Representação Numérica em Inteiros de Gauss-Eisenstein

D. F. G. Coelho R. J. Cintra L. C. Souza A. Madanayake V. S. Dimitrov

***Resumo*— Este artigo apresenta uma nova representação inteira para números complexos usuais. É mostrado que as raízes da cúbica e sexta da unidade são representadas sem erro empregando apenas os inteiros $\{0, \pm 1\}$. Este resultado torna promissor o uso da representação proposta em algoritmos para a DFT de comprimento 3 e 6.**

***Palavras-Chave*— Transformada discreta de Fourier, inteiros algébricos, inteiros gaussianos, inteiros de Eisenstein.**

***Abstract*— This paper presents a new integer representation for usual complex numbers. We show that the 3rd and 6th roots of the unity can be exactly represented using only elements $\{0, \pm 1\}$. Therefore, the 3- and 6-point DFT can be implemented in a multiplication-free framework.**

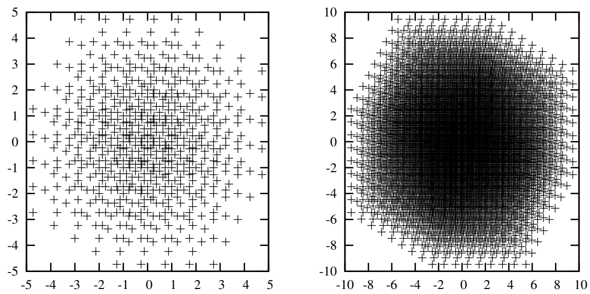
***Keywords*— Discrete Fourier transform, algebraic integers, Gaussian integers, Eisenstein integers**

I. INTRODUÇÃO

Uma representação numérica muito empregada é a de ponto fixo [1], [2]. Embora muito adequada para a representação de números racionais, não é tão adequada para números irracionais. Aproximações na tentativa de representar os números irracionais introduzem erros que podem propagar-se ao longo do sistema [3], decrementando a relação sinal-ruído.

Uma alternativa para representar números irracionais é a codificação usando inteiros algébricos [3]–[5]. A codificação em inteiros algébricos consiste em mapear possíveis números irracionais em vetores de inteiros que podem ser processados em uma estrutura aritmética livre de erro. Técnicas de codificação por inteiros algébricos foram introduzidas no contexto de processamento digital de sinais via o algoritmo paralelizado para a computação da DFT de Cozzens e Finkelstein [6], [7]. Trabalhos recentes contribuíram com diversas arquiteturas relacionadas com inteiros algébricos. Por exemplo, pode-se citar: (i) sistema de processamento de sinais baseado em sistema de resíduos de inteiros de Eisenstein [8], (ii) arquitetura de hardware para transformada discreta do cosseno 2-D 8×8 baseada em inteiros algébricos [3], e (iii) implementação da transformada real ortogonal usando sistema de resíduo numérico [9].

D. Coelho, Programa de Graduação do Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, E-mail: diego.felipe@ufpe.br
R. J. Cintra, Universidade Federal de Pernambuco e University of Akron, E-mail: rjdsc@pq.cnpq.br
L. C. Souza, Programa de Pós-graduação em Estatística, Universidade Federal de Pernambuco.
A. Madanayake, Department of Electrical and Computer Engineering, University of Akron. E-mail: arjuna@uakron.edu
V. S. Dimitrov, Department of Electrical and Computer Engineering, University of Calgary. E-mail: vdimitro@ucalgary.ca



(a) $N = 2$ (b) $N = 3$

Fig. 1. Inteiros de G-E com elementos de N bits.

Este artigo propõe uma nova representação numérica que é resultado de uma combinação da estrutura dos inteiros gaussianos e os de Eisenstein. A nova representação é denominada de representação em inteiros de Gauss-Eisenstein.

II. REPRESENTAÇÃO DE INTEIROS DE GAUSS-EISENSTEIN

Definição 1: Seja $j = \sqrt{-1}$. Um inteiro gaussiano é um número complexo $a_0 + a_1 j$, em que a_0 e a_1 são inteiros usuais.

