Transformadas do Cosseno sobre Corpos de Característica 2: Construções e Aplicação

Edmar S. da Silva, João Victor da Silva e Juliano B. Lima

***Resumo*— Neste artigo, são apresentadas construções de transformadas do cosseno sobre corpos finitos de característica 2 (FFCT). Um algoritmo rápido para o cálculo de uma das FFCT construídas é desenvolvido e uma aplicação dessas transformadas em processamento digital de imagens é descrita.**

***Palavras-Chave*— Transformada do cosseno, corpos finitos, algoritmos rápidos.**

***Abstract*— In this paper, cosine transforms over fields of characteristic 2 (FFCT) are constructed. A fast algorithm for computing a specific FFCT is developed and an application of such transforms in digital image processing is described.**

***Keywords*— Cosine transform, finite fields, fast algorithms.**

I. Introdução

As transformadas sobre corpos finitos desempenham um importante papel em diversas aplicações relacionadas à área de processamento de sinais. Nesse contexto, em que essas transformadas são mais conhecidas como transformadas numéricas, tais ferramentas matemáticas têm sido utilizadas principalmente na implementação de algoritmos para o cálculo eficiente de convoluções lineares [1].

Nas últimas décadas, vários tipos de transformadas sobre corpos finitos foram introduzidas e a gama de aplicações dessa classe de transformadas foi ampliada [2]–[5]. Em [6], especificamente, é descrita uma família de transformadas trigonométricas sobre corpos finitos com característica ímpar, a qual inclui oito transformadas do cosseno e oito do seno.

Neste artigo, são construídos exemplos particulares das recém-definidas transformadas do cosseno sobre corpos finitos de característica 2 [7], as quais são denotadas por FFCT (do inglês, *finite field cosine transform*). Inicialmente, constrói-se uma FFCT com 8-pontos sobre $\mathrm{GF}(2^8)$ e descreve-se um algoritmo rápido para o seu cálculo. Em seguida, apresenta-se uma FFCT com 32-pontos sobre $\mathrm{GF}(2^{24})$ e demonstra-se a sua aplicabilidade ao processamento de imagens coloridas.

II. Definição da FFCT

A definição da transformada do cosseno sobre corpos de característica 2 requer uma versão modificada da função cosseno sobre corpos finitos, a qual é fornecida a seguir.

Definição 1: Seja $\zeta \in \mathrm{GF}(2^r)$ um elemento com ordem multiplicativa $\mathrm{ord}(\zeta)$. A função cosseno sobre corpos finitos relacionada a ζ é definida como $\cos_\zeta(x) := \zeta^x + \zeta^{-x}$, para $x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

Edmar S. da Silva, João Victor da Silva e Juliano B. Lima, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife-PE, Brasil, E-mails: edmarcmr@gmail.com, jvsilva21.03@gmail.com, juliano_bandeira@ieee.org. Este trabalho foi parcialmente financiado pelo CNPq (307686/2014-0 e 456744/2014-2; PICME, Dpto. Matemática/UFPE).

Definição 2 (FFCT): Seja $\zeta \in \mathrm{GF}(2^r)$ um elemento tal que $\mathrm{ord}(\zeta) = 2N - 1$. A FFCT do vetor $\mathbf{x} = (x_i), x_i \in \mathrm{GF}(2^r), i = 0, 1, \ldots, N-2$, é o vetor $\mathbf{X} = (X_k), X_k \in \mathrm{GF}(2^r)$, cujas componentes são

$$X_k := \sum_{i=0}^{N-2} x_i \cos_\zeta(k(i+1/2)), k = 1, 2, \ldots, N-1. \quad (1)$$

Na FFCT inversa, as componentes de $\mathbf{x}$ são obtidas por

$$x_i = \sum_{k=1}^{N-1} X_k \cos_\zeta(k(i+1/2)), i = 0, 1, \ldots, N-2. \quad (2)$$

Pode-se expressar o cálculo da FFCT do vetor $\mathbf{x}$ como $\mathbf{X} = \mathbf{C}\cdot\mathbf{x}$, em que $\mathbf{C}$ é a matriz de transformação $(N-1)\times(N-1)$, cujo elemento na k-ésima linha e na i-ésima coluna é dado por $C_{k,i} = \cos_\zeta(k(i+1/2))$.

