UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

EDUARDA SIMÕES VELOSO FREIRE

CONSTRUÇÃO DE CÓDIGOS DE BLOCO LINEARES VIA TRANSFORMADAS DIGITAIS

Recife, 24 de julho de 2009.

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

CONSTRUÇÃO DE CÓDIGOS DE BLOCO LINEARES VIA TRANSFORMADAS DIGITAIS

Elaborado por:

EDUARDA SIMÕES VELOSO FREIRE

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para a obtenção do grau de **Mestre em Engenharia Elétrica**.

ORIENTADOR: RICARDO MENEZES CAMPELLO DE SOUZA, Ph.D.

Recife, Julho de 2009.

F866c **Freire, Eduarda Simões Veloso.**

Construção de códigos de bloco lineares via transformadas digitais / Eduarda Simões Veloso Freire. – Recife: O Autor, 2009.

83 folhas, il : figs., tabs.

Dissertação (Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2009.

Inclui Referências e Apêndices.

1. Engenharia Elétrica. 2.Códigos Corretores de Erros. 3. Transformadas Digitais. I. Título.

UFPE

621.3 **CDD (22. ed.)** **BCTG/2009-159**

Universidade Federal de Pernambuco

Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO DO MESTRADO ACADÊMICO DE

EDUARDA SIMÕES VELOSO FREIRE

TÍTULO

"CONSTRUÇÃO DE CÓDIGOS DE BLOCO LINEARES VIA TRANSFORMADAS DIGITAIS"

A comissão examinadora composta pelos professores: CECÍLIO JOSÉ LINS PIMENTEL, DES/UFPE, HÉLIO MAGALHÃES DE OLIVEIRA, DES/UFPE e JULIANO BANDEIRA LIMA, DEE/UPE sob a presidência do primeiro, consideram a candidata **EDUARDA SIMÕES VELOSO FREIRE APROVADA.**

Recife, 24 de julho de 2009.

EDUARDO FONTANA
Coordenador do PPGEE

CECÍLIO JOSÉ LINS PIMENTEL
Membro Titular Interno

JULIANO BANDEIRA LIMA
Membro Titular Externo

HÉLIO MAGALHÃES DE OLIVEIRA
Membro Titular Interno

AGRADECIMENTOS

Agradeço aos meus pais Eduardo Cantinho Veloso Freire e Mariza P. V. Simões Veloso Freire e, às minhas irmãs Camila Simões Veloso Freire e Milena Simões Veloso Freire, pela ajuda, suporte e compreensão durante esse período de estudo.

Agradeço especialmente ao Prof. Ricardo Menezes Campello de Souza, que desde a graduação admiro e considero um modelo a ser seguido. Agradeço-o por ter me dado a oportunidade de mais uma vez estudar com ele, aceitando ser meu orientador de mestrado, e também pelo incentivo, pela vibração, dedicação e ajuda constante.

Agradeço também ao professor Valdemar Cardoso da Rocha Jr. por estar sempre presente, pela dedicação e incentivo.

Agradeço aos demais professores do DES, em especial, aos professores do grupo de comunicações: Cecílio José Lins Pimentel, Hélio Magalhães de Oliveira e Márcia Mahon Campello de Souza, pela disposição, apoio e ensinamento, fazendo parte da minha formação acadêmica da melhor maneira possível.

Agradeço aos meus amigos da pós-graduação e da graduação: Alessandra Barbosa, André Ricardson, Andrei Formiga, Brenno Miro, Caio Marcelo Barros, Daniel da Rocha Simões, Elda Lizandra, Eurico Moura, Gabriel de França, Gilson Jerônimo da Silva Jr., Giovanna Angelis, José Mário de Oliveira, Juliano Bandeira, Márcio Lima, Roberto Sotero, Victor Nascimento, e todos os outros que fizeram parte da minha pós-graduação, propiciando um ambiente de agradável convivência e cooperação.

Agradeço ao programa de Pós-Graduação em Engenharia Elétrica, ao coordenador professor Eduardo Fontana, à CAPES e aos funcionários do DES, em especial à Andréa Tenório.

EDUARDA SIMÕES VELOSO FREIRE

Universidade Federal de Pernambuco

Julho de 2009

Resumo da Dissertação apresentada à UFPE como parte dos requisitos necessários para a obtenção do grau de Mestre em Engenharia Elétrica.

CONSTRUÇÃO DE CÓDIGOS DE BLOCO LINEARES VIA TRANSFORMADAS DIGITAIS

Eduarda Simões Veloso Freire

Julho/2009

Orientador: Prof. Ricardo Menezes Campello de Souza, Ph.D.
Área de Concentração: Comunicações
Palavras-chave: Códigos Corretores de Erros, Transformadas Digitais
Número de Páginas: 83

Novas famílias de códigos corretores de erros, criados a partir da transformada numérica de Fourier (Códigos de Fourier) e de transformadas trigonométricas sobre corpos finitos (Códigos FFCT tipo 4 par, do inglês *finite field cosine transform*, e Códigos FFST tipo 4 par, do inglês *finite field sine transform*), são apresentadas nesta dissertação. A matriz de paridade de cada código, sua dimensão e distância mínima são obtidas a partir da autoestrutura da transformada numérica de Fourier unitária e das transformadas do seno e do cosseno de corpo finito unitária. Uma técnica de decodificação para os Códigos de Fourier é proposta. No caso dos Códigos FFCT-4P e FFST-4P, se observa que, em alguns casos, os mesmos são códigos de máxima distância de Hamming mínima.

Abstract of Dissertation presented to UFPE as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering.

CONSTRUCTION OF LINEAR BLOCK CODES VIA DIGITAL TRANSFORMS

Eduarda Simões Veloso Freire

July/2009

Supervisor: Prof. Ricardo Menezes Campello de Souza, Ph.D.
Area of Concentration: Communications
Keywords: Error Correcting Codes, Digital Transforms
Number of pages: 83

New families of error-correcting codes, created from the Fourier number theoretic transform (Fourier Codes) and from trigonometric transforms over finite fields (FFCT-4e and FFST-4e Codes), are introduced in this dissertation. The code parity-check matrix, its dimension and minimum distance are obtained from the eigenstructure of the unitary Fourier number theoretic transform and from the finite field sine and cosine transform. A decoding technique for the Fourier Codes is proposed. Regarding the FFCT-4P and FFST-4P Codes, our results show that some of the constructed codes are maximum distance separable (MDS) codes.

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO 1
INTRODUÇÃO

Transformadas em corpos finitos têm sido muito usadas em áreas como processamento digital de sinais, códigos corretores de erros e criptografia. Tais transformadas são digitais, uma vez que suas componentes são elementos de um corpo finito. Nesse cenário, estão as transformadas numéricas de Fourier (FNTT, do inglês *Fourier number theoretic transform*) e as transformadas trigonométricas sobre corpos finitos (FFTT, do inglês *finite field trigonometric transform*).

A transformada de corpo finito mais conhecida é a de Fourier (FFFT, *finite field Fourier transform*), introduzida por Pollard em 1971 em sua versão numérica [1]. As duas primeiras FFTTs, a do cosseno e a do seno, foram introduzidas por Campello de Souza et al. [2], [3]. Posteriormente, as demais transformadas, completando um total de 16 transformadas trigonométricas, foram construídas por J. B. Lima [4]. As FFTTs têm diversas aplicações, como por exemplo, marca d'água digital, filtragem de imagens e separação de sequências na comunicação multiusuário [5], [6], [7].

Nesta dissertação, novas famílias de códigos corretores de erros, baseadas em transformadas digitais, são propostas. A FNTT unitária é utilizada para a construção de códigos de bloco lineares não-binários, chamados de Códigos de Fourier, e duas transformadas trigonométricas sobre corpos finitos, a transformada do cosseno de corpo finito (FFCT, *finite field cosine transform*), e a transformada do seno de corpo finito (FFST, *finite field sine transform*) são usadas para a construção dos Códigos FFCT-4P e FFST-4P, respectivamente. A existência de transformadas rápidas sobre corpos finitos é um fator decisivo para a implementação desses códigos, podendo facilitar bastante a sua decodificação.

Um código corretor de erro deve ser avaliado não apenas pela sua taxa e distância mínima, mas também pela facilidade de decodificação. A escolha para utilização de um determinado código depende, portanto, não somente dos seus parâmetros, como comprimento de bloco e distância mínima, mas também da velocidade e facilidade de decodificação requerida, dependendo do tipo de aplicação. Nesse contexto, a transformada de Fourier sobre corpos finitos pode ser utilizada em técnicas de decodificação no domínio da frequência, como visto em [8].

A idéia principal deste trabalho não é a construção de códigos corretores com máxima capacidade de correção, mas sim a construção de códigos que utilizem as autoestruturas das transformadas digitais, assim como a existência de algoritmos rápidos dessas transformadas, incluindo algoritmos com complexidade multiplicativa nula [9], [10], para facilitar a decodificação de tais códigos.

Para a implementação dos códigos baseados em transformadas digitais usou-se o *software* MATLAB. Nele foram desenvolvidos programas para implementar as transformadas numéricas de Fourier sobre corpos finitos, as transformadas trigonométricas do seno e do cosseno sobre corpos finitos, bem como todas as demais funções básicas, usando aritmética de corpo finito, para suas implementações.

O restante deste trabalho é composto por cinco capítulos e cinco apêndices. O Capítulo 2 inicia-se com uma revisão das transformadas numéricas de Fourier, incluindo sua definição e algumas propriedades. Este Capítulo descreve ainda a autoestrutura da FNTT, mostrando detalhadamente como as autossequências dessas transformadas são geradas. Alguns algoritmos rápidos para o cálculo de transformadas de Fourier são descritos na Seção 2.4, na qual é feita uma breve revisão dos algoritmos de Cooley-Tukey [11], Good-Thomas [12] e Goertzel [13].

O Capítulo 3 apresenta as transformadas trigonométricas sobre corpos finitos, desde a definição dos números complexos sobre corpos finitos (Seção 3.1), passando pelas funções trigonométricas sobre corpos finitos e suas propriedades (Seção 3.2), que são as bases das FFTTs, até a descrição das transformadas trigonométricas do cosseno e do seno tipo 4 par (FFCT-4P e FFST-4P) e suas versões unitárias (Seção 3.3). Algumas propriedades das FFTTs são mostradas na Seção 3.4 e sua autoestrutura é revista na Seção 3.5

No Capítulo 4, os códigos baseados na autoestrututa da FNTT unitária, Códigos de Fourier, são introduzidos. A Seção 4.1 mostra a construção dos Códigos de Fourier, descrevendo como obter a matriz de paridade, H, do código, e consequentemente, a matriz geradora, G, para um determinado autovalor λ. Na Seção 4.2, os parâmetros do código, n (comprimento de bloco), k (dimensão), e uma cota superior para a distância mínima de Hamming, d, são obtidos. Uma técnica de decodificação baseada na autoestrutura da FNTT unitária, para corrigir um e dois erros é proposta na Seção 4.3. O resultado dessa pesquisa gerou o artigo intitulado "*Fourier Codes*", In: Proceedings of the Tenth International Symposium on Communication Theory and Applications, ISCTA'09, Ambleside, Lake District, UK, 2009, p. 370-375 [14].

No Capítulo 5 é introduzida a nova família de códigos corretores de erros baseada na autoestrutura das transformadas trigonométricas sobre corpos finitos. As Seções 5.1 e 5.3 mostram, respectivamente, a construção dos Códigos FFCT-4P e FFST-4P, assim como alguns exemplos. Os parâmetros dos códigos FFCT-4P e FFST-4P são introduzidos nas Seções 5.2 e 5.4, e é observado que, para alguns valores de n, os códigos são de máxima distância mínima (MDS, do inglês *maximum distance separable*).

A dissertação é finalizada com algumas conclusões deste trabalho e algumas sugestões para trabalhos futuros, apresentadas no Capítulo 6.

O Apêndice A aborda a Lei da Reciprocidade Quadrática [15], em que o Símbolo de Legendre é usado para determinar os valores do número primo p, para os quais a FNTT unitária de comprimento N existe.

O Apêndice B trata do Teorema Chinês do Resto [15], sendo utilizado para resolver alguns sistemas de congruências lineares do Apêndice A.

O Apêndice C mostra uma tabela de possíveis comprimentos N para a FNTT unitária.

O Apêndice D mostra diversas tabelas de elementos unimodulares em $GI(p)$, incluindo suas respectivas ordens complexas, que são utilizados para o cálculo das transformadas trigonométricas sobre corpos finitos, descritas no Capítulo 3.

Finalmente, o Apêndice E apresenta todas as matrizes de paridade, H, e geradoras, G, dos códigos apresentados nas tabelas do Capítulo 5 desta dissertação.

CAPÍTULO 2
A TRANSFORMADA NUMÉRICA DE FOURIER

A transformada de Fourier sobre corpos finitos (FFFT, *finite field Fourier transform*) [1], introduzida por J. M. Pollard em 1971, é uma ferramenta muito útil nos campos de Códigos Corretores de Erros, Criptografia e Processamento Digital de Sinais e tem sido usada, por exemplo, como um veículo para reduzir a complexidade da decodificação e para implementar convolução de sinais de uma forma rápida [16], [17]. O cálculo de transformadas em corpos finitos tem a vantagem de não apresentar erros de truncamento ou arredondamento e de apresentar baixa complexidade aritmética devido à existência de algoritmos rápidos, incluindo algoritmos com complexidade multiplicativa nula [9].

Em geral, a FFFT é um mapeamento relacionando vetores do campo de Galois *GF(q)* para sua extensão *GF* (q^r), onde q é uma potência de um número primo, p^m. Quando $m=r=1$, a FFFT é chamada de transformada numérica de Fourier (FNTT, *Fourier number theoretic transform*), tendo aplicações tipicamente no campo de processamento digital de sinais [18-21].

Este capítulo faz uma breve revisão da FNTT unitária e de sua autoestrutura [22], mostrando detalhadamente como as autossequências de tais transformadas são geradas. Além disso, descreve os algoritmos de Cooley-Tukey, Good-Thomas e Goertzel [11], [12], [13].

2.1 A TRANSFORMADA NUMÉRICA DE FOURIER UNITÁRIA

Definição 2.1.1: As sequências $x=(x_0,x_1,\ldots,x_{N-1})$ e $X=(X_0,X_1,\ldots,X_{N-1})$, com valores sobre $GF(p)$, p primo, formam um par da FNTT unitária quando

$$X_k=(\sqrt{N})^{-1}(\bmod p)\sum_{n=0}^{N-1}x_n\alpha^{kn}$$

e

$$x_n=(\sqrt{N})^{-1}(\bmod p)\sum_{k=0}^{N-1}X_k\alpha^{-kn},$$

em que $\alpha\in GF(p)$ tem ordem multiplicativa N e $N^{\frac{p-1}{2}}\equiv 1(\bmod p)$. O par FNTT é denotado por $x\leftrightarrow X$ ou $X=Fx$, em que F é a matriz de transformação. ■

Observe que a FNTT está restrita àqueles comprimentos N para os quais existe um elemento $\alpha \in GF(p)$ de ordem N, ou seja, N precisa ser um divisor de *p-1*. Além disso, N deve ser um resíduo quadrático de *p*. Os valores de N e p para os quais a FNTT existe são descritos no Apêndice A.

Por serem definidas sobre corpos finitos, as amplitudes dos coeficientes das transformadas numéricas são discretas. Assim, tais transformadas podem ser caracterizadas como legítimas "transformadas digitais".

2.2 AUTOSSEQUÊNCIAS DA TRANSFORMADA NUMÉRICA DE FOURIER

Uma sequência $x = (x_i)$, $x_i \in GF(p)$, é dita ser uma autossequência da FNTT, com autovalor associado $\lambda \in GF(p^2)$, quando ela satisfaz $X = \lambda x$.

A FNTT e a transformada discreta de Fourier definida sobre corpos infinitos têm autoestruturas semelhantes. Em particular, ambas satisfazem ao seguinte lema [23] (versão FNTT do lema):

Lema 2.2.1: i) Os autovalores da FNTT são as raízes quartas da unidade $(\pm 1, \pm j)$, em que $j^2 \equiv -1 (\mathrm{mod}\ p)$.

ii) Se x é uma autossequência da FNTT, então ela tem simetria par (i.e. $x_i = x_{N-i}$) se $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$ e simetria ímpar (i.e. $x_i = -x_{N-i}$) se $\lambda \equiv \pm j (\mathrm{mod}\ p)$. ■

Sequências com simetria par (ímpar) são chamadas de sequências pares (ímpares). Tais sequências podem ser usadas para gerar autossequências de acordo com os Lemas 2.2.2 e 2.2.3 [24].

