Códigos de Hartley em Corpos Finitos

R. M. Campello de Souza, R. M. Cardim Britto e H. M. de Oliveira

***Resumo*— Uma nova família de códigos corretores de erros multiníveis, chamada de Códigos de Hartley, é introduzida. A matriz de verificação de paridade, a dimensão e uma cota superior para sua distância mínima são obtidas a partir da autoestrutura da transformada numérica de Hartley. Uma subfamília de códigos de taxa ½, denominados códigos de Hartley balanceados, é apresentada.**

Palavras-Chave*— *transformada de Hartley de corpo finito, transformada numérica, autossequências, código de Hartley balanceado.

Abstract— **A new class of non-binary error-correcting codes, called Hartley codes, is introduced. The code parity-check matrix, dimension and an upper bound on its minimum distance are obtained from the eigenstructure of the Hartley number theoretic transform. A subclass of codes with rate ½, namely the balanced Hartley codes, is presented.**

Keywords—finite field Hartley transform, number theoretic transform, eigensequences, balanced Hartley code.

I. INTRODUÇÃO

Transformadas sobre corpos finitos têm sido largamente utilizadas no campo da Engenharia Elétrica para alcançar diferentes metas. Estas transformadas têm aplicações significativas em assuntos como codificação de canal, criptografia e processamento digital de sinais e imagens [1-6].

Neste contexto, a Transformada de Hartley de corpo finito (THCF) é uma ferramenta que apresenta propriedades de simetria interessantes e importantes aplicações no campo da multiplexação digital [7]. Em geral, a THCF é um mapeamento de vetores do campo de Galois GF(q) para sua extensão GF(q^r), em que q é a potência de um primo p^m. Quando $m = r = 1$, obtém-se a transformada numérica de Hartley (TNH) introduzida em [8].

Neste artigo, uma nova família de códigos de bloco lineares não-binários corretores de erros, chamados "Códigos de Hartley", que são baseados na autoestrutura da TNH, é introduzida. As palavras do código são autossequências da TNH. A definição dos autovetores fornece elementos necessários para determinação da matriz de paridade, **H**, do código, cujos parâmetros n (comprimento do bloco), k (dimensão) e uma cota superior da distância mínima de Hamming, d, são obtidos.

Este texto está organizado da seguinte forma. Na próxima seção são apresentadas as tabelas contendo as multiplicidades dos autovalores das transformadas numéricas de Fourier e de Hartley, em função do comprimento das transformadas. Na Seção III, apresenta-se a autoestrutura da TNH, o procedimento de construção dos códigos de Hartley, bem como os parâmetros desses códigos. O artigo é finalizado com algumas conclusões na Seção IV.

II. SOBRE A MULTIPLICIDADE DE AUTOVALORES

A Tabela I apresenta a multiplicidade dos autovalores ($\pm 1, \pm j$) da transformada numérica de Fourier (TNF) [9], [10]. A multiplicidade de λ depende do valor de $\sqrt{N} \equiv \pm b \pmod{p}$. As colunas 2 e 3 ou 4 e 5 podem ser trocadas dependendo do valor considerado (b ou (p-b)) [11].

TABELA I. MULTIPLICIDADE DOS AUTOVALORES DA TNF

N	Mult. de 1	Mult. de -1	Mult. de $-j$	Mult. de j
$4m$	m+1	m	m	m-1
$4m$+1	m+1	m	m	m
$4m$+2	m+1	m+1	m	m
$4m$+3	m+1	m+1	m+1	m

Observando a Tabela I, verifica-se que os códigos gerados a partir da Transformada numérica de Fourier (TNF), assintoticamente, têm taxa ¼.

Na próxima seção é mostrado como são obtidas as tabelas contendo as multiplicidades dos autovalores da TNH. Pelo mesmo motivo relativo aos autovalores da TNF, a tabela que apresenta a multiplicidade dos autovalores da TNH pode ter as colunas 2 e 3 permutadas entre si, gerando valores diferentes de multiplicidade para um mesmo autovalor.

TABELA II. MULTIPLICIDADE DOS AUTOVALORES DA TNH

N	Mult. de 1	Mult. de -1
$4m$	$2m$+1	$2m$-1
$4m$+1	$2m$+1	$2m$
$4m$+2	$2m$+1	$2m$+1
$4m$+3	$2m$+2	$2m$+1

Outro fator que influencia a multiplicidade de cada autovalor é o elemento ζ considerado para a geração da

Ricardo Menezes Campello de Souza, Rafael Menezes Cardim Britto e Hélio Magalhães de Oliveira, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, Brasil, E-mails: ricardo@ufpe.br, mcbrafael@gmail.com, hmo@ufpe.br.

matriz. A Tabela III apresenta outra possibilidade para as multiplicidades dos autovalores da TNH.

