TRANSFORMADAS EM CORPOS FINITOS

E GRUPOS DE INTEIROS GAUSSIANOS

D. Silva, R.M. Campello de Souza, H.M. de Oliveira

CODEC - Grupo de Pesquisas em Comunicações
Departamento de Eletrônica e Sistemas - CTG - UFPE
C.P. 7800, 50711-970, Recife-PE, Brazil
E-mail: danilo_s@uol.com.br, ricardo@npd.ufpe.br, hmo@npd.ufpe.br

RESUMO

Transformadas discretas desempenham um importante papel em muitas aplicações em Engenharia Elétrica. Especificamente, transformadas discretas definidas sobre corpos finitos são atraentes por não introduzirem erros de truncagem ou arredondamento, e por permitirem aplicações com aritmética de baixa complexidade. Neste artigo, algumas estruturas algébricas finitas relacionadas com a Transformada de Hartley de Corpo Finito são introduzidas. Em particular, os grupos dos módulos e das fases de um corpo finito são introduzidos e a representação polar dos elementos do corpo finito $GF(p^2)$ é definida. Aplicações envolvendo a Transformada Numérica de Hartley são apresentadas.

1. INTRODUÇÃO

Transformadas Discretas definidas sobre corpos finitos são ferramentas que, embora recentes, desempenham um papel importante em Engenharia. A transformada de Fourier em um corpo finito foi introduzida em [1] como uma ferramenta para efetuar convoluções discretas finitas usando aritmética inteira. Recentemente, a transformada de Hartley sobre corpos finitos foi introduzida [2], a qual apresenta propriedades de simetria que a tornam mais atraente, para diversas aplicações, que a transformada de Fourier de corpo finito, e tem importantes aplicações no campo da multiplexação digital [3].

Transformadas em corpos finitos que mapeiam vetores com elementos em GF(p) e, portanto, empregam aritmética modulo p, são chamadas transformadas numéricas. Tais transformadas não provocam erros de arredondamento ou truncagem e tem, em muitos casos de interesse, uma implementação em *hardware* consideravelmente simples. Um exemplo bem conhecido de uma tal Transformada é a Transformada Numérica de Fourier [4]. Um outro exemplo mais recente é a chamada Transformada Numérica de Hartley [5], a qual é construída a partir da Transformada de Hartley de Corpo Finito.

Neste artigo, algumas estruturas algébricas finitas relacionadas com a transformada de Hartley de Corpo Finito são introduzidas. Em particular, os grupos dos módulos e das fases de um corpo finito são introduzidos e uma representação polar dos elementos do corpo finito $GF(p^2)$ é definida. Aplicações envolvendo a Transformada Numérica de Hartley são apresentadas. Na próxima seção é introduzida a idéia de uma representação polar para corpos finitos. Isto requer uma nova definição de módulo que seja adequada para os elementos de um corpo finito $GF(p^2)$, a qual é obtida vinculando-se o módulo do elemento à condição de resíduo quadrático módulo p. Na seção 3 o conceito de grupo unimodular é estendido e a estrutura algébrica denominada grupo supra-unimodular é definida e algumas de suas propriedades investigadas. Aplicações dos conceitos introduzidos são consideradas na seção 4 no contexto das transformadas numéricas. A seção 5 apresenta as conclusões do trabalho.

2. FORMA POLAR PARA INTEIROS GAUSSIANOS EM CORPOS FINITOS

É um fato bem conhecido, na aritmética usual dos números complexos, que a chamada representação polar apresenta aspectos que a tornam atraente em muitas aplicações, principalmente quando as operações usuais de multiplicação e exponenciação estão presentes. Mantendo este mesmo ponto de vista, e objetivando a implementação de uma aritmética módulo p mais eficiente, uma representação polar para os elementos do corpo finito $GF(p^2)$ é proposta nesta seção. Inicialmente os inteiros gaussianos sobre o corpo finito GF(p) são definidos.

Definição 1 - O conjunto dos inteiros gaussianos sobre GF(p) é o conjunto $G(p) = \{a + jb, a, b \in GF(p)\}$, onde p

é um primo para o qual $j^2 = -1$ é um resíduo não-quadrático em GF(p).
Apenas os primos da forma $p \equiv 3 \pmod 4$ satisfazem esse requisito [6]. Seja $\otimes$ o produto cartesiano. Pode-se mostrar que G(p), juntamente com as operações $\oplus$ e *, é um corpo.