Lema 2.2.2: Seja $x \leftrightarrow X$ um par FNTT. Então a sequência $y = E(x) \pm E(X)$ é uma autossequência com autovalor $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$, em que $E(x)$ denota a parte par de x. ■

Corolário 2.2.1: Toda sequência x, de simetria par, gera uma autossequência $y = x \pm X$. ■

Lema 2.2.3: Seja $x \leftrightarrow X$ um par FNTT. Então a sequência $y = O(x) \mp jO(X)$ é uma autossequência com autovalor $\lambda \equiv \pm j (\mathrm{mod}\ p)$, em que $O(x)$ denota a parte ímpar de x. ■

Corolário 2.2.2: Toda sequência x, ímpar, gera uma autossequência $y = x \mp jX$. ■

Exemplo 2.1: Considere a sequência $x = (4 \quad 2 \quad 1 \quad 4)$ com valores sobre GF(*5*) e a matriz FNTT $4 \text{ x } 4$ sobre GF(5), $F = \left(\sqrt{N}\right)^{-1} (\text{mod } p)\, \alpha^{kn}$, com $\alpha = 2$,

$$F = \begin{pmatrix} 3 & 3 & 3 & 3 \\ 3 & 1 & 2 & 4 \\ 3 & 2 & 3 & 2 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

O espectro de x é $X = (3 \quad 2 \quad 2 \quad 1)$. As partes pares e ímpares de x e X são $E(x) = (4 \quad 3 \quad 1 \quad 3)$, $E(X) = (3 \quad 4 \quad 2 \quad 4)$, $O(x) = (0 \quad 4 \quad 0 \quad 1)$ e $O(X) = (0 \quad 3 \quad 0 \quad 2)$, respectivamente.

Portanto, $y_1 = E(x) + E(X) = (2 \quad 2 \quad 3 \quad 2)$ e $y_2 = O(x) - 2O(X) = (0 \quad 3 \quad 0 \quad 2)$, são, respectivamente, autossequências com autovalores associados $\lambda \equiv 1 (\text{mod } 5)$ e $\lambda \equiv j \equiv 2 (\text{mod } 5)$. ■

Exemplo 2.2: Considere a sequência $x = (36 \quad 1 \quad 1 \quad 1 \quad 1)$ com valores sobre GF(*61*) e a matriz FNTT $5 \text{ x } 5$ sobre GF(*61*), com $\alpha = 9$,

$$F = \begin{pmatrix} 7 & 7 & 7 & 7 & 7 \\ 7 & 2 & 18 & 40 & 55 \\ 7 & 18 & 55 & 2 & 40 \\ 7 & 40 & 2 & 55 & 18 \\ 7 & 55 & 40 & 18 & 2 \end{pmatrix}.$$

O espectro de x é $X = (36 \quad 1 \quad 1 \quad 1 \quad 1)$. Como x é uma sequência par, de acordo com o corolário do Lema 2.2.2, a sequência $y_3 = x + X = (11 \quad 2 \quad 2 \quad 2 \quad 2)$ é uma autossequência. Pode ser facilmente verificado que tal autossequência tem autovalor associado $\lambda \equiv 1 (\text{mod } 61)$. ■

Exemplo 2.3: Considere agora a sequência $x = (0 \quad 60 \quad 14 \quad 47 \quad 1)$ com valores sobre GF(*61*) e a mesma matriz FNTT $5 \text{ x } 5$ sobre GF(*61*) do Exemplo 2.2.

O espectro de x é $X = (0 \quad 50 \quad 32 \quad 29 \quad 11)$. Como x é uma sequência ímpar, de acordo com o corolário do Lema 2.2.3, a sequência $y_4 = x - jX = (0 \quad 59 \quad 28 \quad 33 \quad 2)$ é uma autossequência. Pode ser facilmente verificado que tal autossequência tem autovalor associado $\lambda \equiv j \equiv 11 (\text{mod } 61)$. ■

A Tabela 2.1 a seguir apresenta exemplos de autossequências da FNTT para diversos valores de p e de λ.

Tabela 2.1 *Autossequências de comprimento* N *da FNTT* sobre $GF(p)$.

N	λ	p	$\sqrt{N} \pmod p$	α	*sequência*
4	1	5	2	2	(2 1 0 1)
5	-1	41	13	10	(29 1 1 1 1)
6	j=27	73	15	9	(0 72 33 0 40 1)
7	-j=17	29	6	7	(0 28 11 10 19 18 1)
8	j=4	17	5	8	(0 16 0 16 0 1 0 1)
9	-1	37	3	7	(22 1 0 26 3 3 26 0 1)
10	j=9	41	16	4	(0 40 0 21 23 0 18 20 0 1)
11	1	89	10	2	(6 0 0 1 87 28 28 87 1 0 0)
12	-1	13	5	2	(9 1 0 0 6 1 8 1 6 0 0 1)
16	j=4	17	4	3	(0 0 0 16 8 8 0 8 0 9 0 9 9 1 0 0)

2.3 PROPRIEDADES DA FNTT

Sejam $x \leftrightarrow X$, $y \leftrightarrow Y$ e $z \leftrightarrow Z$ pares transformados de uma FNTT de comprimento N, definida na Seção 2.1. As seguintes propriedades são válidas [25].

(a) Ortogonalidade

As funções da base α^{kn} formam um conjunto ortogonal:

$$\sum_{n=0}^{N-1} \alpha^{nk} \alpha^{-nm} = \sum_{n=0}^{N-1} \alpha^{(k-m)n} = \begin{cases} N, \text{ k} \equiv \text{m(mod N)}, \\ 0, \text{ caso contrário.} \end{cases}$$

(b) Periodicidade

Se $x_n = x_{n+N}$, então $X_k = X_{k+N}$.

(c) Deslocamento no Tempo

Se $x_n = x_{n-s}$, s um inteiro fixo, então $Y_k = \alpha^{js} X_k$.

(d) Simetria

$X_n = N\, x_{-k}$, em que $x_{-k} = x_{N-k}$.

(e) Convolução Cíclica

A FNTT de uma convolução cíclica de duas sequências é igual ao produto das FNTTs dessas sequências. Assim, dadas as sequências x, y e z, em que $z_n = \sum_{i=0}^{N-1} x_{n-i} y_i$, temos $Z_k = X_k Y_k$.

Percebe-se então que, para calcular convoluções cíclicas entre duas sequências, é muito mais eficiente calcular o produto dos espectros das duas sequências e depois calcular a transformada inversa do resultado obtido.

(f) A transformada Multidimensional

Assim como a FFFT, a FNTT unitária também pode ser estendida para múltiplas dimensões. Por exemplo, em duas dimensões, a FNTT unitária e a sua inversa podem ser definidas como:

$$X_{k_1 k_2} = (\sqrt{N_1})^{-1} (\sqrt{N_2})^{-1} (\mathrm{mod}\, p) \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \alpha_1^{\,kn_1} \alpha_2^{\,kn_2}$$

e

$$x_{n_1 n_2} = (\sqrt{N_1})^{-1} (\sqrt{N_2})^{-1} (\mathrm{mod} p) \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} X_{k_1 k_2} \alpha_1^{\,-kn_1} \alpha_2^{\,-kn_2} ,$$

$k_1, n_1 = 0,1,\ldots,N_1-1;\ k_2, n_2 = 0,1,\ldots,N_2-1$. Aqui, α_1, $\alpha_2 \in GF(p)$ têm ordens, respectivamente, N_1 e N_2.

2.4 ALGORITMOS RÁPIDOS

Uma transformada rápida de Fourier (FFT, do inglês *fast Fourier transform*) é um algoritmo para calcular uma transformada discreta de Fourier (DFT, do inglês *discrete Fourier transform*), de comprimento N, que apresenta complexidade aritmética $< N^2$. Existem vários algoritmos FFT, dentre eles, os algoritmos de Cooley-Tukey [11] e de Good-Thomas [12], [26]. A FFT é uma forma de calcular a DFT que apresenta uma complexidade computacional multiplicativa inferior àquela decorrente de sua definição. Neste caso, o cálculo de uma DFT de comprimento N requer N^2 multiplicações, o que pode significar uma diferença substancial, em complexidade, especialmente para os casos em que N é grande ($N > 64$). Os algoritmos FFT mais conhecidos dependem basicamente da fatoração de N, mas existem FFTs para qualquer valor de N.

É importante ressaltar ainda que os algoritmos de Cooley-Tukey e Good-Thomas podem ser desenvolvidos sobre um corpo finito [10] e por essa razão, eles serão revistos neste capítulo.

2.4.1 O ALGORITMO DE COOLEY-TUKEY

O algoritmo de Cooley-Tukey é o algoritmo FFT mais conhecido e aplicado. A utilização desse algoritmo requer que o comprimento da transformada seja composto, ou seja, $N = n_1 n_2$. Tal

algoritmo recursivamente divide uma DFT de comprimento composto $N = n_1 n_2$ em DFTs de comprimentos menores n_1 e n_2.

De uma forma mais geral, o algoritmo de Cooley-Tukey se baseia na idéia de mapear o vetor a ser transformado num arranjo bidimensional $n_1 \text{ x } n_2$. As novas coordenadas (i_1, i_2) do arranjo bidimensional do vetor v, com coordenadas v_i, são definidas por [9]:

$$i = i_1 + n_1 i_2 ,$$

com $i_1 = 0, \ldots, n_1 - 1$ e $i_2 = 0, \ldots, n_2 - 1$.

Dessa forma, o vetor unidimensional $v = v_0, v_1, \ldots, v_{n_1 n_2 - 1}$ é mapeado no arranjo bidimensional

$$v = \begin{bmatrix} v_0 & v_{n_1} & v_{2n_1} & \cdots & v_{(n_2-1)n_1} \\ v_1 & v_{n_1+1} & v_{2n_1+1} & \cdots & v_{(n_2-1)n_1+1} \\ v_2 & v_{n_1+2} & v_{2n_1+1} & \cdots & v_{(n_2-1)n_1+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{n_1-1} & v_{2n_1-1} & v_{3n_1-1} & \cdots & v_{n_2 n_1-1} \end{bmatrix}.$$

O vetor de entrada, agora bidimensional, é transformado no vetor de saída X, cujas coordenadas (k_1, k_2) são definidas por:

$$k = n_2 k_1 + k_2 ,$$

com $k_1 = 0, \ldots, n_1 - 1$ e $k_2 = 0, \ldots, n_2 - 1$.

Assim, o arranjo bidimensional do vetor de saída é dado por:

$$X = \begin{bmatrix} X_0 & X_1 & X_2 & \cdots & X_{n_2-1} \\ X_{n_2} & X_{n_2+1} & X_{n_2+2} & \cdots & X_{2n_2-1} \\ X_{2n_2} & X_{2n_2+1} & X_{n_2+2} & \cdots & X_{3n_2-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_{(n_1-1)n_2} & X_{(n_1-1)n_2+1} & X_{(n_1-1)n_2+2} & \cdots & X_{n_1 n_2-1} \end{bmatrix}.$$

Aplicando-se a DFT ao arranjo bidimensional do vetor de entrada, temos:

$$X_k = \sum_{i=0}^{N-1} v_i \alpha^{ik} ,$$

que resulta em

$$X_{n_2 k_1 + k_2} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1 + n_1 i_2} \alpha^{(i_1 + n_1 i_2)(n_2 k_1 + k_2)} .$$

Manipulando-se os índices convenientemente e levando-se em consideração que $\alpha^N = 1$, pode-se reescrever a DFT como:

$$X_{k_1,k_2} = \sum_{i_1=0}^{n_1-1} \alpha^{i_1 n_2 k_1} \left[\alpha^{i_1 k_2} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} \alpha^{n_1 i_2 k_2} \right] = \sum_{i_1=0}^{n_1-1} \beta^{i_1 k_1} \left[\alpha^{i_1 k_2} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} \gamma^{i_2 k_2} \right],$$

em que $\beta = \alpha^{n_2}$ e $\gamma = \alpha^{n_1}$.

Após o mapeamento do vetor de entrada no arranjo bidimensional, o algoritmo de Cooley-Tukey se baseia em calcular n_1 DFTs de comprimento n_2, N multiplicações complexas devido ao termo de ajuste $\alpha^{i_1 k_2}$ e, por fim, n_2 DFTs de comprimento n_1.

O algoritmo de Cooley-Tukey mais conhecido é o que divide a transformada de tamanho N em duas DFTs de tamanho $N/2$, reduzindo a complexidade computacional para $(N/2)\log_2 N$ multiplicações complexas e $N \log_2 N$ adições complexas [9]. Tal algoritmo, conhecido como algoritmo de Cooley-Tukey de base 2, assume que N é uma potência de 2, ou seja, o comprimento da transformada, 2^m, pode ser fatorado como 2.2^{m-1} ou $2^{m-1}.2$ para construir uma FFT.

O algoritmo de Cooley-Tukey na base 2 com comprimento de bloco $N = 2^m$ e com $n_1 = 2$ e $n_2 = 2^{m-1}$ é conhecido como **Algoritmo de Cooley-Tukey na base 2 com dizimação no tempo**. Mais explicitamente, a DFT pode ser expressa como

$$X_k = \sum_{i=0}^{N/2-1} \alpha^{2ki} v_{2i} + \alpha^k \sum_{i=0}^{N/2-1} \alpha^{2ki} v_{2i+1}$$

e

$$X_{k+N/2} = \sum_{i=0}^{N/2-1} \alpha^{2ki} v_{2i} - \alpha^k \sum_{i=0}^{N/2-1} \alpha^{2ki} v_{2i+1},$$

para $k = 0, \ldots, (N/2)-1$ e $\alpha^{N/2} = -1$.

A FFT com dizimação no tempo segmenta o **vetor de entrada** em um conjunto de componentes com índice par e outro conjunto de componentes com índice ímpar. O arranjo de saída é formado por dois conjuntos, cada um com $N/2$ componentes.

O algoritmo de Cooley-Tukey na base 2 com comprimento de bloco $N = 2^m$ e com $n_1 = 2^{m-1}$ e $n_2 = 2$ é conhecido como **Algoritmo de Cooley-Tukey na base 2 com dizimação na frequência**. Mais explicitamente, a DFT pode ser expressa como

$$X_{2k} = \sum_{i=0}^{N/2-1} \alpha^{2ki} (v_i + v_{i+N/2})$$

e

$$X_{2k+1} = \sum_{i=0}^{N/2-1} \alpha^{(2k+1)i} (v_i - v_{i+N/2}),$$

para $k = 0, \ldots, (N/2)-1$ e $\alpha^{N/2} = -1$.

A FFT com dizimação na freqüência segmenta o vetor de entrada em dois conjuntos, cada um com $N/2$ componentes. O **arranjo de saída** é formado por um conjunto de componentes com índice par e outro conjunto de componentes com índice ímpar.

2.4.2 O ALGORITMO DE GOOD-THOMAS

O algoritmo de Good-Thomas [12], [26], também chamado de algoritmo do fator primo (PFA, *Prime factor algorithm*) é um algoritmo FFT que re-expressa a DFT de comprimento $N = n_1 n_2$ como uma DFT bidimensional $n_1 \text{ x } n_2$, mas somente para os casos em que n_1 e n_2 são relativamente primos. Essas transformadas de comprimentos n_1 e n_2 podem ser calculadas recursivamente usando-se o algoritmo de Good-Thomas ou algum outro algoritmo FFT, como por exemplo, o de Cooley-Tukey.

De uma forma geral, o algoritmo de Good-Thomas baseia-se em mapear o vetor a ser transformado num arranjo bidimensional de coordenadas (i_1, i_2), sendo esse mapeamento baseado no Teorema Chinês do Resto [15].

As coordenadas do mapeamento do vetor v, com coordenadas v_i, no arranjo bidimensional, são definidas por:

$$i_1 \equiv i (\mathrm{mod}\, n_1) \text{ e } i_2 \equiv i (\mathrm{mod}\, n_2) .$$

Usando-se o Teorema Chinês do Resto, i pode ser recuperado a partir de:

$$i \equiv i_1 n_2^{-1} n_2 + i_2 n_1^{-1} n_1 (\mathrm{mod}\, N) ,$$

em que n_2^{-1} é o inverso multiplicativo de n_2 módulo n_1 e n_1^{-1} é o inverso multiplicativo de n_1 módulo n_2. O vetor de entrada, agora bidimensional, será transformado no vetor de saída X de coordenadas:

$$k_1 \equiv n_2^{-1} k (\mathrm{mod}\, n_1) \text{ e } k_2 \equiv n_1^{-1} k (\mathrm{mod}\, n_2) ,$$

tal que k pode ser obtido a partir de

$$k \equiv k_1 n_2 + k_2 n_1 (\mathrm{mod}\, N) .$$

Aplicando-se a DFT ao arranjo bidimensional do vetor de entrada, tem-se:

$$X_k = \sum_{i=0}^{N-1} v_i \alpha^{ik} \Rightarrow X_{n_2 k_1 + n_1 k_2} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1 n_2^{-1} n_2 + i_2 n_1^{-1} n_1} \alpha^{(i_1 n_2^{-1} n_2 + i_2 n_1^{-1} n_1)(n_2 k_1 + n_1 k_2)} .$$

Manipulando-se os índices convenientemente e levando-se em consideração que $\alpha^N = 1$, pode-se reescrever a DFT como:

$$X_{k_1,k_2} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} \left(\alpha^{n_2^{-1} n_2^2}\right)^{i_1 k_1} \left(\alpha^{n_1^{-1} n_1^2}\right)^{i_2 k_2} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} (\beta)^{i_1 k_1} (\gamma)^{i_2 k_2} ,$$

em que $\beta = \alpha^{n_2^{-1} n_2^2}$ e $\gamma = \alpha^{n_1^{-1} n_1^2}$.

O PFA não deve ser confundido com o algoritmo de Cooley-Tukey, que também divide uma DFT de comprimento $N = n_1 n_2$ em transformadas menores de comprimentos n_1 e n_2. Esse último pode usar quaisquer fatores (não necessariamente primos entre si), mas tem a desvantagem de necessitar de multiplicações por um termo de ajuste. Por outro lado, o algoritmo de Good-Thomas

tem as desvantagens de funcionar apenas para fatores primos entre si e necessitar de uma reindexação mais complicada. O que se pode fazer é combinar os dois algoritmos para reduzir a complexidade computacional do cálculo da DFT. O algoritmo de Good-Thomas fatoraria N em fatores primos, enquanto que o de Cooley-Tukey seria usado para lidar com fatores repetidos.