TABELA III. MULTIPLICIDADE DOS AUTOVALORES DA TNH

N	Mult. de 1	Mult. de -1
$4m$	$2m$	$2m$
$4m+1$	$2m+1$	$2m$
$4m+2$	$2m+1$	$2m+1$
$4m+3$	$2m+1$	$2m+2$

Como veremos mais adiante, ambas as tabelas sobre a multiplicidade dos autovalores na TNH demonstram que os códigos de Hartley, assintoticamente, têm taxa ½. Em particular, os códigos com parâmetros definidos pela Tabela III têm, quando $N \equiv 0(mod 4)$, taxa igual a ½.

III. CÓDIGOS DE HARTLEY EM CAMPOS DE GALOIS

A. *Autoestrutura da Transformada Numérica de Hartley*

No que se segue GI(q^m) denota o conjunto de inteiros (elementos de corpo finito) da forma $\zeta = a + jb$, em que $a, b \in$ GF(q^m), com $q = p^r$, e $j \in$ GF(q^{2m}), com $j^2 \equiv -1 \pmod p$. Por analogia com os números complexos, os elementos de GF(q^m) e GI(q^m) são ditos reais e complexos, respectivamente.

Definição 1 (Transformada de Hartley de Corpo Finito): Seja $v = (v_0, v_1, \dots, v_{N-1})$ um vetor de comprimento N com componentes em GF(q), em que $q = p^r$, r um inteiro ímpar, e $p \equiv 3 \pmod 4$. O vetor $V = (V_0, V_1, \dots, V_{N-1})$, com componentes em GI($q^m$) dadas por

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

em que ζ é um elemento de ordem N em GI(q^m), é a transformada de Hartley de corpo finito de v.

O núcleo da THCF é a função cas(.) (*cosine and sine*) em um corpo finito, dada por $cas_k(\zeta^i) = cos_k(\zeta^i) + sen_k(\zeta^i)$, em que $cos_k(\zeta^i) = [(\zeta^{ik}) + (\zeta^{-ik})]/2$ e $sen_k(\zeta^i) = [(\zeta^{ik}) - (\zeta^{-ik})]/2j$ são as funções seno e cosseno definidas em um corpo finito [12].

Pode-se construir a TNH a partir da THCF, usando-se a Proposição 1 mostrada a seguir.

Proposição 1: Considerando-se $m = r = 1$, se $\zeta = a + jb$ é o argumento da função cas(.) empregada como núcleo na definição da THCF, então as componentes de V_k pertencem a GF(p) (ou seja, são reais) se $a^2+b^2 \equiv 1 \pmod p$.

Demonstração: Denotando ζ^{ik} por z, as funções seno e cosseno em um corpo finito podem ser reescritas como $cos_k(\zeta^i) = (z + z^{-1})/2$ e $sen_k(\zeta^i) = \frac{z-z^{-1}}{2j}$. Considerando a condição $a^2+b^2 \equiv 1 \pmod p$, tem-se como resultado que $cos_k(\zeta^i) = Re(z)$ e $sen_k(\zeta^i) = Im(z)$, de modo que $cas_k(\zeta^i) = cos_k(\zeta^i) + sen_k(\zeta^i) = Re(z) + Im(z) \in GF(p)$.

A Tabela IV lista valores de ζ e p satisfazendo à Proposição 1.