Proposição 1 – Sejam $\oplus$ e * operações definidas por
$\oplus : G(p) \otimes G(p) \rightarrow G(p)$
$(a + jb, c + jd) \rightarrow (a + jb) \oplus (c + jd) = (a + c) + j(b + d)$
e
$* : G(p) \otimes G(p) \rightarrow G(p)$
$(a + jb, c + jd) \rightarrow (a + jb) * (c + jd) = (ac - bd) + j(ad + bc)$.
A estrutura GI(p) := <G(p); $\oplus$, *> é um corpo. De fato, GI(p) é isomorfo a $GF(p^2)$ [4].

Na definição de GI(p) acima, os elementos são representados na forma a + jb, que é chamada de forma retangular. No que se segue, é proposta uma nova representação que permite escrever os elementos do grupo multiplicativo de GI(p) na forma $r\varepsilon^{\theta}$. Por analogia com o contínuo, esta representação será chamada de polar.

Proposição 2 - Sejam G_A e G_B subgrupos do grupo multiplicativo G_C dos elementos não nulos de GI(p), de ordens $N_A=(p-1)/2$ e $N_B=2(p+1)$, respectivamente. Todos os elementos de GI(p), com exceção do zero, podem ser escritos na forma $\zeta = AB$, onde $A \in G_A$ e $B \in G_B$.
Prova: Sendo G_C um grupo cíclico, então os subgrupos G_A e G_B de GI(p) existem, pois N_A e N_B são divisores de p^2-1, a ordem do grupo multiplicativo de GI(p). Além disso, o grupo G_Z formado pelo produto direto [9] entre os grupos G_A e G_B, tem ordem p^2-1, uma vez que, como p é da forma 4k+3, então o máximo divisor comum entre N_A e N_B satisfaz $MDC(N_A, N_B) = MDC(2k+1, 4(2k+2)) = 1$; ou seja, o número de elementos de G_Z, que é dado pelo mínimo múltiplo comum das ordens de G_A e G_B, é $|G_Z| = mmc(|G_A|, |G_B|) = N_A N_B = p^2-1$. Assim, G_Z é o próprio grupo multiplicativo de GI(p), ou seja, todos os elementos deste último grupo podem ser escritos na forma $\zeta = AB$, onde $A \in G_A$ e $B \in G_B$. $\in$

Tendo em vista que qualquer elemento de um grupo cíclico pode ser escrito como potência de um elemento gerador desse grupo, podemos fazer $r = A$ e $\varepsilon^{\theta} = B$, onde ε é um gerador de G_B. Assim, a representação polar adquire a forma procurada, $\zeta = r\varepsilon^{\theta}$.

Antes de prosseguir com as propriedades da representação polar, precisamos introduzir o conceito de módulo de um elemento em um corpo finito. Considerando os elementos não nulos de GF(p), metade deles possui raiz quadrada e são chamados de resíduos quadráticos (RQ) de p [6]. Os que não possuem são chamados de resíduos não-quadráticos (RNQ). Da mesma forma, no corpo infinito dos reais, os números são divididos em postivos e negativos, que são, respectivamente, os que possuem e os que não possuem raiz quadrada. A operação convencional de módulo, nos reais, produz sempre um resultado positivo. Por analogia, definiremos a operação de módulo em GF(p) para que produza sempre um resíduo quadrático.

Definição 2 - O módulo de um elemento de GF(p), onde p=4k+3, é dado por:

$$|a| = \begin{cases} a, & \text{se } a^{\frac{p-1}{2}} \equiv 1 \pmod p \\ -a, & \text{se } a^{\frac{p-1}{2}} \equiv -1 \pmod p \end{cases}$$

Proposição 3 - O módulo de qualquer elemento de GF(p) é sempre um resíduo quadrático.
Prova: Como p=4k+3, temos que (p-1)/2=2k+1, e portanto $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$. Pelo critério de Euler [6], se $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, então a é um RQ de p; se $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, então a é um RNQ. No caso, $(-a)^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 \pmod p$, e segue-se portanto que -a é um RQ de p. $\in$

Definição 3 - O módulo de um elemento de GI(p), onde p=4k+3, é dado por:

$$|a + jb| = \left|\sqrt{|a^2 + b^2|}\right|$$

O módulo interior na expressão acima é necessário para que sempre se possa extrair a raiz quadrada da norma a^2+b^2, e o módulo exterior garante que essa operação forneça um único resultado apenas. No contínuo, essas expressões se reduzem às conhecidas, pois tanto a^2+b^2 quanto a operação de raiz quadrada fornecem apenas resíduos quadráticos.