2.4.3 O ALGORITMO DE GOERTZEL

A FFT permite que se calcule a DFT de uma sequência de comprimento N com complexidade computacional menor que N^2. Como calcular um único elemento da DFT requer uma complexidade computacional multiplicativa igual a N, está claro que, quando não se deseja calcular muitos elementos da DFT, é preferível calcular os elementos isoladamente, e não a sequência inteira. O algoritmo de Goertzel [13] é uma maneira simples de calcular uma componente isolada da transformada de Fourier. Por meio dele, uma componente de Fourier é obtida pela implementação de um filtro de segunda ordem. O desenvolvimento do algoritmo inicia notando-se que a DFT pode ser formulada em termos de uma convolução, explorando a periodicidade de α_N^k:

$$\begin{aligned} X_k &= \sum_{i=0}^{N-1} v_i \alpha_N^{ik} \\ &= \sum_{i=0}^{N-1} v_i \alpha_N^{-k(N-i)}, \ \alpha_N^{-kN} = 1. \\ &= \left(v_i * \alpha_N^{-ki}\right)\big|_{i=N} \\ &= \left[v_i * \left(\alpha_N^{-ki} u_i\right)\right]\big|_{i=N} = \left(v_i * h_i\right)\big|_{i=N}. \end{aligned}$$

Isso é equivalente a processar um sinal v_i através de um filtro com resposta ao impulso $h_i = \alpha_N^{-ki} u_i$. A saída do filtro em $i = N$ fornece o coeficiente da DFT de comprimento N, X_k. O filtro tem resposta em frequência dada por

$$H_k(z) = \frac{1}{1 - \alpha_N^{-k} z^{-1}} = \frac{1 - \alpha_N^k z^{-1}}{1 - 2\cos(2\pi k / N) z^{-1} + z^{-2}} \ .$$

Como se deseja calcular a saída desse filtro em um determinado ponto, o multiplicador $-\alpha_N^k$ precisa ser usado apenas uma vez. Assim, o algoritmo requer N multiplicações reais e uma única multiplicação complexa para calcular X_k para um dado k.

Embora o algoritmo de Goertzel possa ser usado para calcular uma componente da DFT, ele não é uma transformada rápida, porque sua complexidade computacional para uma DFT de comprimento N é proporcional a N^2, caso se queira calcular todas as componentes do espectro. É um procedimento atrativo, do ponto de vista de implementação, para aplicações em que apenas um número de componentes da DFT precisa ser calculado [36].

CAPÍTULO 3
TRANSFORMADAS TRIGONOMÉTRICAS SOBRE CORPOS FINITOS

Transformadas trigonométricas são largamente utilizadas em processamento e compressão de sinais e imagens. Exemplos de tais transformadas são as transformadas discretas do cosseno (DCT, *Discrete Cossine Transform*) e as transformadas discretas do seno (DST, *Discrete Sine Transform*). A DCT, especialmente, tem sido a base para alguns padrões de compactação como o JPEG (*Joint Photographic Experts Group*) e o MPEG (*Moving Picture Experts Group*) e tem sido muito usada também em aplicações como marca d'água digital [27], [28], [29]. O desenvolvimento de algoritmos rápidos para a implementação da DCT tem contribuído ainda mais com a sua popularidade.

De forma análoga ao que acontece nos reais [30], existem 16 transformadas trigonométricas sobre corpos finitos, oito do tipo cosseno e oito do tipo seno. A primeira transformada do cosseno sobre corpos finitos foi introduzida por Campello de Souza et al., em 2004 [2], e a primeira transformada do seno sobre corpos finitos foi introduzida por Campello de Souza em 2005 [3]. Posteriormente, as outras 14 transformadas foram construídas, constituindo a família das transformadas trigonométricas sobre corpos finitos (FFTTs, *finite field trigonometric transforms*) [4].

Neste capítulo, dar-se-á atenção especial às transformadas do cosseno tipo 4 par e seno tipo 4 par [4], já que serão as bases para a construção de alguns dos tipos dos códigos corretores de erros descritos nesta dissertação.

3.1 NÚMEROS COMPLEXOS SOBRE CORPOS FINITOS

Definição 3.1.1 O conjunto de inteiros gaussianos sobre $GF(p)$ é o conjunto $GI(p) = \{a + jb, a, b \in GF(p)\}$, em que p é um número primo tal que $j^2 = -1$ é um resíduo não-quadrático sobre $GF(p)$, ou seja, $p \equiv 3 \equiv -1 (\text{mod } 4)$. ■

Proposição 3.1.1 O corpo de extensão $GF(p^2)$ é isomórfico à estrutura $GI(p)$ [31]. ■

Definição 3.1.2 O **conjunto unimodular** de $GI(p)$, denotado por G_1, é o conjunto de elementos $\zeta = (a + jb) \in GI(p)$, tais que $a^2 + b^2 \equiv 1 (\text{mod } p)$. ■

Os inteiros gaussianos possuem algumas propriedades importantes, que envolvem conceitos como a norma quadrática e a ordem complexa.

Definição 3.1.3 Norma Quadrática: Seja $\zeta = a + jb \in GI(q^m)$. A Norma Quadrática desse elemento é definida como:

$$|\zeta|^2 = |a + jb|^2 = a^2 + b^2 \in GF(q^m).$$

■

Definição 3.1.4 Ordem complexa: Seja $\zeta = a + jb \in GI(q^m)$. Define-se a ordem complexa desse elemento, $ord(\zeta)$, como sendo o menor número natural N tal que $(a + jb)^N \equiv 1 (\mathrm{mod}\, q^m)$. ■

No **Apêndice D,** são mostrados alguns elementos unimodulares, assim como suas ordens complexas.

Algumas propriedades dos inteiros gaussianos sobre corpos finitos podem ser demonstradas para $\zeta = a + jb \in GI(q)$, com $q = p^r$ [32].

(a) $ord(\zeta) \mid (q+1)(q-1)$;

(b) $\zeta^q = \zeta^*$, onde * denota o complexo conjugado;

(c) $\zeta^{q+1} = |\zeta|^2 = a^2 + b^2$;

Prova: $\zeta^q = (a + jb)^q \equiv a^p + j^p b^p (\mathrm{mod}\, p)$, pois $G_1(p)$ é isomorfo a $GF(p^2)$, um corpo de característica p. Como $p \equiv 3 (\mathrm{mod}\, 4)$, $j^p = -j$, de modo $\zeta^q \equiv a - jb = \zeta^* (\mathrm{mod}\, p)$. Portanto, $\zeta^{q+1} = \zeta^q \zeta \equiv \zeta^* \zeta = |\zeta|^2 (\mathrm{mod}\, p)$. ■

Proposição 3.1.2 G_1 é um grupo cíclico de ordem $(p+1)$ [33].

Prova: G_1 é fechado em relação à multiplicação, pois se $(a + jb)$ e $(c + jd)$ estão em G_1, isto é, se $a^2 + b^2 \equiv c^2 + d^2 \equiv 1 (\mathrm{mod}\, p)$, então,

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

de modo que

$$e^2 + f^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2$$

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2)$$

$$= (a^2 + b^2)(c^2 + d^2) \equiv 1 (\text{mod } p),$$

e portanto, $(e + jf) \in G_1$. Por outro lado, o conjunto dos elementos não-nulos de $GF(p^2)$, juntamente com a operação de multiplicação do corpo, forma um grupo cíclico de ordem $(p^2 - 1)$ (denotado aqui por G). Portanto, sendo G_1 um subconjunto fechado de G, o mesmo é um subgrupo cíclico de G [34]. Além disso, da propriedade (c), $\zeta \in G_1$ satisfaz $\zeta^{p+1} \equiv 1 (\text{mod } p)$ e ζ é uma das $(p+1)$ raízes da unidade em $GF(p^2)$. Como existem $(p+1)$ tais raízes, G_1 tem ordem $(p+1)$. ■

Corolário 3.1.1 A ordem N de ζ divide $(p+1)$ [34]. ■

Exemplo 3.1: Os grupos unimodulares $GI(19)$ e $GI(23)$. A Tabela 3.1 mostra os elementos dos subgrupos G_1 de ordens $p_1 + 1 = 20$ e $p_2 + 1 = 24$, e suas respectivas ordens.

Tabela 3.1 – *Elementos dos grupos unimodulares de (a) $GI(19)$ e (b) $GI(23)$.*

(a)

ζ	*ordem*
1	1
-1	2
j,-*j*	4
2+4*j*,2+15*j*,7+3*j*,7+16*j*	5
12+3*j*,12+16*j*,17+4*j*,17+15*j*	10
3+7*j*,3+12*j*,4+2*j*,4+17*j*,15+2*j*,15+17*j*,16+7*j*,16+12*j*	20

(b)

ζ	*ordem*
1	1
-1	2
11+8*j*,11+15*j*	3
j,-*j*	4
12+8*j*,12+15*j*	6
9+9*j*,9+14*j*,14+9*j*,14+14*j*	8
8+11*j*,8+12*j*,15+11*j*,15+12*j*	12
4+10*j*,4+13*j*,10+4*j*,10+19*j*,13+4*j*,13+19*j*,19+10*j*,19+13*j*	24

3.2 FUNÇÕES TRIGONOMÉTRICAS SOBRE CORPOS FINITOS

Nesta seção serão revistas as funções trigonométricas sobre corpos finitos. Tais funções foram inicialmente propostas por Campello de Souza et al., para se definir a transformada de Hartley sobre corpos finitos (FFHT, *finite field Hartley transform*) [31].

Definição 3.2.1 Seja ζ um elemento não-nulo de $GI(p)$, $p \equiv 3 (\mathrm{mod}\, 4)$, com ordem multiplicativa denotada por $ord(\zeta)$. As funções trigonométricas cosseno e seno sobre corpos finitos relacionadas à ζ são calculadas módulo p, respectivamente, por

$$\cos_\zeta(x) = (2^{-1} \bmod p)(\zeta^x + \zeta^{-x})$$

e

$$sen_\zeta(x) = (2^{-1} \bmod p)(\zeta^x - \zeta^{-x})/j,$$

em que $x = 0,1,\ldots,ord(\zeta)-1$ [31]. ■

As funções trigonométricas sobre corpos finitos se assemelham muito às funções trigonométricas sobre os reais, possuindo propriedades similares, como se pode ver a seguir.

Propriedade 3.2.1 Círculo Unitário:

$$sen_\zeta^2(x) + \cos_\zeta^2(x) = 1\,.$$

Prova:

$$\left(\frac{\zeta^x - \zeta^{-x}}{2j}\right)^2 + \left(\frac{\zeta^x + \zeta^{-x}}{2}\right)^2 = -\frac{1}{4}\left(\zeta^{2x} - 2 + \zeta^{-2x}\right) + \frac{1}{4}\left(\zeta^{2x} + 2 + \zeta^{-2x}\right) = 1.$$

■

Propriedade 3.2.2 Arco Duplo:

$$\text{(a)}\ \cos_\zeta^2(x) = \frac{1 + \cos_\zeta(2x)}{2}$$

e

$$\text{(b)}\ sen_\zeta^2(x) = \frac{1 - \cos_\zeta(2x)}{2}\,.$$

Prova: Para o item (a), tem-se

$$\left(\frac{\zeta^x+\zeta^{-x}}{2}\right)^2=\frac{1}{4}\left(\zeta^{2x}+2+\zeta^{-2x}\right)=\frac{1+\frac{\zeta^{2x}+\zeta^{-2x}}{2}}{2}=\frac{1+\cos_\zeta(2x)}{2}.$$

Usando um raciocínio semelhante, o resultado do item (b) pode ser obtido. ■

Propriedade 3.2.3 Adição de Arcos:

$$\text{(a)}\ \cos_\zeta(x+t)=\cos_\zeta(x)\cos_\zeta(t)-sen_\zeta(x)sen_\zeta(t)$$

e

$$\text{(b)}\ sen_\zeta(x+t)=sen_\zeta(x)\cos_\zeta(t)+sen_\zeta(t)\cos_\zeta(x).$$

Prova: Para o item (a), tem-se

$$\frac{\zeta^{x+t}+\zeta^{-(x+t)}}{2}=\frac{\zeta^x\zeta^t+\zeta^{-x}\zeta^{-t}}{2}=\frac{2\zeta^x\zeta^t+2\zeta^{-x}\zeta^{-t}}{4}$$

$$=\frac{\zeta^x+\zeta^{-x}}{2}\frac{\zeta^t+\zeta^{-t}}{2}+\frac{\zeta^x-\zeta^{-x}}{2}\frac{\zeta^t-\zeta^{-t}}{2}$$

$$=\frac{\zeta^x+\zeta^{-x}}{2}\frac{\zeta^t+\zeta^{-t}}{2}-\frac{\zeta^x-\zeta^{-x}}{2j}\frac{\zeta^t-\zeta^{-t}}{2j}$$

$$=\cos_\zeta(x)\cos_\zeta(t)-sen_\zeta(x)sen_\zeta(t).$$

Usando um raciocínio semelhante, o resultado do item (b) pode ser obtido. ■

Propriedade 3.2.4 Fórmula de Euler:

$$\zeta^x=\cos_\zeta(x)+jsen_\zeta(x).$$

Prova:

$$\cos_\zeta(x)+jsen_\zeta(x)=\frac{\zeta^x+\zeta^{-x}}{2}+j\frac{\zeta^x-\zeta^{-x}}{2j}=\zeta^x.$$

■

Propriedade 3.2.5 Simetria Par/Ímpar:

$$\text{(a)}\ \cos_\zeta(x)=\cos_\zeta(-x)$$

e

$$\text{(b)}\ sen_\zeta(x)=-sen_\zeta(-x).$$

Prova: Segue direto da Definição 3.2.1 ■

Propriedade 3.2.6 Complemento:

$$\text{(a) } \cos_\zeta(x) = \cos_\zeta(t), \text{com } xt \neq 0 \text{ e } x + t = N$$

e

$$\text{(b) } sen_\zeta(x) = -sen_\zeta(t), \text{com } xt \neq 0 \text{ e } x + t = N$$

Prova: Para o item (a), temos

$$\cos_\zeta(x) = \cos_\zeta(N-t) = \frac{\zeta^{N-t} + \zeta^{-(N-t)}}{2} \frac{\zeta^N \zeta^{-t} + \zeta^{-N}\zeta^t}{2}.$$

Sabendo-se que $\zeta^N = \zeta^{-N} = 1,$ pois ζ tem ordem $N,$ tem-se

$$\cos_\zeta(x) = \frac{\zeta^{-t} + \zeta^t}{2} = \cos_\zeta(t).$$

Usando um raciocínio semelhante, o resultado do item (b) pode ser obtido. ■

Propriedade 3.2.7 Periodicidade:

$$\text{(a) } \cos_\zeta(x + N) = \cos_\zeta(x)$$

e

$$\text{(b) } sen_\zeta(x + N) = sen_\zeta(t).$$

■

Propriedade 3.2.8 Somatório de $\cos_\zeta(x)$:

$$\sum_{x=0}^{N-1} \cos_\zeta(x) = \begin{cases} N, \text{ se x} = 0, \\ 0, \text{ se x} \neq 0. \end{cases}$$

Prova: Para $x = 0,$ tem-se

$$\cos_\zeta(x) = \frac{\zeta^0 + \zeta^{-0}}{2} = 1$$

e

$$\sum_{x=0}^{N-1} \cos_\zeta(x) = \sum_{x=0}^{N-1} 1 = N.$$

Para $x \neq 0,$ tem-se

$$\sum_{x=0}^{N-1} \cos_\zeta(x) = \frac{1}{2}(\zeta^0 + \zeta^{-0} + \zeta^1 + \zeta^{-1} + \cdots + \zeta^{N-1} + \zeta^{-(N-1)})$$

$$= \frac{1}{2}(\zeta^0 + \zeta^1 + \cdots + \zeta^{N-1}) + \frac{1}{2}(\zeta^{-0} + \zeta^{-1} + \cdots + \zeta^{-(N-1)}) = 0 + 0 = 0.$$

■

Propriedade 3.2.9 Somatório de $sen_\zeta(x)$:

$$\sum_{x=0}^{N-1} sen_\zeta(x) = 0 .$$

Prova: Para $x = 0,$ tem-se

$$sen_\zeta(x) = \frac{\zeta^0 - \zeta^{-0}}{2} = 0$$

e

$$\sum_{x=0}^{N-1} sen_\zeta(x) = \sum_{x=0}^{N-1} 0 = 0.$$

Para $x \neq 0,$ tem-se

$$\sum_{x=0}^{N-1} sen_\zeta(x) = \frac{1}{2j}(\zeta^0 - \zeta^{-0} + \zeta^1 - \zeta^{-1} + \cdots + \zeta^{N-1} - \zeta^{-(N-1)})$$

$$= \frac{1}{2j}(\zeta^0 + \zeta^1 + \cdots + \zeta^{N-1}) - \frac{1}{2j}(\zeta^{-0} + \zeta^{-1} + \cdots + \zeta^{-(N-1)}) = 0 - 0 = 0.$$

■

Lema 3.2.1 Se $\zeta = a + jb$ é um elemento unimodular de $GI(p),$ então, $\cos_\zeta(x) = \Re e\{\zeta^x\}$ e $sen_\zeta(x) = \Im m\{\zeta^x\},\ x = 0,1,\ldots,ord(\zeta) - 1$ [38].