TABELA IV. ALGUNS VALORES DE $\zeta = a + jb$ SATISFAZENDO À PROPOSIÇÃO 1

p	$\zeta = a + jb$
3	$2, j, j2$
7	j, $2+j2$, $2+j5$, $5+j2$, $5+j5$
11	$3+j5$, $5+j3$, $8+j5$, $5+j8$, $3+6j$,$6+j3$,$6+j8$,$8+j6$
19	$2+j4$, $4+j2$, $17+j4$, $4+j17$, $2+j15$, $15+j2$, $17+j15$, $15+j17$, $3+j7$, $7+j3$, $16+j7$, $7+j16$, $3+j12$, $12+j13$, $16+j12$, $12+16j$
23	$4+j10$, $10+j4$, $19+j10$, $10+j19$, $4+j13$, $13+j4$, $19+j13$, $13+j19$, $8+j12$, $12+j8$, $15+j12$, $12+j15$, $8+j11$, $11+j8$, $15+j11$, $11+j15$, $9+j9$, $14+j9$, $9+j14$, $14+j14$
31	$2+j20$, $20+j2$, $29+j20$, $20+j29$, $2+j11$, $11+j2$, $29+j11$, $11+j29$, $4+j4$, $27+j4$, $4+j27$, $27+j27$, $5+j21$, $21+j5$, $26+j21$, $21+j26$, $5+j10$, $10+j5$, $26+j10$, $10+j26$, $7+j13$, $13+j7$, $24+j13$, $13+j24$, $7+j18$, $18+j7$, $24+j18$, $18+j24$

Definição 2 (Transformada numérica de Hartley): Seja $v = (v_0, v_1, \dots, v_{N-1})$ um vetor de comprimento N com componentes em GF(p), $p \equiv 3 \pmod 4$. A transformada numérica de Hartley do vetor v é o vetor $V = (V_0, V_1, \dots, V_{N-1})$ com componentes em GF(p) dadas por

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

em que $\zeta = a + jb$ é um elemento de ordem N em GF(p) satisfazendo $a^2+b^2 \equiv 1 \pmod p$.

Teorema 1 (Transformada numérica de Hartley inversa): A TNH inversa de V é o vetor v de componentes v_i, em GI(p), dadas por

$$v_i \equiv \frac{1}{N(mod\ p)} \sum_{k=0}^{N-1} V_k cas_k(\zeta^i),$$

em que $\zeta = a + jb$ é um elemento de ordem N em GI(p) satisfazendo $a^2+b^2 \equiv 1 \pmod p$ [8].

O par TNH é denotado por $v \leftrightarrow V$ ou $V = \mathbf{H_T} v$, em que $\mathbf{H_T}$ é a matriz da transformada. Uma sequência v é dita uma autossequência da TNH, com autovalor associado $\lambda \in$GF(p), quando satisfaz à relação $V = \lambda v$.

Proposição2: Os autovalores associados à TNH são 1 e -1.

Demonstração: O resultado decorre diretamente do fato de que a TNH, assim como a transformada discreta de Hartley, é uma involução, o que significa que aplicando-se a TNH duas vezes à sequência v obtem-se a própria sequência v, isto é, $\mathbf{H_T}V = (\mathbf{H_T})^2 v = v$. Se v é uma autossequência da TNH, isso implica em $\lambda^2 v = v$ e o resultado segue.

Na Proposição 3, a seguir, é caracterizada a relação entre as palavras-código dos códigos de Hartley e de Fourier.

Proposição 3: Os autovetores de $\mathbf{H_T}$ com autovalor *1* correspondem aos autovetores de **F** com autovalores *1* e *j*. Os autovetores de $\mathbf{H_T}$ com autovalor *-1* correspondem aos autovetores de **F** com autovalores *-1* e *-j*.

Demonstração: A prova deriva da relação entre a TNF e a TNH,

$$\mathbf{F} = F_R + jF_I, \quad (1)$$

$$\mathbf{H_T} = F_R + F_I, \quad (2)$$

em que **F** e $\mathbf{H_T}$ representam, respectivamente, as matrizes de transformação da TNF e da TNH, e as matrizes F_R *e* F_I são definidas por $F_R(k,i) = [cos_k(\zeta^i)]$ e $F_I(k,i) = [sen_k(\zeta^i)]$. Considerando os autovalores $(\pm 1, \pm j)$ da TNF e usando-os nas expressões (1) e (2), chega-se à correspondência entre os autovetores da TNF e da TNH. Especificamente, para λ=1, $\mathbf{F}x = \lambda x = x$, ou seja, $(F_R + jF_I)x = x$. Como x é real, tem-se $F_R x = x$ e $F_I x = 0$. Portanto $\mathbf{H_T}x = (F_R + F_I)x = x$ e λ=1 é autovalor de $\mathbf{H_T}$. O procedimento para os demais autovalores é semelhante.

Da Proposição 3, resulta a multiplicidade dos autovalores da TNH indicada na Tabela III. Os valores são obtidos somando-se os valores das colunas (2 e 5) e das colunas (3 e 4) da Tabela I. Caso as colunas dessa tabela sejam intercambiadas, conforme mencionado no início da Seção II, chega-se às multiplicidades dos autovalores da TNH apresentadas na Tabela II, agora somando-se as colunas (2 e 4) e as colunas (3 e 5) da Tabela I.