Nesse ponto, podemos substituir G_A e G_B por denominações mais adequadas à representação polar.

Definição 4 - O grupo dos módulos de GI(p), denotado por G_r, é definido como sendo o subgrupo de ordem (p-1)/2 de GI(p).

Definição 5 - O grupo das fases de GI(p), denotado por G_θ, é definido como sendo o subgrupo de ordem 2(p+1) de GI(p).

Proposição 4 - Se $\zeta = a + jb = r\varepsilon^{\theta}$, onde $r \in G_r$ e $\varepsilon^{\theta} \in G_{\theta}$, então $r = |\zeta|$.
Prova: Todos os elementos de G_r possuem ordem que divide (p-1)/2. Assim, se $r \in G_r$, então $r^{\frac{p-1}{2}} \equiv 1 \pmod p$, e portanto $|r|=r$. Além disso, como mostrado na seção seguinte, o grupo G_{θ} é formado pelos elementos a+jb tais que $a^2 + b^2 \equiv \pm 1 \pmod p$. Portanto, de acordo com a definição 3, o módulo desses elementos é igual a 1. Temos então que $|\zeta| = |r\varepsilon^{\theta}| = |r||\varepsilon^{\theta}| = r \cdot 1 = r$. €

Uma expressão para a fase θ em função de a e b pode ser encontrada normalizando-se o elemento ($\zeta/r = \varepsilon^{\theta}$), e em seguida resolvendo-se o problema do logaritmo discreto de ζ/r na base ε, que é viável para valores não muito elevados de p. Assim, é possível a conversão da representação retangular para a polar. A conversão inversa é feita simplesmente efetuando-se as potenciações.

Como se pode observar, a representação proposta é consistente com a representação polar no contínuo: o módulo r pertence a GF(p) (o módulo é um número real) e é um resíduo quadrático (número positivo), e a componente exponencial ε^{θ} ($e^{j\theta}$) tem módulo 1 e pertence a GI(p) ($e^{j\theta}$ pertence ao corpo dos complexos).

3. GRUPOS SUPRA-UNIMODULARES

Um subconjunto de GI(p) já estabelecido na literatura [5] é o conjunto unimodular, definido a seguir.

Definição 6 - O conjunto unimodular de GI(p), denotado por G_U, é o conjunto dos elementos $\zeta = a+jb \in GI(p)$ que satisfazem $a^2 + b^2 \equiv 1 \pmod p$.

É possível provar que, juntamente com a operação de multiplicação, esse conjunto forma um grupo cíclico de ordem p+1 [5].

Definição 7 - O conjunto supra-unimodular de GI(p), denotado por G_S, é o conjunto dos elementos $\zeta = a + jb \in GI(p)$ tais que $(a^2 + b^2)^2 \equiv 1 \pmod p$.

Proposição 5 - Se $\zeta = a + jb$, então $\zeta^{2(p+1)} \equiv (a^2 + b^2)^2 \pmod p$.
Prova - $\zeta^p = (a + jb)^p \equiv a^p + j^p b^p \pmod p$, pois GI(p) é isomorfo a $GF(p^2)$, um corpo de característica p. Como $p = 4k+3$, $j^p=-j$, de modo que $\zeta^p \equiv a - jb \pmod p$. Portanto, $\zeta^{p+1} \equiv (a + jb)(a - jb) \equiv a^2 + b^2 \pmod p$. Assim, $\zeta^{2(p+1)} \equiv (a^2 + b^2)^2 \pmod p$. €

Proposição 6 – A estrutura $<G_S,*>$, denominada supra-unimodular, é um grupo cíclico de ordem 2(p+1).