Prova: Usando a Definição 3.2.1 e fazendo $\zeta^x = c + jd, c, d \in GF(p),$ tem-se

$$\cos_\zeta(x) = \frac{(c + jd) + (c + jd)^{-1}}{2}.$$

Devido à Proposição 3.1.2, $\zeta^x = c + jd$ é unimodular e $\zeta^{p+1} \equiv 1(\text{mod } p).$ Sabendo-se que $\zeta^p \equiv \zeta^*,$ tem-se $\zeta^* \equiv \zeta^p \Rightarrow \zeta^*\zeta = \zeta^{p+1} \Rightarrow \zeta^*\zeta \equiv 1(mop).$ Dessa forma, $\zeta^{-1} \equiv \zeta^*,$ e $(c + jd)^{-1} = c - jd.$ Portanto, pode-se escrever

$$\cos_\zeta(x) = \frac{(c + jd) + (c - jd)}{2} = c = \Re e\{\zeta^x\}.$$

Analogamente, verifica-se que $sen_\zeta(x) = d = \Im m\{\zeta^x\}.$ ■

Exemplo 3.2 Seja $\zeta = 15 + j31,$ um elemento unimodular de ordem 10 sobre $GI(79).$ As funções $\cos_\zeta(x) = \Re e\{\zeta^x\}$ e $sen_\zeta(x) = \Im m\{\zeta^x\}$ assumem os seguintes valores sobre $GF(79)$:

x	0	1	2	3	4	5	6	7	8	9
$\cos_\zeta(x)$	1	15	54	25	64	78	64	25	54	15

x	0	1	2	3	4	5	6	7	8	9
$sen_\zeta(x)$	1	31	61	61	31	0	48	18	18	48

■

3.3 AS TRANSFORMADAS TRIGONOMÉTRICAS DO COSSENO E DO SENO TIPO 4 PAR

Esta seção faz uma revisão das transformadas trigonométricas do cosseno e do seno tipo 4 par (FFCT-4P e FFST-4P, respectivamente) introduzidas por J. B. Lima [4], mostrando também suas versões unitárias. É importante observar que, nas definições e teoremas descritos a seguir, o inverso de N é calculado $(\mathrm{mod}\, p)$.

Definição 3.3.1 (FFCT-4P) Se $\zeta \in GI(p)$ tem ordem multiplicativa $2N$, então a transformada do cosseno de corpo finito da sequência $x=(x_i),\ i=0,1,\ldots,N-1,\ x_i \in GF(p),$ é a sequência $X=(X_k),\ k=0,1,\ldots,N-1,\ X_k \in GI(p),$ de elementos

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

■

Teorema 3.3.1 (FFCT-4P^{-1}) A transformada do cosseno de corpo finito inversa da sequência $X=(X_k),\ k=0,1,\ldots,N-1,\ X_k \in GI(p),$ é a sequência $x=(x_i),\ i=0,1,\ldots,N-1,\ x_i \in GF(p),$ de elementos

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

Prova: Vide [4]. ■

Definição 3.3.2 (FFST-4P) Se $\zeta \in GI(p)$ tem ordem multiplicativa $2N$, então a transformada do seno de corpo finito da sequência $x=(x_i),\ i=0,1,\ldots,N-1,\ x_i \in GF(p),$ é a sequência $X=(X_k),\ k=0,1,\ldots,N-1,\ X_k \in GI(p),$ de elementos

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

■

Teorema 3.3.2 (FFST-4P^{-1}) A transformada do seno de corpo finito inversa da sequência $X=(X_k),\ k=0,1,\ldots,N-1,\ X_k \in GI(p),$ é a sequência $x=(x_i),\ i=0,1,\ldots,N-1,\ x_i \in GF(p),$ de elementos

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

Prova: Vide [4]. ■

Matricialmente, pode-se representar uma transformada $X=(X_k),\ X_k \in GI(p),$ de uma sequência $x=(x_i),\ x_i \in GF(p),$ pela equação $X = x \text{ x } M^T,$ em que M é a matriz de transformação. Assim, denotando as matrizes de transformação do cosseno tipo 4 par por FC_{4p} e as do seno tipo 4 par por $FS_{4p},$ temos que os elementos de cada uma dessas matrizes são dados, respectivamente, por

$$[FC_{4p}]_{ik} = 2\cos_\zeta((k+1/2)(i+1/2)),\ i,k = 0,1,\ldots,N-1$$

e

$$[FS_{4p}]_{ik} = 2sen_\zeta((k+1/2)(i+1/2)),\ i,k = 0,1,\ldots,N-1,$$

em que *i* e *k* são respectivamente os índices das linhas e colunas da matriz.

3.3.1 Versões Unitárias da FFCT-4P e da FFST-4P

Empregando-se um fator de normalização nas transformadas do cosseno tipo 4 par e do seno tipo 4 par, se obtém suas versões unitárias. Nesse caso, as expressões das transformadas e suas inversas são as mesmas.

Representando por $F\widetilde{C}_{4p}$ e $F\widetilde{S}_{4p},$ respectivamente, as matrizes de transformação do cosseno tipo 4 par unitária e do seno tipo 4 par unitária, tem-se que os elementos de cada uma dessas matrizes são dados por [4]

$$\left[F\widetilde{C}_{4p}\right]_{ik} = \left(\sqrt{2/N}\right)\cos_\zeta((k+1/2)(i+1/2)),\ i,k = 0,1,\ldots,N-1$$

e

$$\left[F\widetilde{S}_{4p}\right]_{ik} = \left(\sqrt{2/N}\right)sen_\zeta((k+1/2)(i+1/2)),\ i,k = 0,1,\ldots,N-1,$$

em que *i* e *k* são respectivamente os índices das linhas e colunas da matriz.

Nesta dissertação, apenas os elementos $\zeta \in G_1$ serão considerados para o cálculo das FFTTs, ou seja, serão considerados apenas os elementos $\zeta \in GI(p)$ que são unimodulares. Dessa forma, de acordo com o Lema 3.2.1, as funções $\cos_\zeta(x)$ e $sen_\zeta(x)$ assumirão apenas valores "reais", ou seja, pertencentes a $GF(p).$ Nesse caso, as transformadas são chamadas de transformadas numéricas.

Para o cálculo de cada FFTT alguns fatores devem ser considerados. Uma condição necessária para a existência das versões unitárias da FFCT-4P e da FFST-4P é a existência do elemento $\sqrt{2/N} (\mathrm{mod}\, p),$ ou seja, $2/N$ deve ser resíduo quadrático módulo $p.$ Além disso, as ordens dos elementos ζ do corpo em questão devem ser conhecidas, já que elas determinam os comprimentos das possíveis transformadas. De acordo com as definições da FFCT-4P e da FFST-4P, seriam necessários, inicialmente, para o cálculo de tais transformadas, elementos ζ com ordem $2N$. Porém, devido à presença de dois termos (½), que indicam a necessidade de extração da raiz quadrada, na definição dessas transformadas, percebe-se que são necessários elementos $\psi = \zeta^{1/4}$ com ordem multiplicativa $8N$. Uma condição necessária e suficiente para que $\zeta' \in GI(p)$ seja um resíduo quadrático módulo p, é apresentada na Proposição 3.3.1.1 a seguir. Alguns valores de elementos ζ unimodulares e suas respectivas ordens podem ser vistos no Apêndice D.

Proposição 3.3.1.1 O elemento unimodular $\zeta' = c + jd \in GI(p)$ admite raiz quadrada sobre $GI(p)$ se e somente se $\frac{-c \pm 1}{2}$ é um resíduo quadrático módulo $p.$

Prova: Seja $\zeta = a + jb \in GI(p)$ a raiz quadrada do elemento $\zeta' = c + jd \in GI(p)$, ou seja, $(a + jb)^2 = c + jd.$

Dessa forma, tem-se

$$\begin{cases} a^2 + b^2 = c, \\ 2ab = d \Rightarrow a = d/2b. \end{cases}$$

Substituindo o valor de a, tem-se

$$\frac{d^2}{4b^2} - b^2 = c \Rightarrow 4b^4 + 4cb^2 - d^2 = 0.$$

Resolvendo a equação acima para $b^2,$ tem-se

$$b^2 = \frac{-4c \pm \sqrt{16c^2 + 16d^2}}{8}.$$

Considerando o fato de que $\zeta' = c + jd \in GI(p)$ é um elemento unimodular, ou seja, $b^2 + c^2 = 1,$ tem-se

$$b^2 = \frac{-4c \pm 4}{8} = \frac{-c \pm 1}{2} \Rightarrow b = \pm\sqrt{\frac{-c \pm 1}{2}}.$$

■

Exemplos de transformadas unitárias do cosseno de corpo finito e do seno de corpo finito são mostrados a seguir.

Exemplo 3.3 (FFCT-4P) Para $p = 79,$ o elemento $\zeta = 15 + j31 \in GI(79)$ possui ordem $10 = 2N.$ Assim, a FFCT-4P tem comprimento $N = 5,$ e é dada por

$$F\widetilde{C}_{4p} = \sqrt{2/N}\,(\mathrm{mod}\,p)\begin{bmatrix} \cos_{\zeta^{1/4}}(1) & \cos_{\zeta^{1/4}}(3) & \cos_{\zeta^{1/4}}(5) & \cos_{\zeta^{1/4}}(7) & \cos_{\zeta^{1/4}}(9) \\ \cos_{\zeta^{1/4}}(3) & \cos_{\zeta^{1/4}}(9) & \cos_{\zeta^{1/4}}(15) & \cos_{\zeta^{1/4}}(21) & \cos_{\zeta^{1/4}}(27) \\ \cos_{\zeta^{1/4}}(5) & \cos_{\zeta^{1/4}}(15) & \cos_{\zeta^{1/4}}(25) & \cos_{\zeta^{1/4}}(35) & \cos_{\zeta^{1/4}}(45) \\ \cos_{\zeta^{1/4}}(7) & \cos_{\zeta^{1/4}}(21) & \cos_{\zeta^{1/4}}(35) & \cos_{\zeta^{1/4}}(49) & \cos_{\zeta^{1/4}}(63) \\ \cos_{\zeta^{1/4}}(9) & \cos_{\zeta^{1/4}}(27) & \cos_{\zeta^{1/4}}(45) & \cos_{\zeta^{1/4}}(63) & \cos_{\zeta^{1/4}}(81) \end{bmatrix}.$$

Observando o fato que $\zeta = 15 + j31$ é um elemento unimodular de $GI(79),$ de acordo com o Lema 3.2.1, a função $\cos_{\zeta}((k+1/2)(i+1/2)) = \cos_{\zeta^{1/4}}((2k+1)(2i+1))$ só terá valores sobre $GF(79).$ Dessa forma, levando-se em consideração também que $\zeta^{1/4} = 30 + 72j$ tem ordem multiplicativa $8N = 40,$ a matriz de transformação é dada por

$$F\widetilde{C}_{4p} = \sqrt{2/5}\,(\mathrm{mod}\,p)\begin{bmatrix} \Re e\left(\zeta^{(1/4).1}\right) & \Re e\left(\zeta^{(1/4).3}\right) & \Re e\left(\zeta^{(1/4).5}\right) & \Re e\left(\zeta^{(1/4).7}\right) & \Re e\left(\zeta^{(1/4).9}\right) \\ \Re e\left(\zeta^{(1/4).3}\right) & \Re e\left(\zeta^{(1/4).9}\right) & \Re e\left(\zeta^{(1/4).15}\right) & \Re e\left(\zeta^{(1/4).21}\right) & \Re e\left(\zeta^{(1/4).27}\right) \\ \Re e\left(\zeta^{(1/4).5}\right) & \Re e\left(\zeta^{(1/4).15}\right) & \Re e\left(\zeta^{(1/4).25}\right) & \Re e\left(\zeta^{(1/4).35}\right) & \Re e\left(\zeta^{(1/4).5}\right) \\ \Re e\left(\zeta^{(1/4).7}\right) & \Re e\left(\zeta^{(1/4).21}\right) & \Re e\left(\zeta^{(1/4).35}\right) & \Re e\left(\zeta^{(1/4).9}\right) & \Re e\left(\zeta^{(1/4).23}\right) \\ \Re e\left(\zeta^{(1/4).9}\right) & \Re e\left(\zeta^{(1/4).27}\right) & \Re e\left(\zeta^{(1/4).5}\right) & \Re e\left(\zeta^{(1/4).23}\right) & \Re e\left(\zeta^{(1/4).1}\right) \end{bmatrix},$$

e finalmente,

$$F\widetilde{C}_{4p} = 43.\begin{bmatrix} 30 & 75 & 35 & 8 & 72 \\ 75 & 72 & 44 & 49 & 71 \\ 35 & 44 & 44 & 35 & 35 \\ 8 & 49 & 35 & 72 & 4 \\ 72 & 71 & 35 & 4 & 30 \end{bmatrix} \equiv \begin{bmatrix} 26 & 65 & 4 & 28 & 15 \\ 65 & 15 & 75 & 53 & 51 \\ 4 & 75 & 75 & 4 & 4 \\ 28 & 53 & 4 & 15 & 14 \\ 51 & 51 & 4 & 14 & 26 \end{bmatrix}.$$

Assim, por exemplo, a FFCT-4P de $x = (7 \quad 23 \quad 40 \quad 2 \quad 6)$ é a sequência $X = (66 \quad 25 \quad 45 \quad 30 \quad 42).$

■

Exemplo 3.4 (FFST-4P) Para $p = 31,$ o elemento $\zeta = 27 + j27 \in GI(31)$ possui ordem $8 = 2N.$ Assim, a FFST-4P tem comprimento $N = 4,$ e é dada por

$$F\widetilde{S}_{4p} = \sqrt{2/N}\,(\mathrm{mod}\,p)\begin{bmatrix} sen_{\zeta^{1/4}}(1) & sen_{\zeta^{1/4}}(3) & sen_{\zeta^{1/4}}(5) & sen_{\zeta^{1/4}}(7) \\ sen_{\zeta^{1/4}}(3) & sen_{\zeta^{1/4}}(9) & sen_{\zeta^{1/4}}(15) & sen_{\zeta^{1/4}}(21) \\ sen_{\zeta^{1/4}}(5) & sen_{\zeta^{1/4}}(15) & sen_{\zeta^{1/4}}(25) & sen_{\zeta^{1/4}}(35) \\ sen_{\zeta^{1/4}}(7) & sen_{\zeta^{1/4}}(21) & sen_{\zeta^{1/4}}(35) & sen_{\zeta^{1/4}}(49) \end{bmatrix}.$$

Observando o fato que $\zeta = 27 + j27$ é um elemento unimodular de $GI(31)$, de acordo com o Lema 3.2.1, a função $sen_{\zeta}((k+1/2)(i+1/2)) = sen_{\zeta^{1/4}}((2k+1)(2i+1))$ só terá valores sobre $GF(31)$. Dessa forma, levando-se em consideração também que $\zeta^{1/4} = 5 + 21j$ tem ordem multiplicativa $8N = 32$, a matriz de transformação é dada por

$$F\widetilde{S}_{4p} = \sqrt{2/4}(\text{mod } p)\begin{bmatrix} \Im m\left(\zeta^{(1/4).1}\right) & \Im m\left(\zeta^{(1/4).3}\right) & \Im m\left(\zeta^{(1/4).5}\right) & \Im m\left(\zeta^{(1/4).7}\right) \\ \Im m\left(\zeta^{(1/4).3}\right) & \Im m\left(\zeta^{(1/4).9}\right) & \Im m\left(\zeta^{(1/4).15}\right) & \Im m\left(\zeta^{(1/4).21}\right) \\ \Im m\left(\zeta^{(1/4).5}\right) & \Im m\left(\zeta^{(1/4).15}\right) & \Im m\left(\zeta^{(1/4).25}\right) & \Im m\left(\zeta^{(1/4).35}\right) \\ \Im m\left(\zeta^{(1/4).7}\right) & \Im m\left(\zeta^{(1/4).21}\right) & \Im m\left(\zeta^{(1/4).35}\right) & \Im m\left(\zeta^{(1/4).17}\right) \end{bmatrix},$$

e finalmente,

$$F\widetilde{S}_{4p} = 27.\begin{bmatrix} 21 & 2 & 20 & 5 \\ 2 & 5 & 21 & 11 \\ 20 & 21 & 26 & 2 \\ 5 & 11 & 2 & 10 \end{bmatrix} \equiv \begin{bmatrix} 9 & 23 & 13 & 11 \\ 23 & 11 & 9 & 18 \\ 13 & 9 & 20 & 23 \\ 11 & 18 & 23 & 22 \end{bmatrix}.$$

Assim, por exemplo, a FFST-4P de $x = (5 \quad 13 \quad 26 \quad 1)$ é a sequência $X = (11 \quad 14 \quad 12 \quad 10)$. ■

3.4 PROPRIEDADES DAS FFTTs

Nesta seção, serão revistas as principais propriedades das FFTTs, dando-se ênfase às transformadas trigonométricas do cosseno tipo 4 par e do seno tipo 4 par. Serão consideradas apenas as versões unitárias das FFTTs, já que elas diferem apenas por um fator de escala e as propriedades podem ser estendidas para as versões não-unitárias [4].