B. Construção dos Códigos de Hartley

De acordo com a Definição 2, a matriz $\mathbf{H_T}$ é dada por

$$\begin{pmatrix} cas(\zeta^{0.0}) & cas(\zeta^{0.1}) & \dots & cas(\zeta^{0.(N-1)}) \\ cas(\zeta^{1.0}) & cas(\zeta^{1.1}) & \dots & cas(\zeta^{1.(N-1)}) \\ \vdots & \vdots & \ddots & \vdots \\ cas(\zeta^{(N-1).0}) & cas(\zeta^{(N-1).1}) & \dots & cas(\zeta^{(N-1).(N-1)}) \end{pmatrix}$$

em que $\zeta = a + jb$ é um elemento de ordem N em GF(p) satisfazendo $a^2+b^2 \equiv 1 \pmod p$. Se $v \leftrightarrow V$ e v é uma autossequência da transformação linear definida por $\mathbf{H_T}$, então $\mathbf{H_T}v = \lambda v$, ou $(\mathbf{H_T} - \lambda\mathbf{I})v = 0$. Como resultado, a matriz $(\mathbf{H_T} - \lambda\mathbf{I})$ faz um papel análogo ao da matriz de paridade do código de bloco linear com comprimento N e dimensão K, em que $N-K$ = posto$(\mathbf{H_T} - \lambda\mathbf{I})$. A forma padrão de representação da matriz de paridade e da matriz geradora do código é usada, isto é, $\mathbf{H}=[\mathbf{I}_{N-K}|\mathbf{P}]$ e $\mathbf{G} = [-\mathbf{P}^T|\mathbf{I}_k]$.

Dois códigos de bloco sobre GF(p) podem ser gerados, um para cada autovalor λ. Os valores possíveis para p são determinados pelas restrições da Definição 2.

Exemplo 1: Construção de códigos de bloco lineares de comprimento 8, com $\zeta = 5 + 2j$, sobre GF(7). A matriz de transformação é

$$\mathbf{H}_T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 6 & 4 & 6 & 0 & 1 & 3 \\ 1 & 6 & 6 & 1 & 1 & 6 & 6 & 1 \\ 1 & 4 & 1 & 0 & 6 & 3 & 6 & 0 \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 0 & 6 & 3 & 6 & 0 & 1 & 4 \\ 1 & 1 & 6 & 6 & 1 & 1 & 6 & 6 \\ 1 & 3 & 1 & 0 & 6 & 4 & 6 & 0 \end{pmatrix}.$$

Após algumas operações elementares de linha, chega-se às matrizes de paridade na representação padrão, para os dois autovalores λ=±1, respectivamente,

$$\mathbf{H}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 4 & 0 & 4 \\ 0 & 1 & 0 & 0 & 6 & 2 & 4 & 1 \\ 0 & 0 & 1 & 0 & 3 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 4 & 3 & 5 \end{pmatrix},$$

e

$$\mathbf{H}^{(-1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 6 & 4 & 1 \\ 0 & 1 & 0 & 0 & 4 & 5 & 1 & 3 \\ 0 & 0 & 1 & 0 & 0 & 4 & 6 & 3 \\ 0 & 0 & 0 & 1 & 4 & 6 & 1 & 2 \end{pmatrix},$$

o que leva aos seguintes códigos de Hartley, $H_{T,\lambda}(n, k, d)$, com matrizes geradoras $\mathbf{G}^{(\lambda)}$:

$H_{T,1}(8,4,4)$,

$$\mathbf{G}^{(-1)} = \begin{pmatrix} 6 & 3 & 0 & 3 & 1 & 0 & 0 & 0 \\ 1 & 2 & 3 & 1 & 0 & 1 & 0 & 0 \\ 3 & 6 & 1 & 6 & 0 & 0 & 1 & 0 \\ 6 & 4 & 4 & 5 & 0 & 0 & 0 & 1 \end{pmatrix};$$

e

$H_{T,-1}(8,4,4)$,

$$\mathbf{G}^{(1)}=\begin{pmatrix}1&1&4&6&1&0&0&0\\3&5&6&3&0&1&0&0\\0&3&6&4&0&0&1&0\\3&6&6&2&0&0&0&1\end{pmatrix}.$$

A distância mínima é 4, pois este é o número mínimo para formarmos um conjunto LD de vetores coluna da matriz de paridade .