III. FFCT com 8-pontos sobre $\mathrm{GF}(2^8)$

Para construir o corpo $\mathrm{GF}(2^8)$, considera-se o polinômio primitivo $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, que tem α como raiz, com $\mathrm{ord}(\alpha) = 255$. Para definir uma transformada com $N - 1 = 8$ pontos, emprega-se o elemento $\zeta = \alpha^{15}$, uma vez que $\mathrm{ord}(\zeta) = \mathrm{ord}(\alpha^{15}) = 255/15 = 17 = 2N - 1$. Empregando as definições enunciadas na Seção II, obtém-se

$$\mathbf{C} = \begin{bmatrix} \alpha^{153} & \alpha^{136} & \alpha^{34} & \alpha^{68} & \alpha^{204} & \alpha^{17} & \alpha^{102} & \alpha^{51} \\ \alpha^{51} & \alpha^{17} & \alpha^{68} & \alpha^{136} & \alpha^{153} & \alpha^{34} & \alpha^{204} & \alpha^{102} \\ \alpha^{136} & \alpha^{204} & \alpha^{51} & \alpha^{102} & \alpha^{68} & \alpha^{153} & \alpha^{34} & \alpha^{17} \\ \alpha^{102} & \alpha^{34} & \alpha^{136} & \alpha^{17} & \alpha^{51} & \alpha^{68} & \alpha^{153} & \alpha^{204} \\ \alpha^{34} & \alpha^{51} & \alpha^{204} & \alpha^{153} & \alpha^{17} & \alpha^{102} & \alpha^{136} & \alpha^{68} \\ \alpha^{17} & \alpha^{153} & \alpha^{102} & \alpha^{204} & \alpha^{136} & \alpha^{51} & \alpha^{68} & \alpha^{34} \\ \alpha^{68} & \alpha^{102} & \alpha^{153} & \alpha^{51} & \alpha^{34} & \alpha^{204} & \alpha^{17} & \alpha^{136} \\ \alpha^{204} & \alpha^{68} & \alpha^{17} & \alpha^{34} & \alpha^{102} & \alpha^{136} & \alpha^{51} & \alpha^{153} \end{bmatrix}.$$

O algoritmo rápido para o cálculo de $\mathbf{X} = \mathbf{C}\cdot\mathbf{x}$ é baseado na decomposição da matriz $\mathbf{C}$ em quatro submatrizes, 4×4, $\mathbf{C}_1$, $\mathbf{C}_2$, $\mathbf{C}_3$ e $\mathbf{C}_4$, de modo que

$$[X_0\, X_1\, X_3\, X_7]^T = \mathbf{C}_1 \cdot [x_0\, x_4\, x_6\, x_7]^T + \mathbf{C}_2 \cdot [x_1\, x_2\, x_3\, x_5]^T;$$

$$[X_2\, X_4\, X_5\, X_6]^T = \mathbf{C}_3 \cdot [x_0\, x_4\, x_6\, x_7]^T + \mathbf{C}_4 \cdot [x_1\, x_2\, x_3\, x_5]^T.$$

$\mathbf{C}_1$ é a matriz circulante com primeira linha dada por $[\alpha^{153}\,\alpha^{51}\,\alpha^{102}\,\alpha^{204}]$; permutando a segunda e terceira linhas de $\mathbf{C}_3$, obtém-se a matriz circulante com primeira linha dada por $[\alpha^{136}\,\alpha^{68}\,\alpha^{34}\,\alpha^{17}]$. Além disso,

$$\mathbf{C}_2 = \begin{bmatrix} \alpha^{136} & \alpha^{34} & \alpha^{68} & \alpha^{17} \\ \alpha^{17} & \alpha^{68} & \alpha^{136} & \alpha^{34} \\ \alpha^{34} & \alpha^{136} & \alpha^{17} & \alpha^{68} \\ \alpha^{68} & \alpha^{17} & \alpha^{34} & \alpha^{136} \end{bmatrix}; \mathbf{C}_4 = \begin{bmatrix} \alpha^{204} & \alpha^{51} & \alpha^{102} & \alpha^{153} \\ \alpha^{51} & \alpha^{204} & \alpha^{153} & \alpha^{102} \\ \alpha^{153} & \alpha^{102} & \alpha^{204} & \alpha^{51} \\ \alpha^{102} & \alpha^{153} & \alpha^{51} & \alpha^{204} \end{bmatrix}.$$