Propriedade 3.4.1 Linearidade Se duas sequências $x = (x_i)$ e $y = (y_i)$, $x_i, y_i \in GF(p)$, com FFTTs dadas respectivamente por $X = (X_k)$ e $Y = (Y_k)$, $X_k, Y_k \in GI(p)$, são combinadas linearmente, isto é,

$$z = ax + by,$$

em que $a, b \in GF(p)$, então, a FFTT de $z = (z_i)$ é dada por $Z = aX + bY$. ■

Propriedade 3.4.2 Deslocamento no tempo

i) A FFCT-4P da sequência $\hat{x} = (\hat{x}_i)$, em que, para qualquer $i, \hat{x}_i = x_{i+i_0}$, é dada por

$$\widehat{C}_k = \cos_\zeta((k+1/2)i_0)C_k + sen_\zeta((k+1/2)i_0)S_k + \sum_{r=0}^{i_0-1} 2x_r\left\{(-1)^{k+1/2}-1\right\}\cos_\zeta((k+1/2)(r+1/2-i_0)),$$

em que S_k está associada à FFST-4P.

Prova: Da Definição 3.3.1, obtém-se

$$\begin{aligned}\hat{C}_k &= \sum_{i=0}^{N-1} 2\hat{x}_i \cos_\zeta((k+1/2)(i+1/2)) \\ &= \sum_{i=0}^{N-1} 2x_{i+i_0} \cos_\zeta((k+1/2)(i+1/2)) \\ &= \sum_{i=0}^{N-1} 2x_{i+i_0} \cos_\zeta((k+1/2)(i+i_0+1/2-i_0)).\end{aligned}$$

Aplicando-se a fórmula da adição de arcos para o cosseno, Propriedade 3.2.3, tem-se

$$\begin{aligned}\hat{C}_k &= \cos_\zeta((k+1/2)i_0)\sum_{i=0}^{N-1} 2x_{i+i_0} \cos_\zeta((k+1/2)(i+i_0+1/2)) \\ &+ sen_\zeta((k+1/2)i_0)\sum_{i=0}^{N-1} 2x_{i+i_0} sen_\zeta((k+1/2)(i+i_0+1/2)) .\end{aligned}$$

Para simplificar os cálculos, faz-se

$$\hat{C}'_k = \sum_{i=0}^{N-1} 2x_{i+i_0} \cos_\zeta((k+1/2)(i+i_0+1/2))$$

e

$$\hat{C}''_k = \sum_{i=0}^{N-1} 2x_{i+i_0} sen_\zeta((k+1/2)(i+i_0+1/2)) .$$

Utilizando-se a mudança de variáveis $r = i + i_0$ na expressão para $\hat{C}'_k$, tem-se

$$\begin{aligned}\hat{C}'_k &= \sum_{r=i_0}^{N+i_0-1} 2x_r \cos_\zeta((k+1/2)(r+1/2)) \\ &= \sum_{r=0}^{N-1} 2x_r \cos_\zeta((k+1/2)(r+1/2)) \\ &+ \sum_{r=N}^{N+i_0-1} 2x_r \cos_\zeta((k+1/2)(r+1/2)) \\ &- \sum_{r=0}^{i_0-1} 2x_r \cos_\zeta((k+1/2)(r+1/2)) .\end{aligned}$$

Assumindo-se que a sequência x possui período N, o deslocamento considerado equivale a um deslocamento cíclico. Assim, lembrando que $\zeta^N \equiv -1 (\mathrm{mod}\ p)$, tem-se

$$\hat{C}'_k = C_k + \sum_{r=0}^{i_0-1} 2x_r\left\{(-1)^{k+1/2}-1\right\}\cos_\zeta((k+1/2)(r+1/2)).$$

Usando-se o mesmo raciocínio, pode-se obter

$$\hat{C}''_k = S_k + \sum_{r=0}^{i_0-1} 2x_r \left\{(-1)^{k+1/2} - 1\right\} sen_\zeta((k+1/2)(r+1/2)),$$

em que S_k está associado à FFST-4P da sequência x. Substituindo-se os resultados, tem-se

$$\begin{aligned}
\hat{C}_k &= \cos_\zeta((k+1/2)i_0)C_k \\
&+ \cos_\zeta((k+1/2)i_0)\sum_{r=0}^{i_0-1} 2x_r \left\{(-1)^{k+1/2} - 1\right\} \cos_\zeta((k+1/2)(r+1/2)) \\
&+ sen_\zeta((k+1/2)i_0)S_k \\
&+ sen_\zeta((k+1/2)i_0)\sum_{r=0}^{i_0-1} 2x_r \left\{(-1)^{k+1/2} - 1\right\} sen_\zeta((k+1/2)(r+1/2)) .
\end{aligned}$$

Usando-se novamente a fórmula de adições de arcos para o cosseno, chega-se ao resultado desejado:

$$\hat{C}_k = \cos_\zeta((k+1/2)i_0)C_k + sen_\zeta((k+1/2)i_0)S_k + \sum_{r=0}^{i_0-1} 2x_r \left\{(-1)^{k+1/2} - 1\right\} \cos_\zeta((k+1/2)(r+1/2-i_0)).$$ ■

Da mesma forma, de acordo com a Definição 3.3.2, a FFST-4P da sequência $x = (x_i)$, $i = 0, 1, \ldots, N-1$, $x_i \in GF(p)$, é a sequência $S = (S_k)$, $k = 0, 1, \ldots, N-1$, $S_k \in GI(p)$, de elementos

$$S_k = \sum_{i=0}^{N-1} 2x_i sen_\zeta((k+1/2)(i+1/2)).$$

ii) A FFST-4P da sequência $\hat{x} = (\hat{x}_i)$, em que, para qualquer i, $\hat{x}_i = x_{i+i_0}$, é dada por

$$\hat{S}_k = \cos_\zeta((k+1/2)i_0)S_k - sen_\zeta((k+1/2)i_0)C_k + \sum_{r=0}^{i_0-1} 2x_r \left\{(-1)^{k+1/2} - 1\right\} sen_\zeta((k+1/2)(r+1/2-i_0)),$$

em que C_k está associada à FFCT-4P.

Prova: Da Definição 3.3.2, obtém-se

$$\begin{aligned}
\hat{S}_k &= \sum_{i=0}^{N-1} 2\hat{x}_i sen_\zeta((k+1/2)(i+1/2)) \\
&= \sum_{i=0}^{N-1} 2x_{i+i_0} sen_\zeta((k+1/2)(i+1/2)) \\
&= \sum_{i=0}^{N-1} 2x_{i+i_0} sen_\zeta((k+1/2)(i+i_0+1/2-i_0)).
\end{aligned}$$

Aplicando-se a fórmula da adição de arcos para o seno, Propriedade 3.2.3, tem-se

$$\begin{aligned}
\hat{S}_k &= \cos_\zeta((k+1/2)i_0)\sum_{i=0}^{N-1} 2x_{i+i_0} sen_\zeta((k+1/2)(i+i_0+1/2)) \\
&- sen_\zeta((k+1/2)i_0)\sum_{i=0}^{N-1} 2x_{i+i_0} \cos_\zeta((k+1/2)(i+i_0+1/2))
\end{aligned}$$

$$= \cos_\varsigma((k+1/2)i_0)\hat{C}''_k - sen_\varsigma((k+1/2)i_0)\hat{C}'_k .$$

Substituindo-se os valores de $\hat{C}''_k$ e $\hat{C}'_k$ na equação de $\hat{S}_k$, tem-se

$$\begin{aligned}\hat{S}_k &= \cos_\varsigma((k+1/2)i_0)S_k \\ &+ \cos_\varsigma((k+1/2)i_0)\sum_{r=0}^{i_0-1} 2x_r\left\{(-1)^{k+1/2}-1\right\}sen_\varsigma((k+1/2)(r+1/2)) \\ &- sen_\varsigma((k+1/2)i_0)C_k \\ &- sen_\varsigma((k+1/2)i_0)\sum_{r=0}^{i_0-1} 2x_r\left\{(-1)^{k+1/2}-1\right\}\cos_\varsigma((k+1/2)(r+1/2)).\end{aligned}$$

Usando-se novamente a fórmula de adições de arcos para o seno, chega-se ao resultado desejado:

$$\hat{S}_k = \cos_\varsigma((k+1/2)i_0)S_k - sen_\varsigma((k+1/2)i_0)C_k + \sum_{r=0}^{i_0-1} 2x_r\left\{(-1)^{k+1/2}-1\right\}sen_\varsigma((k+1/2)(r+1/2-i_0)) . \quad \blacksquare$$

Propriedade 3.4.3 Teorema de Parseval Esse teorema relaciona a energia associada a uma determinada sequência com a energia associada à sua transformada.

Se $X=(X_k),\ k=0,1,\ldots,N-1,\ X_k \in GI(p),$ é a FFTT unitária de uma sequência $x=(x_i),\ i=0,1,\ldots,N-1,\ x_i \in GF(p),$ então

$$\sum_{i=0}^{N-1}|x_i|^2 \equiv \sum_{k=0}^{N-1}|X_k|^2 \pmod p.$$

3.5 AUTOESTRUTURA DAS FFTTs

A autoestrutura das matrizes de transformação da FFCT-4P e da FFST-4P, isto é, a forma como os autovalores e autovetores dessas transformadas se relacionam, é revista nesta seção. Para o estudo dessas autoestruturas, é necessária a definição da versão generalizada da transformada de Fourier de corpo finito, a qual é denotada por GFFFT.

Definição 3.5.1 A transformada de Fourier de corpo finito generalizada

A GFFFT de uma sequência $x=(x_i)$, $i=0,1,\ldots,N-1,\quad x_i \in GF(p),$ é a sequência $X=(X_k)$, $k=0,1,\ldots,N-1,\ X_k \in GF(p),$ cuja matriz de transformação é dada por

$$FF_{N,G} = \sqrt{N^{-1}}\,\alpha^{(i+1/2)(k+1/2)}.$$

Na relação acima, α é um elemento com ordem multiplicativa $ord(\alpha)=N$ em $GF(p)$ e $p \equiv 3 \pmod 4$. O fator de escala $\sqrt{N^{-1}}$ torna a $FF_{N,G}$ unitária. Sua inversa é dada por

$$\left(FF_{N,G}\right)^{-1} = \sqrt{N^{-1}}\,\alpha^{-(i+1/2)(k+1/2)}.$$

■

A partir das propriedades da autoestrutura da GFFFT [35], as seguintes proposições relacionadas à autoestrutura da FFCT-4P e à FFST-4P são obtidas [4].

Proposição 3.5.1 Os autovetores da FFCT-4P e os da FFST-4P são construídos a partir dos autovetores da GFFFT de acordo com as relações enunciadas a seguir.

Se $x = [x_0, \ldots, x_{N-1}, -x_{N-1}, \ldots, -x_0]$ for um autovetor ímpar da matriz $FF_{2N,G}$, ou seja, $FF_{2N,G}.x^T = \lambda.x^T$ ($\lambda = \pm 1$), então $\hat{x} = [x_0, \ldots, x_{N-1}]$ será um autovetor da matriz $FC_{N,4P}$, ou seja, $FC_{N,4P}.\hat{x}^T = \lambda.\hat{x}^T$ ($\lambda = \pm 1$).

Se $x = [x_0, \ldots, x_{N-1}, -x_{N-1}, \ldots, -x_0]$ for um autovetor par da matriz $FF_{2N,G}$, ou seja, $FF_{2N,G}.x^T = \lambda.x^T$ ($\lambda = \pm j$), então $\hat{x} = [x_0, \ldots, x_{N-1}]$ será um autovetor da matriz $FS_{N,4P}$, ou seja, $FS_{N,4P}.\hat{x}^T = \lambda.\hat{x}^T$ ($\lambda = \pm j$) ■

Proposição 3.5.2 Os únicos autovalores das matrizes de transformação da FFCT-4P e da FFST-4P são 1 e -1. Suas multiplicidades são apresentadas nas Tabelas 3.2 e 3.3, respectivamente.

Tabela 3.2 *Multiplicidades dos autovalores da matriz de transformação da FFCT-4P com dimensões* N x N

N	Mult. de 1	Mult. de -1
ímpar	$\frac{N+1}{2}$	$\frac{N-1}{2}$
par	$\frac{N}{2}$	$\frac{N}{2}$

Tabela 3.3 *Multiplicidades dos autovalores da matriz de transformação da FFST-4P com dimensões* N x N

N	Mult. de 1	Mult. de -1
ímpar	$\frac{N+1}{2}$	$\frac{N-1}{2}$
par	$\frac{N}{2}$	$\frac{N}{2}$

CAPÍTULO 4
CÓDIGOS DE FOURIER

Neste capítulo será introduzida uma nova família de códigos corretores de erros, chamados de códigos de Fourier. Estes são códigos de bloco lineares, q-ários, e se baseiam na autoestrutura da FNTT [22]. As palavras-código de um código de Fourier são as autossequências da FNTT. A definição das autossequências fornece os elementos necessários para determinar a matriz de paridade, H, do código, a partir da qual os parâmetros do código n (comprimento de bloco), k (dimensão) e uma cota para a distância mínima de Hamming d, são obtidos. Além disso, será apresentada neste capítulo, uma técnica de decodificação para corrigir um e dois erros. Essa técnica é diferente das técnicas de decodificação usuais e se baseia na autoestrutura da FNTT.

4.1 CONSTRUÇÃO DOS CÓDIGOS DE FOURIER

A partir da Definição 2.1, a matriz F da transformada numérica de Fourier unitária é dada por

$$F = \left(\sqrt{N}\right)^{-1} (\mathrm{mod}\, p) \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)(N-1)} \end{pmatrix},$$

em que $\alpha \in GF(p)$ tem ordem multiplicativa N. Se $x \leftrightarrow X$ e x é uma autossequência da transformada linear F, então seu espectro satisfaz $Fx = \lambda x$, de forma que $(F - \lambda I)x = 0$, em que λ é um autovalor associado a x. Como resultado, a matriz $(F - \lambda I)$ desempenha papel semelhante ao da matriz de paridade de um código de bloco linear com comprimento $n = N$ e dimensão k, em que $n - k = posto(F - \lambda I)$. No que se segue, a forma escalonada padrão das matrizes de paridade e geradora são usadas, isto é, $H = [I_{n-k} \mid P]$ e $G = [-P^T \mid I_k]$. Quatro códigos de bloco sobre $GF(p)$ podem ser gerados, um para cada valor de λ. Os possíveis valores para p são determinados a partir das restrições impostas pela Definição 2.1, a saber, n é um resíduo quadrático de p que divide $p - 1$. Alguns desses valores podem ser vistos no Apêndice C.

Exemplo 4.1 Construção de códigos de bloco lineares a partir da FNTT de comprimento $n = 7,$ sobre $GF(29).$ Considere $\alpha = 7,$ um elemento de ordem 7 no campo dado. $\sqrt{7} \equiv 23 (\mathrm{mod}\, 29)$ e $j \equiv 12 (\mathrm{mod}\, 29).$ A partir da matriz de transformação F, obtemos

$$F - \lambda I = \begin{pmatrix} 24-\lambda & 24 & 24 & 24 & 24 & 24 & 24 \\ 24 & 23-\lambda & 16 & 25 & 1 & 7 & 20 \\ 24 & 16 & 1-\lambda & 20 & 23 & 25 & 7 \\ 24 & 25 & 20 & 16-\lambda & 7 & 23 & 1 \\ 24 & 1 & 23 & 7 & 16-\lambda & 20 & 25 \\ 24 & 7 & 25 & 23 & 20 & 1-\lambda & 16 \\ 24 & 20 & 7 & 1 & 25 & 16 & 23-\lambda \end{pmatrix}.$$

Após algumas operações elementares de linhas, as matrizes de paridade, na forma escalonada padrão, associadas com os quatro autovalores $\lambda = \pm 1, \pm j,$ são respectivamente,

$$H^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 10 & 24 \\ 0 & 1 & 0 & 0 & 0 & 0 & 28 \\ 0 & 0 & 1 & 0 & 0 & 28 & 0 \\ 0 & 0 & 0 & 1 & 0 & 24 & 4 \\ 0 & 0 & 0 & 0 & 1 & 24 & 4 \end{pmatrix}; \qquad H^{(-1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 13 & 19 \\ 0 & 1 & 0 & 0 & 0 & 0 & 28 \\ 0 & 0 & 1 & 0 & 0 & 28 & 0 \\ 0 & 0 & 0 & 1 & 0 & 19 & 9 \\ 0 & 0 & 0 & 0 & 1 & 19 & 9 \end{pmatrix};$$

$$H^{(j)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 18 \\ 0 & 0 & 0 & 1 & 0 & 0 & 19 \\ 0 & 0 & 0 & 0 & 1 & 0 & 10 \\ 0 & 0 & 0 & 0 & 0 & 1 & 11 \end{pmatrix}; \qquad H^{(-j)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 25 & 3 \\ 0 & 0 & 0 & 0 & 1 & 4 & 26 \end{pmatrix},$$

que geram os seguintes códigos de Fourier $F(n,k)$ com matrizes geradoras $G_K^{(\lambda)}$:

$$F(7,2), \qquad G_2^{(1)} = \begin{pmatrix} 19 & 0 & 1 & 5 & 5 & 1 & 0 \\ 5 & 1 & 0 & 25 & 25 & 0 & 1 \end{pmatrix};$$

$$F(7,2), \qquad G_2^{(-1)} = \begin{pmatrix} 16 & 0 & 1 & 10 & 10 & 1 & 0 \\ 10 & 1 & 0 & 20 & 20 & 0 & 1 \end{pmatrix};$$

$$F(7,1), \qquad G_1^{(j)} = \begin{pmatrix} 0 & 28 & 11 & 10 & 19 & 18 & 1 \end{pmatrix};$$

$$F(7,2), \qquad G_2^{(-j)} = \begin{pmatrix} 0 & 0 & 28 & 4 & 25 & 1 & 0 \\ 0 & 28 & 0 & 26 & 3 & 0 & 1 \end{pmatrix}.$$

4.2 OS PARÂMETROS DOS CÓDIGOS

Usando-se uma notação mais apropriada, considere o código de Fourier $F^{\lambda}(n,k,d)$. O comprimento de bloco n do código é a ordem N da matriz FNTT unitária. A dimensão do código k é a multiplicidade do autovalor associado λ, já que essa é a dimensão do subespaço gerado pelas autossequências associadas com λ [23]. As multiplicidades dos quatro autovalores são mostradas na Tabela 4.1. Devido ao fator $\left(\sqrt{N}\right)^{-1}(\text{mod } p)$ na Definição 2.1, a multiplicidade de λ depende do valor $\sqrt{N} \equiv \pm b(\text{mod } p)$ usado. Isso significa que na Tabela 4.1, as colunas 2 e 3 ou 4 e 5 poderão ser trocadas, dependendo do valor considerado b ou $(p-b)$. Pode ser observado também que os códigos de Fourier, assintoticamente, têm taxa igual a ¼. Uma cota superior para a distância mínima d é demonstrada na Proposição 4.2.1.