C. Parâmetros dos Códigos

Os códigos de Hartley $H_{T,\lambda}(n, k, d)$ tem comprimento n igual à ordem N do elemento $\zeta = a + jb$, que corresponde à ordem da matriz da TNH. A dimensão k do código é a multiplicidade geométrica do autovalor λ, ou seja, é a dimensão do subespaço de autossequências associadas a λ [13]. Os possíveis valores de k estão indicados nas Tabelas II e III. Assim, considerando a Proposição 3, deve-se observar as multiplicidades dos autovalores da TNF para se determinar o valor de k. A escolha do elemento ζ influencia diretamente na multiplicidade de cada autovalor, como observado para os casos do Exemplo 2.

Proposição 4: (Uma cota superior para a distância mínima) Os parâmetros de um código de Hartley $H_{T,\lambda}(n, k, d)$ satisfazem $d \leq n - k$.

Demonstração: Em [11] são determinadas cotas superiores para a distância mínima dos códigos de Fourier $F_\lambda(n, k, d)$, as quais dependem do autovalor associado ao código. Especificamente, para códigos associados ao autovalor $\lambda = \pm 1$, tem-se $d \leq n - 2k + 2$ e para códigos associados ao autovalor $\lambda = \pm j$, tem-se $d \leq n - 2k$.
Como vimos na Proposição 3, as palavras do código de Hartley associado ao autovalor *1* (respectivamente *-1)*, correspondem às palavras dos códigos de Fourier associados aos autovalores *1* e *j* (respectivamente *-1* e *-j*). Portanto, um código de Hartley possui palavras-código dos códigos de Fourier associados a um dos autovalores, *j* ou *–j*, e assim, considerando a relação entre as dimensões dos subespaços associados a cada uma das transformadas, sua distância mínima satisfaz $d \leq n - k$. Esta cota é portanto, menos restritiva do que a cota para os códigos de Fourier, mas limita mais do que a *Cota de Singleton* ($d \leq n – k + 1$)[14].

Exemplo 2: Com os elementos $\zeta_x = 5 + j2$ e $\zeta_y = 2 + j2$, ambos de ordem 8, sobre GF(7), é possível construir os códigos:

$$G_x^{(1)}(8, 4, 4) \text{ e } G_x^{(-1)}(8, 4, 4).$$

$$G_y^{(1)}(8, 5, 2) \text{ e } G_y^{(-1)}(8, 3, 5).$$

A Tabela V mostra os parâmetros de alguns códigos de Hartley. Os valores destacados em negrito atingem a cota estabelecida na Proposição 4.

TABELA V. PARÂMETROS DE ALGUNS CÓDIGOS DE HARTLEY EM GF(p)

n	$\zeta = a + jb$	p	$k^{(1)}$	$d^{(1)}$	$k^{(-1)}$	$d^{(-1)}$
8	$2+j2$	7	5	2	3	5
8	$5+j2$	7	4	4	4	4
8	$5+j5$	7	3	5	5	2
12	$3+j5$	11	6	**6**	6	**6**
12	$3+j6$	11	7	**5**	5	**7**
20	$4+j2$	19	9	**11**	11	**9**

Um caso particular de especial interesse, por apresentar uma maior simetria, corresponde aos códigos de Hartley, cujos parâmetros são definidos pela Tabela III, com comprimento $N \equiv 0(mod 4)$. As investigações computacionais realizadas indicam a existência de uma família de códigos $H_{T,\lambda}(4m, 2m, 2m)$, os quais atingem a cota superior da Proposição 4. Esta família constitui o que denominamos códigos de Hartley balanceados (CHB). Os dois códigos dessa família, com os mesmos parâmetros, correspondentes aos autovalores $\lambda = \pm 1$, formam um par CHB casado.