O produto envolvendo $\mathbf{C}_1$ corresponde a uma convolução cíclica de 4-pontos entre $[\alpha^{153}\,\alpha^{51}\,\alpha^{102}\,\alpha^{204}]$ e $[x_0\, x_4\, x_6\, x_7]$, a qual pode ser calculada por meio do algoritmo descrito na

Tabela 2 de [5]. Observando que $\alpha^{153}+\alpha^{51}+\alpha^{102}+\alpha^{204}=1$, tal operação requer 15 adições e 5 multiplicações. Um procedimento análogo pode ser empregado para o cálculo do produto envolvendo $\mathbf{C}_3$. Observando que $\alpha^{136}+\alpha^{34}=1$ e $\alpha^{136}+\alpha^{17}+\alpha^{34}+\alpha^{68}=0$, o referido produto requer 11 adições e 4 multiplicações. Permutando a segunda e a terceira linhas de $\mathbf{C}_2$, obtém-se uma matriz na forma

$$\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}' & \mathbf{A} \end{bmatrix},$$

em que $\mathbf{A}$, $\mathbf{B}$ e $\mathbf{B}'$ são matrizes 2×2, cujo produto por um vetor pode ser calculado de forma eficiente empregando recursivamente o algoritmo descrito na Equação (4) de [5]. Para isso, são necessárias 11 adições e 3 multiplicações. A aplicação de ideia semelhante ao produto relacionado a $\mathbf{C}_4$ envolve 10 adições e 4 multiplicações.

Incluindo algumas adições extras, é necessário um total de 55 adições e 16 multiplicações para calcular a FFCT com 8-pontos construída nesta seção. Embora o total de adições permaneça praticamente o mesmo em comparação àquele necessário ao produto matriz-vetor sem utilização do algoritmo ($7\times 8=56$), o número de multiplicações é substancialmente diminuído; mais precisamente, realizando o cálculo direto, um número de multiplicações quatro vezes maior é necessário.

IV. FFCT com 32-pontos sobre $\mathrm{GF}(2^{24})$

O corpo finito $\mathrm{GF}(2^{24})$, sobre o qual se define a FFCT considerada nesta seção, é construído utilizando $p(x)=x^{24}+x^7+x^2+x+1$, tendo α como raiz, com $\mathrm{ord}(\alpha)=2^{24}-1$. Para definir uma transformada com $N-1=32$ pontos, emprega-se o elemento $\zeta=\alpha^{258111}$, uma vez que $\mathrm{ord}(\zeta)=\mathrm{ord}(\alpha^{258111})=(2^{24}-1)/258111=65=2N-1$.

Em função da limitação de páginas, neste trabalho, não se apresenta a matriz $\mathbf{C}$ propriamente dita da FFCT obtida. De qualquer modo, a aplicação desta transformada a uma estrutura matricial $\mathbf{m}$ (um bloco de imagem digital, por exemplo) corresponde ao cálculo de

$$\mathbf{M}=\mathbf{C}\cdot\mathbf{m}\cdot\mathbf{C}^T. \tag{3}$$

Como a matriz $\mathbf{C}$ da FFCT em questão possui estrutura similar àquela construída na Seção III, é possível efetuar o produto matricial da Equação (3) por meio de um algoritmo rápido semelhante ao desenvolvido na referida seção.

A. Aplicação em Processamento de Imagem

Nesta subseção, é ilustrada a aplicação da FFCT sobre $\mathrm{GF}(2^{24})$ em processamento de imagem. Considera-se uma imagem RGB, denotada por $\mathbf{I}$, e justapõe-se os bytes referentes a cada uma das três camadas de cor, de maneira que, a cada pixel, associa-se um número binário com 24 bits. Esses números são, então, mapeados diretamente em elementos de $\mathrm{GF}(2^{24})$, formando uma matriz que representa uma espécie de *camada unificada de cores*. Essa matriz é dividida em submatrizes com dimensões 32×32, às quais é aplicada a versão bidimensional da FFCT construída. Finalmente, a partir da matriz resultante deste processo, são obtidas as camadas R, G e B que compõem a versão transformada da imagem ($\mathbf{I}_t$).