Definição 2: Um inteiro de Gauss-Eisenstein (G-E) ζ é definido como

$$\zeta = z_1 + z_2\omega,$$

em que $z_1 = a_0 + a_1 j$ e $z_2 = a_2 + a_3 j$ são inteiros gaussianos e $\omega = \frac{-1+j\sqrt{3}}{2}$ é uma raiz cúbica da unidade.

É possível demonstrar que os inteiros de G-E formam um conjunto denso no conjunto dos complexos. Contudo, para uma representação arbitrariamente precisa, os inteiros que formam a representação dos inteiros de G-E não devem ter restrições em magnitude. Este é um problema de implementação, dado que é possível representar apenas inteiros de tamanho finito.

Restrinjamos a escolha dos coeficientes dos inteiros de G-E tais que $|a_i| \leq M$, para $i = 0, 1, 2, 3$, em que M é um inteiro positivo. Convenientemente escolhendo M como uma potência de 2, sendo N o número de bits usados para representar M, temos que $M = 2^N - 1$. A Figura 1 exibe os pontos que representam os inteiros de G-E para 2 e 3 bits em cada coeficiente. É notável o fato de que a densidade de pontos próximo da origem é maior do que na região da fronteira do octógono circunscrito.

A. *Operações Aritméticas*

Sejam $\zeta_1 = a_0 + a_1 j + a_2\omega + a_3 j\omega$ e $\zeta_2 = b_0 + b_1 j + b_2\omega + b_3 j\omega$ dois inteiros de G-E, em que a_i e b_i são inteiros para

TABELA I

MULTIPLICAÇÕES TRIVIAIS POR $\zeta = a_0 + a_1 j + a_2\omega + a_3 j\omega$

$1 \cdot \zeta$	$a_0 + a_1 j + a_2\omega + a_3 j\omega$
$j \cdot \zeta$	$-a_1 + a_0 j - a_3\omega + a_2 j\omega$
$\omega \cdot \zeta$	$-a_2 - a_3 j + (a_0 - a_2)\omega + (a_1 - a_3) j\omega$
$j\omega \cdot \zeta$	$a_3 - a_2 j + (a_3 - a_1)\omega + (a_0 - a_2) j\omega$

$0 \leq i \leq 3$. A operação de adição é definida

$$\begin{aligned}\zeta_1 + \zeta_2 = {} & (a_0 + b_0) + (a_1 + b_1)j \\ & + (a_2 + b_2)\omega + (a_3 + b_3)j\omega\end{aligned}$$

e o produto entre dois inteiros de G-E pode ser definido como

$$\begin{aligned}\zeta_1 \cdot \zeta_2 = {} & a_0 b_0 - a_1 b_1 - a_2 b_2 + a_3 b_3 \\ & + (a_0 b_1 + a_1 b_0 - a_2 b_3 - a_3 b_2) j \\ & + (a_0 b_2 - a_1 b_3 + a_2 b_0 - a_3 b_1 - a_2 b_2 - a_3 b_3)\omega \\ & + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 - a_2 b_3 - a_3 b_2) j\omega.\end{aligned}$$

Embora computando o produto diretamente como na definição possa gerar vinte produtos reais e dezoito adições, é possível reduzir a complexidade multiplicativa para apenas nove produtos reais em detrimento do crescimento do número de somas para vinte e uma.

Um caso importante é quando um dos operandos do produto é um elemento da nova base $\{1, j, \omega, j\omega\}$. Nesta situação, o resultado pode ser obtido por apenas permutações e somas dos elementos, como mostrado na Tabela I.

III. CODIFICAÇÃO

O processo de codificação de um número complexo usual em sua representação em inteiro de G-E pode ser feito em dois passos. Primeiro, arredonda-se o complexo a ser codificado para o inteiro gaussiano mais próximo. Note que a norma máxima do erro de aproximação de um complexo em um inteiro gaussiano é menor ou igual a $\sqrt{2}/2$. Em seguida, adiciona-se a esta primeira aproximação o inteiro de G-E que mais se aproxime da diferença. É suficiente buscar entre os inteiros de G-E de norma menor ou igual que $\sqrt{2}/2$.