IV. CONCLUSÕES

Neste artigo, uma nova família de códigos de bloco lineares multiníveis – os códigos de Hartley sobre corpos finitos – foi introduzida. As palavras-código de $H_{T,\lambda}(n,k,d)$ são autossequências da transformada numérica de Hartley, associadas ao autovalor λ. Assim como os códigos de Fourier, os códigos de Hartley fazem parte de uma nova classe de códigos, os chamados códigos de transformada. Para uma dada transformada de corpo finito de comprimento N, sua autoestrutura pode ser usada para construir um código de bloco linear de comprimento N e possíveis valores para a dimensão k, sendo k a multiplicidade dos autovalores da transformada. Foi observado que este último parâmetro pode variar com a mudança do elemento ζ gerador da matriz da transformada,

Os códigos de blocos lineares cuja taxa é ½ possuem algumas propriedades interessantes como a de se obter os bits de informação através dos bits de paridade por um processo de inversão, e por esta razão são conhecidos como códigos inversíveis. Nesse contexto, os pares CHB estão sendo objeto de uma investigação mais aprofundada.

Os códigos de Hartley apresentam uma taxa assintoticamente duas vezes maior do que a dos códigos

gerados a partir da transformada numérica de Fourier. Naturalmente, há uma pequena perda na distância mínima. Além disso, por uma escolha apropriada de $\boldsymbol{\zeta}$, é possível construir um código com o comprimento de bloco e a dimensão pretendida, com mais liberdade.

Os códigos introduzidos neste trabalho são lineares e podem ser implementados usando as técnicas clássicas de codificação e decodificação para essa classe de códigos. Em se tratando de técnicas eficientes para decodificação de códigos de bloco, aqueles de taxa baixa apresentam uma baixa complexidade de decodificação. Os códigos com altas taxas podem ser decodificados com auxílio do código dual [14], que apresenta taxa baixa e, consequentemente, pequena complexidade de decodificação. Os casos mais críticos para decodificação são precisamente os códigos com taxa próxima a ½, para os quais a decodificação explorando propriedades do código ou do seu dual possui praticamente a mesma complexidade.

Novas técnicas de implementação mais eficientes, baseadas na estrutura matemática adicional que os códigos de Hartley apresentam, estão sendo investigadas. Neste cenário, este trabalho abre perspectivas para concepção de um método de decodificação com base nas propriedades da autoestrutura da transformada, incluindo a possibilidade do uso de algoritmos rápidos para computar a transformada numérica de Hartley, o que pode ser atrativo em comparação com os algoritmos convencionais.

REFERÊNCIAS

[1] I. S. Reed and T. K. Tuong, *The Use of Finite Fields to Compute Convolution*, IEEE Trans. Inform.Theory, vol. IT-21, pp.208-213, Mar 1975.

[2] I. S. Reed, T. K. Tuong, 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.

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

[4] J. L. Massey, *The Discrete Fourier Transform in Coding and Cryptography*, Information Theory Workshop, ITW 98, San Diego, CA, Feb. 1998.

[5] T. Toivonen, J. Heikkilä, *Video Filtering with Fermat Number Theoretic Transforms using Residue Number System*, IEEE Trans. Circuits Systems Video Tech. 16(1), pp. 92-101, 2006.

[6] J.B. Lima, R.M. Campello de Souza, D. Panario, *The eigenstructure of finite field trigonometric ttransforms*, Linear Algebra and its Applications, 435, pp. 1956-1971, 2011.

[7] H. M. de Oliveira and R. M. Campello de Souza, *Orthogonal Multilevel Spreading Sequence Design*, Coding, Communication and Broadcasting, Research Studies Press, Baldock, UK, pp. 291-301, 2000.

[8] R. M. Campello de Souza, H. M. de Oliveira, L. B. Espínola Palma and M. M. Campello de Souza, *Hartley Number Theoretic Transforms*, ISIT2001, Washington, DC, June 24-29, 2001.

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

[10] D. T. Birtwistle, "The eigenstructure of the number theoretic transforms", Signal Processing, vol. 4, no. 4, pp. 287–294, July 1982.

[11] R. M. Campello de Souza, E. S. V. Freire, H. M. de Oliveira, Fourier Codes, in: Proc. of the tenth International Symposium on Communication Theory and Applications, Ambleside, UK, 2009, pp. 370–375.

[12] R. M. Campello de Souza, H. M. de Oliveira and A.N. Kaufmann, *Trigonometry in Finite Fields and a New Hartley Transform*, Proc. of the IEEE Int. Symp. on Info. Theory, p.293, Cambridge, MA, Aug, 1998.

[13] J. H. McClellan and T.W.Parks. *Eigenvalue and Eigenvector Decomposition of Discrete Fourier Transform, IEEE Transactions on Audio and Electroacoustics* AU-20, pp.66-74, 1972.

[14] S. Lin and D. J. Costello Jr. , *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, 2ª edição, 2004.