Prova: G_S é fechado em relação à multiplicação, pois se (a+jb) e (c+jd) estão em G_S, isto é, se

$$(a^2 + b^2)^2 \equiv (c^2 + d^2)^2 \equiv 1 \pmod p,$$

então

$$e + jf = (a + jb)(c + jd) = (ac - bd) + j(ad + bc).$$

Deste modo

$$(e^2 + f^2)^2 = (a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2)^2 =$$
$$= ((a^2 + b^2)(c^2 + d^2))^2 = (a^2 + b^2)^2(c^2 + d^2)^2 \equiv 1 \pmod p,$$

e portanto $(e + jf) \in G_S$. Como G_S é um subconjunto fechado de um grupo cíclico (o grupo multiplicativo de GI(p)), G_S é um subgrupo cíclico. Além disso, da proposição 5, $\zeta \in G_S$ satisfaz $\zeta^{2(p+1)} \equiv 1 \pmod p$. Assim, ζ é uma das raízes 2(p+1)-ésimas da unidade em GI(p). Existem 2(p+1) tais raízes e portanto G_S tem ordem 2(p+1). €

Reconhece-se que no grupo supra-unimodular os elementos $\zeta = a + jb$ são tais que $(a^2 + b^2)^2 \equiv 1 \pmod p$, ou seja, $a^2 + b^2 \equiv \pm 1 \pmod p$, e portanto todos têm módulo igual a 1, assim como no grupo unimodular. Porém, para preservar a definição já estabelecida e ressaltar que o mesmo possui ordem maior, o grupo de ordem 2(p+1) recebeu o nome de supra-unimodular. É importante observar que, devido ao fato de que um grupo cíclico não possui mais de um subgrupo distinto de mesma ordem [8], o grupo supra-unimodular é exatamente o grupo das fases definido na seção anterior.

O problema de encontrar um elemento gerador do grupo supra-unimodular é tratado a seguir.

Proposição 7 - Se p é um primo de Mersenne, isto é, um primo da forma $p = 2^n - 1$, então os elementos $\zeta=a+jb$ tais que $a^2+b^2 \equiv -1 \pmod p$ são geradores do grupo supra-unimodular de GI(p).
Prova. Seja N a ordem do elemento ζ. Como $a^2+b^2 \equiv -1 \pmod p$, ζ é um elemento supra-unimodular, ou seja, N divide $2(p+1)=2^{n+1}$. Entretanto, pelo mesmo motivo, ζ não é unimodular, isto é, N não divide $p+1=2^n$. Dessa forma, $N = 2^{n+1} = 2(p+1)$, e portanto ζ é um gerador do grupo supra-unimodular. €

Assim, se p for um primo de Mersenne, um elemento de ordem 2(p+1) em GI(p) pode ser encontrado da seguinte forma: escolhe-se um elemento aleatório de GI(p), divide-se este elemento por seu módulo, e por fim calcula-se sua norma (a^2+b^2). Se o resultado for -1, tem-se o elemento desejado; caso contrário, repete-se o processo.

3. APLICAÇÕES

Desde a introdução da transformada de Fourier em corpo finito, concebida inicialmente para auxiliar o cálculo de convoluções discretas, muitas outras aplicações da mesma foram propostas, não apenas nas áreas de processamento digital de sinais e imagem [9], mas também em diferentes contextos tais como codificação de canal e criptografia [10-12]. Um outro exemplo relevante é a transformada discreta de Hartley (DHT) introduzida em 1983 [13], que tem se mostrado um instrumento útil com muitas aplicações interessantes [14-18].

Recentemente, uma versão da DHT para corpos finitos (a transformada de Hartley de corpo finito – THCF) foi introduzida [2], a qual tem importantes aplicações no campo da multiplexação digital [3]. Uma THCF de especial interesse é a chamada Transformada Numérica de Hartley (TNH), a qual é construída a partir de uma escolha apropriada do núcleo da THCF, escolha esta que resulta em uma transformada com componentes em GF(p). Dessa forma, não é necessário restringir o corpo de extensão a GF(p) para se obter uma transformada numérica, o que é feito para a Transformada Numérica de Fourier (TNF). Neste caso, isto significa que N, o comprimento da transformada, é um divisor de $(p^2-1) = (p-1)(p+1)$ e não apenas de (p-1) como no caso da TNF. Assim, para um dado p, a TNH apresenta uma maior flexibilidade de aplicação em relação à TNF, uma vez que um número maior de escolhas para o valor de N, o comprimento da transformada, é possível.

