0, F_1, \ldots, F_{N-1})$, com componentes $F_k \in GF(p^m)$, dadas por

$$F_k = \sum_{i=0}^{N-1} f_i \alpha^{ik}.$$

onde α é um elemento de ordem N de $GF(p^m)$.

A fórmula de inversão é dada por [3],

$$f_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} F_k\, \alpha^{-ik}.$$

Empregando-se as funções k-trigonométricas, F_k pode ser expressa por

$$F_k = \frac{1}{2}(a_k - jb_k), \qquad k = 0, 1, \ldots, N-1$$

onde

$$a_k = 2 \cdot \sum_{i=0}^{N-1} f_i \cos_k(i),$$

$$b_k = -2 \cdot \sum_{i=0}^{N-1} f_i\, \mathrm{sen}_k(i).$$

Usando a propriedade P5, na fórmula de inversão, é possível escrever

$$f_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} F_k\, (\cos_k(i) - j\,\mathrm{sen}_k(i)).$$

Assim,

$$f_i = x_0 + \sum_{k=1}^{N-1} x_k \cos_k(i) + \sum_{k=1}^{N-1} y_k\, \mathrm{sen}_k(i),$$

onde

$$x_0 = \frac{1}{N(\text{mod } p)} \sum_{i=0}^{N-1} f_i \qquad \text{é o valor médio do sinal } f \,.$$

$$x_k = \frac{1}{N(\text{mod } p)} F_k \,, \text{ e } y_k = -j \frac{1}{N(\text{mod } p)} F_k = -j\, x_k \,.$$

Eliminando o valor dc do sinal discreto, define-se $\bar{f}_i \equiv f_i - x_0$, $i = 0, 1, ..., N-1$. Consequentemente,

$$\bar{f}_i = \sum_{k=1}^{N-1} x_k \cos_k(i) + \sum_{k=1}^{N-1} y_k \operatorname{sen}_k(i).$$

que corresponde a uma representação do tipo série de Fourier para o sinal $\bar{f}$.

V. COMENTÁRIOS

Este artigo introduz os fundamentos para construir uma análise trigonométrica semelhante à de Fourier sobre corpos finitos, que apresenta propriedades correlatas àquelas da análise de Fourier clássica. Foram introduzidas funções trigonométricas sobre corpos finitos de característica impar, demonstrando-se algumas relações trigonométricas importantes

As transformadas rápidas são, em geral, ferramentas bastante eficazes no processamento de informações. Em particular, a Transformada Aritmética de Fourier aparece como um eficiente e promissor algoritmo para o cálculo da DFT. Um dos principais objetivos do desenvolvimento de uma análise de Fourier em corpos finitos foi o de estabelecer condições para a concepção de um algoritmo rápido, semelhante a AFT, para a computação da transformada de Fourier de Corpo Finito, em corpos de ordem prima ou não. Tal procedimento seria de larga aplicação prática, uma vez que estas transformadas (e.g., NTT, GFT) são de grande utilidade em diversas subáreas da Engenharia Eletrônica moderna.

A ferramenta proposta neste trabalho, entretanto, pode vir a desempenhar um papel muito mais amplo no contexto da área de Processamento Digital de Sinais. Assim, por exemplo, sugerimos sua utilização visando (1) definir em corpos finitos, as transformadas discretas do cosseno (DCT) e do seno (DST) e (2) conceber novos algoritmos, mais rápidos que os atualmente existentes, para a decodificação de códigos algébricos no domínio da frequência e para a computação de convoluções discretas.

AGRADECIMENTOS

Este trabalho recebeu apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

VI. REFERÊNCIAS

[1] D. W. Tufts and G. Sadasiv, "The Arithmetic Fourier Transform", IEEE ASSP Mag., pp. 13-17, Jan. 1988.

[2] I. S. Reed, D. W. Tufts, X. Yu, T. K. Truong, M. T. Shih, and X. Yin, "Fourier Analysis and Signal Processing by Use of the Möbius Inversion Formula", IEEE Trans. Acoust., Speech and Signal Processing, Vol. ASSP-38, Nº 3, pp. 458-470, Março 1990.

[3] J. M. Pollard, "The Fast Fourier Transform in a Finite Field", Mathematics of Computation, Vol. 25, pp. 365-374, Abril 1971.

[4] R. M. Campello de Souza, "Transformadas em Corpos Finitos para codificação de Canal", Número Especial em Códigos Corretores de Erro da Revista da Sociedade Brasileira de Telecomunicações, Vol. 5, Nº 1, pp. 41-58, Junho 1990.

[5] A. J. A. Paschoal, "A Transformada Aritmética de Fourier", Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, UFPE, Maio 1993.