Tabela 4.1 *Multiplicidade dos Autovalores da FNTT unitária*.

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

Proposição 4.2.1: Seja $H^{(\lambda)} = [I_{n-k} \mid P]$ a matriz de paridade de um código de Fourier $F^{\lambda}(n,k,d)$ sobre $GF(p)$. Então a submatriz P contém uma matriz diagonal secundária D_S, de ordem k, com entradas m, em que $m = \begin{cases} p-1, \text{ se } \lambda \equiv \pm 1(\text{mod p}), \\ 1, \text{ se } \lambda \equiv \pm \text{j}(\text{mod p}). \end{cases}$

Prova: De acordo com o Lema 2.1 (ii), x é uma autossequência com simetria par se seu autovalor associado é $\lambda \equiv \pm 1(\text{mod } p)$ e com simetria ímpar se $\lambda \equiv \pm j(\text{mod } p)$. Assim, se $x \in F^{\lambda}(n,k,d)$, temos

i) Para $\lambda \equiv \pm 1(\text{mod } p)$;

Nesse caso, a palavra-código x pode ser escrita como

$$x = (x_0, x_1, x_2, x_3, \cdots, x_{N-3}, x_{N-2}, x_{N-1})$$
$$= (x_0, x_1, x_2, x_3, \cdots, x_3, x_2, x_1).$$

Na forma sistemática, $x = (c_1, c_2, \cdots, c_{n-k}, k_1, k_2, k_k)$, em que c_i e k_j representam os símbolos de paridade e informação, respectivamente. Isso leva às equações de paridade $c_2 = k_k$, $c_3 = k_{k-1}$, $c_4 = k_{k-2}$, …, $c_{k-1} = k_3$, $c_k = k_2$ e $c_{k+1} = k_1$. Essas equações, as quais não representam o conjunto completo das equações de paridade do código, na forma de matriz, correspondem à matriz D_s.

ii) Para $\lambda \equiv \pm j (\text{mod } p)$;

De forma semelhante, a condição

$$x = (x_0, x_1, x_2, x_3, \cdots, x_{N-3}, x_{N-2}, x_{N-1})$$
$$= (x_0, x_1, x_2, x_3, \cdots, -x_3, -x_2, -x_1),$$

nos leva às equações de paridade $c_2 = -k_k$, $c_3 = -k_{k-1}$, $c_4 = -k_{k-2}$, …, $c_{k-1} = -k_3$, $c_k = -k_2$ e $c_{k+1} = -k_1$, e o resultado segue. ■

Exemplo 4.2: i) Considere o código $F^1(8,3,4)$, sobre $GF(17)$ descrito pela matriz de paridade

$$H^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 3 & 5 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 16 \\ 0 & 0 & 1 & 0 & 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 1 & 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 14 & 5 & 14 \end{pmatrix}$$

Como $\lambda = 1$, x é uma autossequência com simetria par, $x = (x_0, x_1, x_2, x_3, x_4, x_3, x_2, x_1)$ $= (c_1, c_2, c_3, c_4, c_5, k_1, k_2, k_3)$. Considerando $xH^T = 0$, as seguintes equações de paridade são obtidas:

$$c_1 + 3k_1 + 5k_2 + 3k_3 = 0;$$
$$c_2 + 16k_3 = 0;$$
$$c_3 + 16k_2 = 0;$$
$$c_4 + 16k_1 = 0;$$
$$c_5 + 14k_1 + 5k_2 + 14k_3 = 0,$$

que levam a matriz D_s indicada pela parte hachurada.

ii) Considere o código $F^j(8,2,4)$, sobre $GF(17)$, com $j = 4$, descrito pela matriz de paridade

$$H^{(j)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 11 & 16 \end{pmatrix}$$

Nesse caso, $x = (x_0, x_1, x_2, x_3, x_4, -x_3, -x_2, -x_1) = (c_1, c_2, c_3, c_4, c_5, c_6, k_1, k_2)$ e as seguintes equações de paridade são obtidas:

$$c_1 = 0;$$

$$c_2 + k_2 = 0;$$

$$c_3 + k_1 = 0;$$

$$c_4 + 6k_1 + k_2 = 0;$$

$$c_5 = 0 \text{ e}$$

$$c_6 + 11k_1 + 16k_2 = 0,$$

que levam a matriz D_s indicada pela parte hachurada. ■

Proposição 4.2.2 (Cota superior para a distância mínima): A distância mínima de um código de Fourier $F^{\lambda}(n,k,d)$ satisfaz $d \le n - 2k + 2.$

Prova: De acordo com a Proposição 4.2.1, existem pelo menos $k-1$ zeros em toda coluna da submatriz P. Portanto, o peso máximo dessas colunas é $p_{\max} = (n-k)-(k-1) = n-2k-1.$ Considerando a matriz geradora $G^{(\lambda)} = [-P_{\lambda}^{T} \mid I_k]$, temos $d \le n - 2k + 2.$ ■

Corolário 4.2.1: Em $F^{\lambda}(n,k,d),$ com $\lambda = \pm j,$ a distância mínima do código satisfaz

$$\begin{cases} d \le n - 2k, \ n \text{ par}, \\ d \le n - 2k + 1, \ n \text{ ímpar}. \end{cases}$$

■

A seguir, são mostrados os parâmetros de alguns Códigos de Fourier. Para construir tais códigos usou-se o *software* MATLAB, para desenvolver programas para se calcular as transformadas numéricas de Fourier, assim como as funções básicas para sua determinação. Para cada N, comprimento da FNTT unitária, se utilizou alguns possíveis valores de p e também alguns elementos α de ordem $N,$ para gerar os quatro códigos de Fourier, um para cada valor de $\lambda.$ Pode-se observar que as dimensões dos códigos satisfazem a Tabela 4.1.

λ	N	p	α	$\sqrt{N} \pmod p$	n	k	d
1	4	5	2	2	4	2	2
-1					4	1	4
j=2					4	1	2
-j=-2					-	-	-
1	4	5	3	2	4	2	2
-1					4	1	4
j=2					-	-	-
-j=-2					4	1	2
1	4	5	2	3	4	1	4
-1					4	2	2
j=2					-	-	-
-j=-2					4	1	2
1	4	5	3	3	4	1	4
-1					4	2	2
j=2					4	1	2
-j=-2					-	-	-

λ	N	p	α	$\sqrt{N} \pmod p$	n	k	d
1	4	29	12	2	4	2	2
-1					4	1	4
j=12					4	1	2
-j=-12					-	-	-
1	4	29	17	2	4	2	2
-1					4	1	4
j=12					-	-	-
-j=-12					4	1	2
1	4	29	12	27	4	1	4
-1					4	2	2
j=12					-	-	-
-j=-12					4	1	2
1	4	29	17	27	4	1	4
-1					4	2	2
j=12					4	1	2
-j=-12					-	-	-

λ	N	p	α	$\sqrt{N} \pmod p$	n	k	d
1	5	41	10	13	5	2	3
-1					5	1	5
j=9					5	1	4
-j=-9					5	1	4
1	5	41	16	13	5	1	5
-1					5	2	3
j=9					5	1	4
-j=-9					5	1	4
1	5	41	18	13	5	1	5
-1					5	2	3
j=9					5	1	4
-j=-9					5	1	4
1	5	41	37	13	5	2	3
-1					5	1	5
j=9					5	1	4
-j=-9					5	1	4
1	5	41	10	28	5	1	5
-1					5	2	3
j=9					5	1	4
-j=-9					5	1	4
1	5	41	16	28	5	2	3
-1					5	1	5
j=9					5	1	4
-j=-9					5	1	4
1	5	41	18	28	5	2	3
-1					5	1	5
j=9					5	1	4
-j=-9					5	1	4
1	5	41	37	28	5	1	5
-1					5	2	3
j=9					5	1	4
-j=-9					5	1	4

λ	N	p	α	$\sqrt{N} \pmod p$	n	k	d
1	6	73	9	15	6	2	4
-1					6	2	4
j=27					6	1	4
-j=-27					6	1	4
1	7	29	7	6	7	2	5
-1					7	2	5
j=12					7	2	4
-j=-12					7	1	6
1	8	17	2	5	8	3	4
-1					8	2	4
j=4					8	2	4
-j=-4					8	1	6
1	9	37	7	3	9	3	3
-1					9	2	6
j=6					9	2	6
-j=-6					9	2	6
1	10	41	4	16	10	3	6
-1					10	3	6
j=9					10	2	6
-j=-9					10	2	6
1	11	89	2	10	11	3	7
-1					11	3	7
j=34					11	3	6
-j=-34					11	2	8
1	12	13	2	5	12	4	4
-1					12	3	6
j=5					12	2	6
-j=-5					12	3	4
1	16	17	3	4	16	5	4
-1					16	4	8
j=4					16	3	8
-j=-4					16	4	4

No caso em que $N = 4,$ é possível observar que os parâmetros dos códigos são independentes do valor de p utilizado. Isso se repete para os demais códigos de diferentes comprimentos. Além disso, o seguinte Lema pode ser provado:

Lema 4.2.1 Seja α^{-1} o inverso multiplicativo de α módulo p. Então, para N, p e $\sqrt{N}(\mathrm{mod}\, p)$ fixos, os parâmetros do código $F^{\lambda}(n,k,d)$ sobre $GF(p)$ gerados por α são os mesmos que os parâmetros dos códigos $F^{\lambda}(n,k,d)$ gerados por $\alpha^{-1}(\mathrm{mod}\, p)$, se $\lambda \equiv \pm 1(\mathrm{mod}\, p)$. Caso contrário, se $\lambda \equiv \pm j(\mathrm{mod}\, p)$, os resultados gerados por $\alpha^{-1}(\mathrm{mod}\, p)$ são os mesmos parâmetros que os do código $F^{-\lambda}(n,k,d)$ gerados por α.

Prova: Considere a sequência $x \in F^{\lambda}(n,k,d)$. De acordo com o Lema 2.1 (ii), x é uma autossequência com simetria par se $\lambda \equiv \pm 1(\mathrm{mod}\, p)$ e é uma sequência com simetria ímpar se $\lambda \equiv \pm j(\mathrm{mod}\, p)$. Dessa forma, considerando uma autossequência x com simetria par, $x = (x_0, x_1, x_2, \cdots, x_2, x_1)$, tem-se

$$Fx = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-2} & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-2)} & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \alpha^{N-2} & \alpha^{2(N-2)} & \cdots & \alpha^{(N-2)(N-2)} & \alpha^{(N-2)(N-1)} \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)(N-2)} & \alpha^{(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_2 \\ x_1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{-2} & \alpha^{-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{-4} & \alpha^{-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^4 & \alpha^2 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^2 & \alpha \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-2} \\ X_{N-1} \end{bmatrix},$$

$$\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-2} \\ X_{N-1} \end{bmatrix} = \begin{bmatrix} x_0 + x_1 + x_2 + \cdots + x_2 + x_1 \\ x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{-2} x_2 + \alpha^{-1} x_1 \\ x_0 + \alpha^2 x_1 + \alpha^4 x_2 + \cdots + \alpha^{-4} x_2 + \alpha^{-2} x_1 \\ \vdots \\ x_0 + \alpha^{-2} x_1 + \alpha^{-4} x_2 + \cdots + \alpha^4 x_2 + \alpha^2 x_1 \\ x_0 + \alpha^{-1} x_1 + \alpha^{-2} x_2 + \cdots + \alpha^2 x_2 + \alpha^1 x \end{bmatrix} = \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_2 \\ X_1 \end{bmatrix}.$$

Observa-se, portanto, que a FNTT de uma sequência com simetria par é a mesma tanto para α quanto para α^{-1}. Resultado semelhante pode ser obtido se uma sequência com simetria ímpar for considerada. Como a construção dos códigos de Fourier se baseia na FNTT de uma sequência x, o resultado segue. ■

Resumidamente, a Tabela 4.2 mostra os valores de n, k e d para alguns códigos de Fourier. Os valores destacados em negrito correspondem aos códigos que atingem a cota superior da distância mínima.

Tabela 4.2 *Parâmetros de alguns códigos de Fourier* $(n,k^{(\lambda)},d^{(\lambda)})$ *para* $\lambda \equiv \pm 1, \pm j \pmod p$

n	$k^{(+1)}$	$d^{(+1)}$	cota n - 2k + 2	$k^{(-1)}$	$d^{(-1)}$	cota n - 2k + 2	$k^{(+j)}$	$d^{(+j)}$	cota n - 2k + 1	$k^{(-j)}$	$d^{(-j)}$	cota n - 2k + 1
3	1	**3**	**3**	1	**3**	**3**	-	-	-	1	**2**	**2**
4	2	**2**	**2**	1	**4**	**4**	-	-	-	1	2	3
5	2	**3**	**3**	1	**5**	**5**	1	**4**	**4**	1	**4**	**4**
6	2	**4**	**4**	2	**4**	**4**	1	4	5	1	4	5
7	2	**5**	**5**	2	**5**	**5**	1	**6**	**6**	2	**4**	**4**
8	3	**4**	**4**	2	4	6	1	6	7	2	4	5
9	3	3	5	2	6	7	2	**6**	**6**	2	**6**	**6**
10	3	**6**	**6**	3	6	6	2	6	7	2	6	7
11	3	**7**	**7**	3	**7**	**7**	2	**8**	**8**	3	**6**	**6**
12	4	4	6	3	6	8	3	4	7	2	6	9
16	5	4	8	4	8	10	3	8	11	4	4	9

Nos casos observados até agora, para N primo, a cota superior para a distância mínima é satisfeita com igualdade.

4.3 CONTROLE DE ERROS BASEADO NA AUTOESTRUTURA DA FNTT

Códigos cíclicos são códigos de bloco lineares e podem ser decodificados por qualquer técnica de decodificação padrão usada para tais códigos. No entanto, a estrutura matemática adicional que esses códigos têm permite a construção de novos e mais eficientes algoritmos de decodificação. Aqui, a mesma estratégia é usada e buscam-se métodos de decodificação baseados na autoestrutura da FNTT. Nesse cenário, as condições de simetria e a possibilidade de usar algoritmos rápidos para calcular a FNTT desempenham um papel importante.

Para ilustrar as idéias básicas, duas situações diferentes são consideradas, a correção de um único erro e a correção de dois erros. Em qualquer dos casos, os passos da decodificação dependem da sequência recebida ser simétrica ou não.

4.3.1 CÁLCULO DA SÍNDROME

Considere a sequência recebida $r = x + e \pmod{p}$, em que $x \in F^{\lambda}(n,k,d)$ e e denota a sequência erro, com elementos sobre $GF(p)$. A síndrome de r é definida como $S = Fr - \lambda r$, que é zero se, e somente se, r é uma autossequência da FNTT associada ao autovalor λ. Uma transformada rápida pode ser usada para calcular S e verificar se a sequência recebida pertence ao código ou não.

4.3.2 CORREÇÃO DE UM ÚNICO ERRO

O algoritmo de decodificação é descrito considerando a possibilidade de simetria da palavra recebida.

4.3.2.1 O CASO SIMÉTRICO (SIMETRIA PAR OU SIMETRIA ÍMPAR)

Considere que a palavra recebida $r = (r_0, r_1, r_2, \ldots, r_{N-1})$ exibe o mesmo tipo de simetria mostrado pelas autossequências associadas com o autovalor λ, a saber, $x = (x_0, x_1, x_2, x_3, \cdots, x_3, x_2, x_1)$ se $\lambda = \pm 1$ e $x = (x_0, x_1, x_2, x_3, \cdots, -x_3, -x_2, -x_1)$ se $\lambda = \pm j$. No que se segue, sem perda de generalidade, $\lambda = \pm 1$ é considerado. O procedimento para $\lambda = \pm j$ segue raciocínio semelhante.

Se N é ímpar e um único erro ocorreu, então ele deve ter ocorrido na primeira posição de r, r_0, já que somente um número par de erros pode preservar a simetria. Essa condição é verificada observando-se que, de acordo com a Definição 2.1, r_0 deve satisfazer

$$r_0 = \left(\lambda\sqrt{N} - 1\right)^{-1}\left(r_1 + r_2 + \ldots + r_{N-1}\right),$$

para que r seja uma autossequência.