Dada $\mathbf{I}_t$, é possível o retorno a $\mathbf{I}$ usando a FFCT inversa. Como as operações aritméticas envolvidas neste processo não requerem arredondamentos, a imagem recuperada é idêntica a $\mathbf{I}$. Todo o processo fora simulado em uma rotina escrita em *Python*, envolvendo a biblioteca de manipulação de imagens *PIL*. O resultado da aplicação da FFCT à imagem *lena.bmp* com dimensões 512×512 (Figura 1a) é apresentado na Figura 1b. Nesta última imagem, observa-se que o conteúdo visual da imagem original foi completamente comprometido.

Observando as Figuras 1c e 1d, verifica-se que, embora as camadas de cor na imagem original tenham histogramas com formatos específico, após a aplicação da FFCT, esses são uniformizados, *escondendo* o conteúdo estatístico da imagem. Isso se reflete no valor da correlação entre pixels vizinhos, que é próximo de 1 na imagem original e próximo de 0 na imagem transformada, e na entropia de cada camada de cor da imagem transformada, que é aproximadamente igual a 8.

V. Considerações Finais

Neste trabalho, foram apresentadas construções de transformadas do cosseno sobre corpos de característica 2. Para a FFCT com 8-pontos definida sobre $\mathrm{GF}(2^8)$, foi apresentado um algoritmo rápido. Para a FFCT com 32-pontos definida sobre $\mathrm{GF}(2^{24})$, foi descrita uma aplicação em processamento de imagem. Os resultados indicam que a FFCT pode ser empregada em esquemas de cifragem como aquele proposto em [4]. Atualmente, têm sido estudadas propriedades das FFCT e desenvolvidas implementações dessas transformadas numa plataforma de *hardware* reconfigurável.

Referências

[1] R. E. Blahut, *Fast Algorithms for Signal Processing*. Cambridge University Press, 2010.

[2] R. M. Campello de Souza e H. M. de Oliveira, "The complex Hartley transform over a finite field," in *Coding, Communications and Broadcasting* (P. G. Farnell, M. Darnell, e B. Honary, eds.), p. 267–276, Hertfordshire: Research Studies Press, Jonh Wiley, 1st ed., 2000.

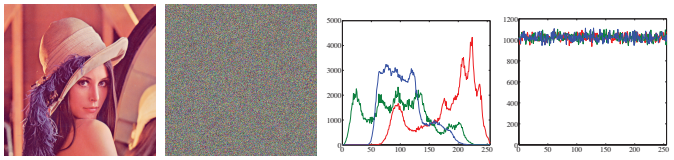
[3] R. J. Cintra, V. S. Dimitrov, R. M. Campello de Souza, e H. M. de Oliveira, "Fragile watermarking using finite field trigonometrical transforms," *Sig. Proc.: Image Comm.*, vol. 24, p. 587–597, 2009.

[4] J. B. Lima, F. Madeiro, e F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Sig. Proc.: Image Comm.*, vol. 35, p. 1–8, July 2015.

[5] T. K. Truong, P. D. Chen, L. J. Wang, e I. S. Reed, "Fast, prime factor, discrete Fourier transform algorithms over $\mathrm{GF}(2^m)$ for $8\leq m\leq 10$," *Information Sciences*, vol. 176, p. 1–26, January 2006.

[6] J. B. Lima e R. M. Campello de Souza, "Finite field trigonometric transforms," *Applicable Algebra in Engineering, Communication and Computing*, vol. 22, p. 393–411, December 2011.

[7] J. B. Lima, M. Barone, e R. M. Campello de Souza, "Cosine transforms over fields of characteristic 2," *submetido a "Finite Fields and Their Applications"*, 2015.



(a) (b) (c) (d)

Fig. 1: (a) versão original e (b) versão transformada de *lena.bmp*; (c) e (d), respectivos histogramas de cada camada de cor das imagens.