Um caso particular de interesse prático da TNH é obtido quando p é um primo de Mersenne, isto é, um primo da forma $p=2^s-1$. As transformadas correspondentes, denominadas Transformadas Numéricas de Hartley-Mersenne, permitem implementações com complexidade multiplicativa nula, bem como comprimentos que permitem a utilização da FFT de Cooley-Tukey, algo que não é possível para a Transformada Numérica de Fourier, uma vez que $p-1 = 2^s-2$ não admite potências não triviais de 2 como divisores [19].

A TNH, sendo uma transformada de Hartley em corpo finito, emprega como núcleo a função trigonométrica cas(.) sobre um corpo finito definida a seguir.

Definição 8 - Seja ζ um elemento de ordem N de GI(p). As funções trigonométricas seno, cosseno e cas sobre GI(p) são definidas a seguir [2]:

$$\cos(x) = \frac{1}{2}\left(\zeta^x + \zeta^{-x}\right),$$

$$\operatorname{sen}(x) = \frac{1}{2j}\left(\zeta^x - \zeta^{-x}\right),$$

$$cas(x) = \cos(x) + \operatorname{sen}(x) = \frac{1}{2}\left((1-j)\zeta^x + (1+j)\zeta^{-x}\right).$$

A função cas(.) é periódica de período N e possui várias propriedades, dentre elas a de ortogonalidade [7]. A partir desta função pode-se definir a TNH [19].

Definição 9 - Seja $v = (v_0, v_1, \ldots, v_{N-1})$ um vetor de comprimento N com componentes em GF(p). A Transformada Numérica de Hartley (TNH) de v é o vetor $V = (V_0, V_1, \ldots, V_{N-1})$ com componentes $V_k \in GF(p)$, relacionadas com os v_i através das expressões

$$V_k = \sum_{i=0}^{N-1} v_i\, cas(ki),$$

$$v_i = \frac{1}{N}\sum_{k=0}^{N-1} V_k\, cas(ki),$$

onde ζ, implícito na definição de cas(.), é um elemento unimodular de ordem N de GI(p). O valor de N é o comprimento da transformada.

Assim, para implementar uma TNH de comprimento N, é necessário primeiramente encontrar um elemento unimodular de ordem N de GI(p). Se p é um primo de Mersenne, isto pode ser feito através do método descrito na seção anterior.

Exemplo 1 - p = 11. Como p não é da forma 2^n-1, o método descrito não resulta necessariamente em geradores de G_S. Temos que 2(p+1) = 24 e (p+1) = 12; assim, os elementos tais que $a^2+b^2 \equiv -1 \pmod p$ possuem ordem 8 ou 24, pois ambos valores dividem 24 mas não dividem 12. Por exemplo, 3 + j tem ordem 24, enquanto 4 + 4j tem ordem 8, apesar de ambos possuírem norma igual a -1.

Exemplo 2 - p = 31 (primo de Mersenne). Como $p = 2^5-1$, pode-se usar o método descrito. Escolhe-se aleatoriamente um elemento de GI(p), por exemplo, $\zeta = 9 + 11j$, após o que seu módulo é calculado através da definição 3: $r = \left|\sqrt{\left|9^2+11^2\right|}\right| \equiv \left|\sqrt{|16|}\right| \equiv |4| \equiv 4 \pmod p$. Em seguida o elemento é normalizado: $\varepsilon = \zeta/r = 10 + 26j$. Finalmente, sua norma é calculada: $a^2+b^2 = 10^2 + 26^2 \equiv 1 \pmod{31}$. Escolhendo um novo elemento, por exemplo, $\zeta = 6 + 16j$, tem-se que

$$r = \left|\sqrt{\left|6^2+16^2\right|}\right| \equiv \left|\sqrt{|13|}\right| \equiv \left|\sqrt{18}\right| \equiv |7| \equiv 7 \pmod p,$$

$\varepsilon = \zeta/r = 23 + 20j$ e $a^2+b^2 = 6^2 + 16^2 \equiv -1 \pmod p$. Portanto, ε tem ordem 2(p+1) = 64. Um elemento unimodular β de ordem N, tal que $N \mid 2^5$, pode ser encontrado fazendo-se $\beta = \varepsilon^{\frac{2(p+1)}{N}} = \varepsilon^{\frac{64}{N}}$.

Por exemplo, $\beta = \varepsilon^2 = 5 + 21j$ é unimodular de ordem 32; assim, pode ser usado como núcleo de uma TNH de comprimento 32.