Se N é par, pela mesma razão, o possível erro ocorreu na posição r_0 ou na posição $r_{N/2}$. Portanto, para decodificar a sequência recebida, usa-se o seguinte algoritmo:

1. Faça $r_0 = \left(\lambda\sqrt{N} - 1\right)^{-1}\left(r_1 + r_2 + \ldots + r_{N-1}\right)$;
2. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, faça $r_{N/2} = r_0\left(\lambda\sqrt{N} - 1\right) - \left(r_1 + \ldots + r_{N/2-1} + r_{N/2+1} + \ldots + r_{N-1}\right)$;
3. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, mais de um erro ocorreu.

4.3.2.2 O CASO NÃO-SIMÉTRICO

Assim como para o caso simétrico, sem perda de generalidade, $\lambda = \pm 1$ é considerado e o procedimento para $\lambda = \pm j$ segue raciocínio semelhante. Considere a sequência recebida $r = (r_0, r_1, r_2, \ldots, r_{N-2}, r_{N-1})$. Se os símbolos r_i e r_{N-i} são diferentes, o erro ocorreu ou na posição r_i ou na posição r_{N-i}. O algoritmo de decodificação para esse caso é:

1. Substitua r_i por r_{N-i};

2. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, substitua r_{N-i} por r_i;

3. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, mais de um erro ocorreu.

4.3.3 CORREÇÃO DE DOIS ERROS

No que se segue, a ocorrência de um único erro é considerada ser um evento mais provável que a ocorrência de dois erros. Portanto, para um código corretor de dois erros, o algoritmo de decodificação consiste em aplicar primeiro o algoritmo para correção de um único erro descrito na seção anterior. Se a decodificação não for possível, a ocorrência de dois erros é assumida e a decodificação segue de acordo com o procedimento descrito a seguir. Sem perda de generalidade, N é considerado ímpar. Quando N é par, o procedimento segue raciocínio semelhante. Em particular, uma vez que a simetria é restabelecida, o símbolo $r_{N/2}$ pode ser calculado a partir dos símbolos simétricos através de sua equação de paridade.

4.3.3.1 O CASO SIMÉTRICO

Se a simetria é preservada na palavra recebida, os erros ocorreram em um par de símbolos $(r_i, r_{N-i}),\ i \neq 0$. Nesse caso, deve-se procurar em qual par de símbolos ocorreram os erros. O algoritmo de decodificação é:

1. Para $1 \leq i \leq \dfrac{N-1}{2}$ faça $r_i = \dfrac{1}{2}\left(\lambda\sqrt{N} r_0 - \sum_{\substack{j=0 \\ j \neq i, N-i}}^{N-1} r_j \right)$ e $r_{N-i} = r_i$.

2. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, mais do que dois erros ocorreram.

4.3.3.2 O CASO NÃO-SIMÉTRICO

Considere a sequência recebida $r=(r_0,r_1,r_2,\ldots,r_{N-2},r_{N-1})$. Se dois erros ocorreram, as possíveis opções são:

i) Erros nos símbolos r_0 e $r_i,\ i\neq 0.$

ii) Erros nos símbolos r_i e $r_{N-i},\ i\neq 0.$

iii) Erro no símbolo $r_i\quad i\neq 0,$ e no símbolo $r_j,\quad j\neq N-i.$

Cada caso é descrito a seguir.

i) Erros nos símbolos r_0 e $r_i,\ i\neq 0.$

Algoritmo de Decodificação 1:

1. Substitua r_i por r_{N-i};

2. Faça $r_0=\left(\lambda\sqrt{N}-1\right)^{-1}\left(r_1+r_2+\ldots+r_{N-1}\right)$;

3. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, substitua r_{N-i} por r_i e faça $r_0=\left(\lambda\sqrt{N}-1\right)^{-1}\left(r_1+r_2+\ldots+r_{N-1}\right)$;

4. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, use o Algoritmo de Decodificação 2.

Exemplo 4.3: Considere o código corretor de dois erros $F^1(7,2,5)$ sobre $GF(29),$ com $\alpha=7,$ $\sqrt{7}\equiv 6(\mathrm{mod}\,29),$ matriz geradora

$$G_7^{(1)}=\begin{pmatrix}16 & 0 & 1 & 10 & 10 & 1 & 0\\ 20 & 1 & 0 & 20 & 20 & 0 & 1\end{pmatrix},$$

e sequência recebida $r=\left(16,\ 2,\ 1,\ 10,\ 10,\ 1,\ 3\right).$

Substituindo r_1 por r_{N-1} e fazendo $r_0=(1.6-1)^{-1}\left(3+1+10+10+1+3\right)\equiv 23(\mathrm{mod}\,29),$ resulta em $r^{(1)}=\left(23,\ 3,\ 1,\ 10,\ 10,\ 1,\ 3\right)$ e $R^{(1)}=\left(23,\ 22,\ 25,\ 25,\ 25,\ 25,\ 22\right),$ em que $R^{(1)}$ representa a FNTT da sequência $r^{(1)}$. Dessa forma, $r^{(1)}$ não é uma autossequência com autovalor associado $\lambda=1.$

Substituindo r_{N-1} por r_1 e fazendo $r_0=(1.6-1)^{-1}\left(2+1+10+10+1+2\right)\equiv 11(\mathrm{mod}\,29),$ resulta em $r^{(2)}=\left(11,\ 2,\ 1,\ 10,\ 10,\ 1,\ 2\right)$ e $R^{(2)}=\left(11,\ 5,\ 17,\ 20,\ 20,\ 17,\ 5\right).$ Dessa forma, $r^{(2)}$ também não é uma

autossequência com autovalor associado $\lambda = 1$. Nesse caso a sequência não pode ser decodificada usando o Algoritmo 1.

ii) Um erro em r_i, e outro em r_{N-i}, $i \neq 0$. O algoritmo de decodificação é parecido com o do caso simétrico, com a diferença que agora as posições dos erros são conhecidas

Algoritmo de Decodificação 2:

1. Faça $r_i = \frac{1}{2}\left(\lambda\sqrt{N} r_0 - \sum_{\substack{j=0 \\ j\neq i, N-i}}^{N-1} r_j \right)$ e $r_{N-i} = r_i$.

2. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, mais do que dois erros ocorreram. ■

Exemplo 4.4: Considerando a decodificação da sequência recebida no Exemplo 4.3, tem-se

$r_{N-1} = r_1 = \frac{1}{2}\left(1.6.16 - \left(16+1+10+10+1\right)\right) = 0.$

Portanto, $r^{(1)} = \left(16,\ 0,\ 1,\ 10,\ 10,\ 1,\ 0\right)$ e $R^{(1)} = \left(16,\ 0,\ 1,\ 10,\ 10,\ 1,\ 0\right)$. Dessa forma, $r^{(1)}$ é uma autossequência com autovalor associado $\lambda = 1$, e a decodificação está completa. ■

iii) Um erro em r_i, $i \neq 0$, e outro em r_j, $j \neq N - i$. Nesse caso, é necessário fazer pelo menos 2^2 substituições para satisfazer a simetria e verificar a condição de autossequência.

Algoritmo de Decodificação 3:

1. Substitua r_i por r_{N-i} e substitua r_j por r_{N-j};

2. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, substitua r_{N-i} por r_i e substitua r_j por r_{N-j};

3. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, substitua r_i por r_{N-i} e substitua r_{N-j} por r_j;

4. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, substitua r_{N-i} por r_i e substitua r_{N-j} por r_j;

5. Se a sequência obtida é uma autossequência, a decodificação está completa. Caso contrário, mais do que dois erros ocorreram.

Exemplo 4.5: No Exemplo 4.3, considere a sequência recebida $r = (16,\ 2,\ 3,\ 10,\ 10,\ 1,\ 0)$. Percebe-se claramente que pelo menos dois erros ocorreram. Assim, usando o Algoritmo de Decodificação 3, tem-se:

Primeira possibilidade: a sequência decodificada é $r^{(1)} = (16,\ 2,\ 3,\ 10,\ 10,\ 3,\ 2)$ e seu espectro $R^{(1)} = (27,\ 13,\ 19,\ 17,\ 17,\ 19,\ 13)$;

Segunda possibilidade: a sequência decodificada é $r^{(2)} = (16,\ 2,\ 1,\ 10,\ 10,\ 1,\ 2)$ e seu espectro $R^{(2)} = (7,\ 1,\ 13,\ 16,\ 16,\ 13,\ 1)$;

Terceira possibilidade: a sequência decodificada é $r^{(3)} = (16,\ 0,\ 3,\ 10,\ 10,\ 3,\ 0)$ e seu espectro $R^{(3)} = (7,\ 12,\ 7,\ 11,\ 11,\ 7,\ 12)$;

Quarta possibilidade: a sequência decodificada é $r^{(4)} = (16,\ 0,\ 1,\ 10,\ 10,\ 1,\ 0)$ e seu espectro $R^{(4)} = (16,\ 0,\ 1,\ 10,\ 10,\ 1,\ 0)$. Então, $r^{(4)}$ é a sequência transmitida estimada. ■

Nos procedimentos de decodificação descritos, os algoritmos requerem apenas cálculos da FNTT, que podem ser implementados através de transformadas rápidas de Fourier, e operações simples tais como adições, multiplicações por constantes e substituições. Considerando que a FNTT de uma sequência simétrica exibe o mesmo tipo de simetria, é possível usar uma variação do algoritmo de Goertzel [36], no lugar de calcular a FNTT, para verificar a condição de simetria, ou seja, no lugar de verificar a simetria para a sequência inteira, é necessário verificar para, no máximo, metade dos elementos da sequência.

CAPÍTULO 5

CÓDIGOS CORRETORES DE ERROS BASEADOS NAS TRANSFORMADAS TRIGONOMÉTRICAS DE CORPO FINITO

Neste capítulo, são utilizadas duas das transformadas trigonométricas digitais, a transformada do cosseno de corpo finito e a transformada do seno de corpo finito, para a construção de novos códigos de blocos lineares não-binários. Os códigos apresentados neste capítulo são baseados na autoestrutura da FFCT unitária do tipo 4 par, FFCT-4P, e na autoestrutura da FFST unitária do tipo 4 par, FFST-4P [4], e são chamados de códigos FFCT-4P e códigos FFST-4P, respectivamente. As palavras-código dos códigos FFCT-4P e dos códigos FFST-4P são as autossequências de suas respectivas transformadas. A definição das autossequências fornece os elementos necessários para determinar a matriz de paridade, H, do código, a partir da qual os parâmetros do código, n (comprimento de bloco), k (dimensão) e d (distância mínima de Hamming), são obtidos. Um fato interessante observado é que, para alguns valores de n, os códigos são de máxima distância mínima (MDS, do inglês *maximum distance separable*).

5.1 CONSTRUÇÃO DOS CÓDIGOS FFCT-4P

A partir da Definição 3.3.1, a matriz de transformação do cosseno tipo 4 par, denotada por FC_{4P}, é dada por

$$FC_{4P} = \sqrt{\frac{2}{N}} (\mathrm{mod}\, p) \begin{pmatrix} \cos_\zeta(\frac{1}{2}.\frac{1}{2}) & \cos_\zeta(\frac{1}{2}.\frac{3}{2}) & \cdots & \cos_\zeta(\frac{1}{2}.\frac{2N-1}{2}) \\ \cos_\zeta(\frac{3}{2}.\frac{1}{2}) & \cos_\zeta(\frac{3}{2}.\frac{3}{2}) & \cdots & \cos_\zeta(\frac{3}{2}.\frac{2N-1}{2}) \\ \vdots & \vdots & \ddots & \vdots \\ \cos_\zeta(\frac{2N-1}{2}.\frac{1}{2}) & \cos_\zeta(\frac{2N-1}{2}.\frac{3}{2}) & \cdots & \cos_\zeta(\frac{2N-1}{2}.\frac{2N-1}{2}) \end{pmatrix},$$

em que $\zeta \in GF(p)$ tem ordem multiplicativa $2N$. Para ζ unimodular, tem-se

$$FC_{4P} = \sqrt{\frac{2}{N}} (\mathrm{mod}\, p) \begin{pmatrix} \Re e(\zeta^{\frac{1}{2}.\frac{1}{2}}) & \Re e(\zeta^{\frac{1}{2}.\frac{3}{2}}) & \cdots & \Re e(\zeta^{\frac{1}{2}.\frac{2N-1}{2}}) \\ \Re e(\zeta^{\frac{3}{2}.\frac{1}{2}}) & \Re e(\zeta^{\frac{3}{2}.\frac{3}{2}}) & \cdots & \Re e(\zeta^{\frac{3}{2}.\frac{2N-1}{2}}) \\ \vdots & \vdots & \ddots & \vdots \\ \Re e(\zeta^{\frac{2N-1}{2}.\frac{1}{2}}) & \Re e(\zeta^{\frac{2N-1}{2}.\frac{3}{2}}) & \cdots & \Re e(\zeta^{\frac{2N-1}{2}.\frac{2N-1}{2}}) \end{pmatrix}.$$

Se $x \leftrightarrow X$ e x é uma autossequência da transformada linear FC_{4P}, então seu espectro satisfaz $FC_{4P}x = \lambda x$, de forma que $(FC_{4P} - \lambda I)x = 0$. Como resultado, a matriz $(FC_{4P} - \lambda I)$ desempenha papel semelhante ao da matriz de paridade de um código de bloco linear com comprimento $n = N$ e dimensão k, em que $n - k = posto(FC_{4P} - \lambda I)$. No que se segue, a forma escalonada padrão das matrizes de paridade e geradora são usadas, isto é, $H^{(\lambda)} = [I_{n-k} \mid P_\lambda]$ e $G^{(\lambda)} = [-P_\lambda^T \mid I_k]$. Dois códigos de bloco sobre $GF(p)$ podem ser gerados, um para cada valor de λ. Os possíveis valores para p são determinados a partir das restrições impostas pela Definição 3.3.1, a saber, $\sqrt{2/N} \pmod p$ e a raiz quarta de ζ precisam existir. Além disso, se utilizará apenas ζ tais que suas raízes quartas sejam unimodulares, ou seja, devem ter ordem $8N$, de forma que os elementos da matriz FFCT-4P pertençam sempre a $GF(p)$. A partir do Corolário 3.1.1, observa-se também que, para um código de comprimento $n = N$, deve-se procurar por um elemento ζ unimodular, de ordem $2N$, tal que $2N \mid (p+1)$. Alguns tais valores podem ser vistos no Apêndice D.

Exemplo 5.1: Construção de códigos de bloco lineares a partir da FFCT-4P unitária de comprimento $N = 5$ sobre $GF(79)$. Considere $\zeta = 15 + j31$, um elemento unimodular de ordem $10 = 2N$, sobre $GI(79)$. A partir da matriz de transformação FC_{4P} obtém-se

$$FC_{4P} - \lambda I = \begin{pmatrix} 26-\lambda & 65 & 4 & 28 & 15 \\ 65 & 15-\lambda & 75 & 53 & 51 \\ 4 & 75 & 75-\lambda & 4 & 4 \\ 28 & 53 & 4 & 15-\lambda & 14 \\ 15 & 51 & 4 & 14 & 26-\lambda \end{pmatrix}.$$

Após algumas operações elementares de linhas, as matrizes de paridade, na forma escalonada padrão, associadas com os dois autovalores $\lambda = \pm 1$, são, respectivamente,

$$H^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 72 & 6 \\ 0 & 1 & 0 & 6 & 74 \\ 0 & 0 & 1 & 52 & 8 \end{pmatrix}$$

e

$$H^{(-1)} = \begin{pmatrix} 1 & 0 & 71 & 74 & 73 \\ 0 & 1 & 52 & 73 & 72 \end{pmatrix},$$

que geram os seguintes códigos $FC_{4P}{}^{(\lambda)}(n,k)$ com matrizes geradoras $G^{(\lambda)}$:

$$FC_{4P}{}^{(1)}(5,2), \qquad G^{(1)} = \begin{pmatrix} 7 & 73 & 27 & 1 & 0 \\ 73 & 5 & 71 & 0 & 1 \end{pmatrix},$$

$$FC_{4P}{}^{(-1)}(5,3), \qquad G^{(-1)} = \begin{pmatrix} 8 & 27 & 1 & 0 & 0 \\ 5 & 6 & 0 & 1 & 0 \\ 6 & 7 & 0 & 0 & 1 \end{pmatrix}.$$

■

5.2 PARÂMETROS DOS CÓDIGOS FFCT-4P

De uma forma mais apropriada, considere o código $FC_{4P}{}^{\lambda}(n,k,d)$. O comprimento de bloco n do código é a ordem N da matriz FFCT-4P unitária. A dimensão do código k é a multiplicidade do autovalor associado λ, já que essa é a dimensão do subespaço gerado pelas autossequências associadas com λ [23]. As multiplicidades dos dois autovalores são mostradas na Tabela 3.2 [4]. Devido ao fator $\sqrt{2/N} \pmod p$ na Definição 3.3.1, a multiplicidade de λ depende do valor $\sqrt{2/N} \equiv \pm c \pmod p$ usado. Isso significa que na Tabela 3.2, as colunas correspondentes aos autovalores 1 e -1 são trocadas, dependendo do valor considerado $(c \text{ ou } (p-c))$. Pode ser observado também que os códigos baseados na FFCT-4P, assintoticamente, têm taxa igual a ½.