A Tabela II exibe a codificação de algumas raízes da unidade na representação em inteiros de G-E e seus respectivos erros de representação. São usados 5 bits para cada inteiro. As raízes da unidade são de fundamental importância por surgirem naturalmente na definição da DFT que exige potências de $\exp\{2\pi j/N\}$.

IV. TRANSFORMADA DISCRETA DE FOURIER

Os coeficientes da DFT para alguns comprimentos são *exatamente* representados em termos de inteiros de G-E. Isso elimina os erros introduzidos na computação da transformada, ao mesmo tempo que evita a sua propagação. Além disso, toda a computação da DFT se resume a cálculos realizados com os coeficientes da representação de G-E, que são inteiros usuais. Usando as propriedades das multiplicações triviais dada pela Tabela I mostra-se que todos os elementos da matriz de transformação da DFT de comprimento 3 e 6 podem ser codificados exatamente empregando apenas os inteiros $\{0, \pm 1\}$.

TABELA II

A N-ÉSIMA RAIZ DA UNIDADE NA REPRESENTAÇÃO DE GAUSS-EISENSTEIN

Raiz	a_0	a_1	a_2	a_3	Norma do erro
1	1	0	0	0	0
-1	-1	0	0	0	0
$\exp\{2\pi j/3\}$	0	0	1	0	0
j	0	1	0	0	0
$\exp\{2\pi j/5\}$	28	-5	19	21	5.61×10^{-3}
$\exp\{2\pi j/6\}$	0	0	-1	0	0

V. CONCLUSÕES

Uma nova representação para números complexos foi introduzida. Esta nova representação pode ser usada para o projeto de algoritmos de complexidade multiplicativa nula para a DFT comprimento 3 e 6.

AGRADECIMENTOS

Os autores agradecem ao suporte parcial dada pelo CNPq e pela FACEPE.

REFERÊNCIAS

[1] K. A. Wahid, V. S. Dimitrov, G. A. Jullien, and W. Badawy, "Error-free computation of daubechie: wavelets for image compression applications," *Electronic Letters*, vol. 39, pp. 428–429, April 2003.

[2] R. J. Cintra and V. S. Dimitrov, "The arithmetic cosine transform: exact and approximate algorithms," *IEEE Transactions on Signal Processing*, vol. 58, pp. 3076–3085, June 2010.

[3] M. A., R. J. Cintra, D. Onen, V. S. Dimitrov, N. T. Rajapaksha, L. T. Bruton, and A. Edirisuriya, "A row-parallel 8 × 8 2-D DCT architecture using algebraic integer based exact computation," *IEEE Transaction on Circuit and Systems for Video Technology*, vol. 99, pp. 1–1, December 2011.

[4] X. dong Dong, C. B. Soh, E. Gunawan, and L. zhong Tang, "Groups of algebraic integers used for coding QAM signals," *IEEE Transactions no Information Theory*, vol. 44, no. 5, 1998.

[5] E. Dubois and A. Venetsanopoulos, "The generalized discrete Fourier transform in rings of algebraic integers," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 28, pp. 169–175, Apr. 1980.

[6] J. H. Cozzens and L. A. Finkelstein, "Computing the discrete Fourier transform using residue number systems in a ring of algebraic integers," *IEEE Transactions on Information Theory*, vol. 31, no. 5, pp. 580–588, 1985.

[7] J. H. Cozzens and L. A. Finkelsteinn, "Range and error analysis for a fast Fourier transform computed over Z[ω]," *IEEE Transactions on Information Theory*, 1987.

[8] V. Dimitrov, G. Jullien, and W. Miller, "Eisenstein residue number system with applications to DSP," vol. 2, pp. 675–678, August 1997.

[9] V. S. Dimitrov, G. A. Jullien, and W. C. Miller, "A residue number system implementation of real orthogonal transforms," *IEEE Transactions on Signal Processing*, vol. 46, pp. 563–570, March 1998.