5. CONCLUSÕES

As chamadas Transformadas Numéricas relacionam vetores com componentes no corpo finito GF(p) e, assim, empregam aritmética módulo p. Embora com características interessantes sob o ponto de vista de sua implementação, a Transformada Numérica de Fourier tem um comprimento N que é um divisor de (p-1), o que limita a escolha dos comprimentos e aplicações possíveis. Por outro lado, a Transformada Numérica de Hartley, introduzida recentemente, permite valores de N que são divisores de (p-1)(p+1), de modo que, para um dado p, um número maior de escolhas para o valor de N é possível.

Neste artigo, algumas estruturas algébricas finitas, relacionadas com a Transformada Numérica de Hartley e relevantes para sua concepção, são introduzidas. Em particular, os grupos dos módulos e das fases de um corpo finito são definidos e, através de uma nova definição de módulo, conveniente para os elementos de um corpo finito GI(p), uma representação polar dos elementos do corpo finito GI(p) é proposta pela primeira vez na literatura. Aplicações dos conceitos introduzidos são consideradas na construção de Transformadas Numérica de Hartley.

REFERÊNCIAS

[1] J. M. Pollard, *The Fast Fourier Transform in a Finite Field*, Mathematics of Computation, vol. 25, No. 114, pp. 365-374, April 1971.

[2] 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 International Symposium on Information Theory, p. 293, Cambridge, MA, August 1998.

[3] H. M. de Oliveira and R. M. Campello de Souza, *Orthogonal Multilevel Spreading Sequence Design*, em *Coding, Communications and Broadcasting*, pp. 291-303, Eds. P. Farrell, M. Darnell and B. Honary, Research Studies Press / John Wiley, 2000.

[4] R. E. Blahut, Fast Algorithms for Digital Signal Processing, Addison Wesley, 1985.

[5] R.M. Campello de Souza, H.M. de Oliveira, L.B.E. Palma e M.M. Campello de Souza, *Hartley Number Theoretic Transforms*, aceito para apresentação no IEEE International Symposium on Information Theory, Washington, junho 2001.

[6] D.M. Burton., *Elementary Number Theory*, Allyn and Bacon, 1976.

[7] A.N. Kauffman, *A Transformada de Hartley em um Corpo Finito e Aplicações*, Dissertação de Mestrado em Engenharia Elétrica, Universidade Federal de Pernambuco, dezembro 1999.

[8] J. R. Dirbin, Modern Algebra: An Introduction, John Wiley, 1992.

[9] I. S. Reed, T. K. Truong, V. S. Kwoh and E. L. Hall, *Image Processing by Transforms over a Finite Field*, IEEE Trans. Comput., vol. C-26, pp. 874-881, Sep. 1977.

[10] R. E. Blahut, *Transform Techniques for Error-Control Codes*, IBM J. Res. Dev., vol. 23, pp. 299-315, May 1979.

[11] R. M. Campello de Souza and P. G. Farrell, *Finite Field Transforms and Symmetry Groups*, Discrete Mathematics, vol. 56, pp. 111-116, 1985.

[12] J. L. Massey, *The Discrete Fourier Transform in Coding and Cryptography*, accepted for presentation at the 1998 IEEE Inform. Theory Workshop, ITW 98, San Diego, CA, Feb 9-11.

[13] R. N. Bracewell, *The Discrete Hartley Transform*, J. Opt. Soc. Amer., vol. 73, pp. 1832-1835, Dec. 1983.

[14] R. N. Bracewell, *The Hartley Transform*, Oxford University Press, 1986.

[15] J.-L. Wu and J. Shiu, *Discrete Hartley Transform in Error Control Coding*, IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-39, pp. 2356-2359, Oct. 1991.

[16] R. N. Bracewell, *Aspects of the Hartley Transform*, IEEE Proc., vol. 82, pp. 381-387, Mar. 1994.

[17] I. Duleba, *Hartley Transform in Compression of Medical Ultrasonic Images*, Proceedings of the 10th International Conference on Image Analysis and Processing, 1998.

[18] C. L. Wang, and C. H. Chang, A Novel DHT-based FFT/IFFT Processor for ADSL Transceivers, Proceedings of the IEEE International Symposium on Circuits and Systems, pp. 51-54, vol. 1, 1999.

[19] L. B. Espínola Silva, *A Transformada Numérica de Hartley*, Dissertação de Mestrado em Engenharia Elétrica, Universidade Federal de Pernambuco, dezembro 2000.