A Tabela 5.1 mostra os valores de n, k e d para alguns códigos baseados na FFCT-4P, assim como a cota $d \le n-k+1$. Pode-se observar que para alguns valores de n, tais códigos são MDS, ou seja, $d_{\min} = n-k+1$. Os valores em negrito representam os valores da distância mínima que atingem a cota de Singleton, $d_{\min} = n-k+1$.

Tabela 5.1 *Parâmetros de alguns códigos FFCT-4P:* $(n, p, \zeta, k^{(\lambda)}, d^{(\lambda)})$ *para* $\lambda \equiv \pm 1 \pmod p$

n	p	ζ	$k^{(+1)}$	$d^{(+1)}$	cota n - k + 1	$k^{(-1)}$	$d^{(-1)}$	cota n - k + 1
3	47	24+*j*41	1	**3**	**3**	2	**2**	**2**
4	31	4+*j*27	2	**3**	**3**	2	**3**	**3**
5	79	15+*j*31	2	**4**	**4**	3	**3**	**3**
6	47	6+*j*23	3	**4**	**4**	3	**4**	**4**
7	167	74+*j*161	3	**5**	**5**	4	**4**	**4**
8	127	21+*j*103	4	4	5	4	4	5
9	71	8+*j*24	4	5	6	5	3	5
10	79	18+*j*25	5	5	6	5	5	6

5.3 CONSTRUÇÃO DOS CÓDIGOS FFST-4P

A partir da Definição 3.3.2, a matriz de transformação do seno tipo 4 par, denotada por FS_{4P} é dada por

$$FS_{4P} = \sqrt{\frac{2}{N}} (\text{mod}\, p) \begin{pmatrix} sen_{\zeta}(\frac{1}{2}.\frac{1}{2}) & sen_{\zeta}(\frac{1}{2}.\frac{3}{2}) & \cdots & sen_{\zeta}(\frac{1}{2}.\frac{2N-1}{2}) \\ sen_{\zeta}(\frac{3}{2}.\frac{1}{2}) & sen_{\zeta}(\frac{3}{2}.\frac{3}{2}) & \cdots & sen_{\zeta}(\frac{3}{2}.\frac{2N-1}{2}) \\ \vdots & \vdots & \ddots & \vdots \\ sen_{\zeta}(\frac{2N-1}{2}.\frac{1}{2}) & sen_{\zeta}(\frac{2N-1}{2}.\frac{3}{2}) & \cdots & sen_{\zeta}(\frac{2N-1}{2}.\frac{2N-1}{2}) \end{pmatrix},$$

em que $\zeta \in GF(p)$ tem ordem multiplicativa $2N$. Para ζ unimodular, tem-se

$$FS_{4P} = \sqrt{\frac{2}{N}} (\text{mod}\, p) \begin{pmatrix} \Im m(\zeta^{\frac{1}{2}.\frac{1}{2}}) & \Im m(\zeta^{\frac{1}{2}.\frac{3}{2}}) & \cdots & \Im m(\zeta^{\frac{1}{2}.\frac{2N-1}{2}}) \\ \Im m(\zeta^{\frac{3}{2}.\frac{1}{2}}) & \Im m(\zeta^{\frac{3}{2}.\frac{3}{2}}) & \cdots & \Im m(\zeta^{\frac{3}{2}.\frac{2N-1}{2}}) \\ \vdots & \vdots & \ddots & \vdots \\ \Im m(\zeta^{\frac{2N-1}{2}.\frac{1}{2}}) & \Im m(\zeta^{\frac{2N-1}{2}.\frac{3}{2}}) & \cdots & \Im m(\zeta^{\frac{2N-1}{2}.\frac{2N-1}{2}}) \end{pmatrix}.$$

Aqui, a matriz $(FS_{4P} - \lambda I)$, em que λ é um autovalor da FFST-4P, desempenha o papel da matriz de paridade de um código linear com comprimento $n = N$ e dimensão k, em que $n - k = posto(FS_{4P} - \lambda I)$. Da mesma forma que para os códigos FFCT-4P, dois códigos de bloco sobre $GF(p)$, códigos FFST-4P, podem ser gerados, um para cada valor de λ. Os possíveis valores para p são determinados a partir das restrições impostas pela Definição 3.3.2, a saber, $\sqrt{2/N} (\text{mod}\, p)$ e a raiz quarta de ζ devem existir. Além disso, serão utilizados apenas ζ tais que suas raízes quartas sejam unimodulares, ou sejam, devem ter ordem $8N$, de forma que os elementos da matriz FFST-4P pertençam sempre a $GF(p)$. A partir do Corolário 3.1.1, observa-se também que, para um código de comprimento $n = N$, deve-se procurar por um elemento ζ unimodular, de ordem $2N$, tal que $2N \mid (p+1)$. Alguns tais valores podem ser vistos no Apêndice D.

Exemplo 5.2: Construção de códigos de bloco lineares a partir da FFST-4P unitária de comprimento $N = 5$ sobre $GF(79)$. Considere $\zeta = 15 + j31$, um elemento unimodular de ordem $10 = 2N$, sobre $GI(79)$. A partir da matriz de transformação FS_{4P} obtém-se

$$FS_{4P} - \lambda I = \begin{pmatrix} 15-\lambda & 28 & 4 & 65 & 26 \\ 28 & 26-\lambda & 4 & 64 & 14 \\ 4 & 4 & 75-\lambda & 75 & 4 \\ 65 & 64 & 75 & 26-\lambda & 51 \\ 26 & 14 & 4 & 51 & 15-\lambda \end{pmatrix}.$$

Após algumas operações elementares de linhas, as matrizes de paridade, na forma escalonada padrão, associadas com os dois autovalores $\lambda = \pm 1,$ são, respectivamente,

$$H^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 14 & 13 \\ 0 & 1 & 0 & 13 & 12 \\ 0 & 0 & 1 & 54 & 35 \end{pmatrix}$$

e

$$H^{(-1)} = \begin{pmatrix} 1 & 0 & 44 & 12 & 66 \\ 0 & 1 & 54 & 66 & 14 \end{pmatrix},$$

que geram os seguintes códigos $FS_{4P}{}^{(\lambda)}(n,k)$ com matrizes geradoras $G^{(\lambda)}$:

$$FS_{4P}{}^{(1)}(5,2), \qquad G^{(1)} = \begin{pmatrix} 65 & 66 & 25 & 1 & 0 \\ 66 & 67 & 44 & 0 & 1 \end{pmatrix},$$

$$FS_{4P}{}^{(-1)}(5,3), \qquad G^{(-1)} = \begin{pmatrix} 35 & 25 & 1 & 0 & 0 \\ 67 & 13 & 0 & 1 & 0 \\ 13 & 65 & 0 & 0 & 1 \end{pmatrix}.$$

■

5.4 PARÂMETROS DOS CÓDIGOS FFST-4P

De uma forma mais apropriada, considere o código $FS_{4P}{}^{\lambda}(n,k,d).$ Assim como para os Códigos FFCT-4P, o comprimento de bloco n do código é a ordem N da matriz FFST-4P unitária. A dimensão do código k é a multiplicidade do autovalor associado $\lambda,$ e as multiplicidades dos dois autovalores são mostradas na Tabela 3.3 [4]. Pelo mesmo motivo que no caso dos Códigos FFCT-4P, na Tabela 3.3, as colunas correspondentes aos autovalores 1 e -1 são trocadas, dependendo do valor de $\sqrt{2/N} \pmod p$ considerado. Pode ser observado que os códigos baseados na FFST-4P, assintoticamente, têm também taxa igual a ½.

A Tabela 5.2 mostra os valores de n, k e d para alguns códigos baseados na FFST-4P, assim como a cota $d \le n-k+1$. Pode-se observar também que para alguns valores de n, tais códigos são MDS, ou seja, $d_{\min} = n-k+1$.

Tabela 5.2 *Parâmetros de alguns códigos FFST-4P:* $(n, p, \zeta, k^{(\lambda)}, d^{(\lambda)})$ *para* $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$

n	p	ζ	$k^{(+1)}$	$d^{(+1)}$	cota n - k + 1	$k^{(-1)}$	$d^{(-1)}$	cota n - k + 1
3	47	24+*j*41	1	**3**	**3**	2	**2**	**2**
4	31	4+*j*27	2	**3**	**3**	2	**3**	**3**
5	79	15+*j*31	2	**4**	**4**	3	**3**	**3**
6	47	6+*j*23	3	**4**	**4**	3	**4**	**4**
7	167	74+*j*161	3	**5**	**5**	4	**4**	**4**
8	127	21+*j*103	4	4	5	4	4	5
9	71	8+*j*24	5	3	5	4	5	6
10	79	18+*j*25	5	5	6	5	5	6

É interessante notar também que, embora os Códigos FFCT-4P e FFST-4P tenham matrizes de paridade diferentes, seus parâmetros n, k e d, são os mesmos. No Apêndice E são mostradas todas as matrizes de paridade e geradoras para os Códigos FFCT-4P e FFST-4P mostrados nas Tabelas 5.1 e 5.2, respectivamente.

CAPÍTULO 6
CONCLUSÕES

6.1 CÓDIGOS CONSTRUÍDOS A PARTIR DE TRANSFORMADAS DIGITAIS

A autoestrutura da transformada discreta de Fourier (DFT) clássica tem sido pesquisada recentemente e tem levado a novos resultados relativos à concepção de novos sistemas de acesso múltiplo no domínio da transformada [24]. Essa dissertação investiga novas aplicações dessa autoestrutura, porém considerando as chamadas transformadas digitais, que são definidas sobre o campo de Galois $GF(p)$, ao invés da DFT. São consideradas a DFT definida sobre $GF(p)$, denominada transformada numérica de Fourier e as transformadas de corpo finito do cosseno e do seno. O cenário alvo das investigações é o de Codificação de Canal. Dessa forma novas famílias de códigos de bloco lineares sobre $GF(p)$, $p > 2$, baseadas nas transformadas digitais, anteriormente mencionadas, são introduzidas. Em particular, as famílias dos Códigos de Fourier e a família dos Códigos do Cosseno tipo 4 par e do Seno tipo 4 par foram construídas.

6.2 CÓDIGOS DE FOURIER

As palavras-código de um código de Fourier $F^{\lambda}(n,k,d)$ são as autossequências da transformada numérica de Fourier associadas ao autovalor λ. Nessa dissertação, as matrizes de paridade, *H*, geradoras, *G*, e os parâmetros n (comprimento de bloco), k (dimensão) e d (distância mínima de Hamming) de alguns códigos de Fourier são encontrados. Uma cota superior para a distância mínina, $d \le n - 2k + 2,$ de tais códigos é demonstrada.

Estratégias para o controle de um e dois erros baseadas na autoestrutura da FNTT são examinadas, considerando-se para isso a simetria inerente às autossequências dessas transformadas. Nos procedimentos de decodificação descritos, os algoritmos requerem apenas cálculos da FNTT que podem ser implementados através de transformadas rápidas de Fourier, e operações simples como adições, multiplicações por constantes e substituições. Esses procedimentos se tornam ainda mais atrativos quando se consideram sequências simétricas para a decodificação, já que a FNTT de tais sequências exibe o mesmo tipo de simetria, e dessa forma uma variação do algoritmo de Goertzel [36] pode ser usado no lugar do cálculo da FNTT para verificar a condição de autossequência.

6.3 CÓDIGOS FFCT E FFST

As palavras-código de um código FFCT-4P $FC_{4P}{}^{\lambda}(n,k,d)$ ou de um código FFST-4P $FS_{4P}{}^{\lambda}(n,k,d)$ são as autossequências da transformada do cosseno tipo 4 par ou da transformada do seno tipo 4 par, respectivamente, associadas ao autovalor λ. As matrizes de paridade, *H*, geradoras, *G*, e os parâmetros n (comprimento de bloco), k (dimensão) e d (distância mínima de Hamming) de alguns códigos FFCT-4P e FFST-4P foram encontrados.

Observou-se nessa dissertação, que para alguns valores de n os códigos gerados a partir das transformadas do cosseno tipo 4 par e do seno tipo 4 par são MDS, ou seja, tais códigos satisfazem $d = n - k + 1$. Além disso, para os resultados obtidos, os códigos FFCT-4P e FFST-4P têm os mesmos parâmetros n, k e d, apesar de suas matrizes geradoras e de paridade serem diferentes.

6.4 CÓDIGOS DE TRANSFORMADA

A abordagem descrita nessa dissertação pode ser estendida para outras famílias de transformadas sobre corpos finitos, tais como a transformada numérica de Hartley [38] e outras transformadas trigonométricas [4]. Essas novas famílias de códigos podem ser construídas seguindo a mesma abordagem apresentada aqui e são membros de uma nova classe de códigos de bloco multiníveis, que pode ser denominada de Códigos de Transformada. Para uma dada transformada em corpo finito de comprimento N, sua autoestrutura pode ser usada para construir um código linear de comprimento N e dimensão k, em que k é a multiplicidade dos autovalores da transformada. Diferentes multiplicidades irão gerar códigos com diferentes taxas. Nesse cenário, transformadas rápidas e propriedades da autoestrutura da transformada podem ajudar na implementação do código.

As restrições dos parâmetros dos códigos que resultam do uso das transformadas padrões podem ser removidas se transformadas lineares arbitrárias forem consideradas. Nesse caso, códigos com taxas arbitrárias podem ser construídos.

6.5 SUGESTÕES PARA TRABALHOS FUTUROS

São sugestões para trabalhos futuros, na linha de pesquisa de códigos corretores de erros a partir de transformadas digitais:

- Estudo da estratégia para o controle de mais de dois erros baseada na autoestrutura da FNTT, para os Códigos de Fourier;

- Estudo de técnicas de decodificação para os Códigos FFCT-4P e FFST-4P;

- Realização de simulações envolvendo os Códigos de Fourier e os Códigos FFCT-4P e FFST-4P para comprimentos de bloco maiores, n;

- Estudo dos parâmetros de Códigos de Transformada criados a partir da autoestrutura da transformada de Hartley e das demais transformadas trigonométricas não descritas nesse trabalho;

- Criação de Códigos de Transformada a partir de novas transformadas sobre corpos finitos, ou seja, criadas de forma arbitrária a fim de se obter diferentes resultados em relação aos parâmetros do código;

- Criação de novas transformadas digitais a partir de códigos corretores de erros já existentes, ou seja, fazer o processo inverso do que foi feito nesse trabalho.

APÊNDICE A
A LEI DA RECIPROCIDADE QUADRÁTICA

A Lei da Reciprocidade Quadrática representa um dos mais interessantes resultados da teoria dos números. Ela foi demonstrada por Gauss e conjecturada anteriormente por Fermat, Euler e Legendre.

Euler se perguntava em que condições a congruência $x^2 \equiv q(\mathrm{mod}\, p)$ admitia solução para os primos p e q dados. Quando essa congruência tem solução, dizemos que q *é um resíduo quadrático de* p. Caso contrário, q *é um resíduo não quadrático de* p. Portanto, q *é um resíduo quadrático de* p quando ele admite raiz quadrada módulo p.

A lei de Gauss da Reciprocidade Quadrática afirma que se p e q são primos, há uma relação direta entre p ser quadrado módulo q e q ser quadrado módulo p. Esse teorema fornece um algoritmo rápido para determinar se a é quadrado módulo p.

Impresso em 1798, *Essai sur la theorie des nombres* introduziu ao mundo o símbolo de Legendre (a/p), que tem um papel muito importante em tornar a notação da Reciprocidade Quadrática mais conveniente [37].

Definição A.1: Seja p um número primo ímpar e a um inteiro tal que $MDC(a,p)=1$. O **símbolo de Legendre** (a/p) assume valores ± 1 dependendo se a é, ou não, um resíduo quadrático módulo p, respectivamente [15]. De uma forma mais generalizada, considera-se que (a/p) seja igual a *0* se $p \mid a$, ou seja,

$$(a/p)=\begin{cases} 0, \text{ se } p \mid \text{a}, \\ 1, \text{ se } a \text{ é um resíduo quadrático módulo } p, \\ -1, \text{ se } a \text{ não é resíduo quadrático módulo } p. \end{cases}$$

O símbolo de Legendre obedece às seguintes identidades:

Teorema A.1: Sejam a e b inteiros que são relativamente primos a p. Então,

(a) Se $a \equiv b(\mathrm{mod}\, p)$, então $(a/p)=(b/p)$.

(b) $(a^2/p)=1$.

(c) $(a/p)=a^{(p-1)/2}(\mathrm{mod}\, p)$.

(d) $(ab/p)=(a/p)(b/p)$.

(e) $(1/p)=1$ e $(-1/p)=(-1)^{(p-1)/2} \Rightarrow (-1/p)=\begin{cases}1, \text{ se } p\equiv 1(\text{mod}4),\\ -1, \text{ se } p\equiv 3(\text{mod}4).\end{cases}$

(f) $(ab^2/p)=(a/p)(b^2/p)=(a/p)$.

O principal resultado relacionado ao símbolo de Legendre é a chamada Lei da Reciprocidade Quadrática.

Teorema A.2: Lei da Reciprocidade Quadrática. Se p e q são primos ímpares distintos, então

$(p/q)=(q/p)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Corolário A.2.1: Se p e q são primos ímpares distintos, então

$$(p/q)=(q/p)=\begin{cases}1, \text{ se } p\equiv 1(\text{mod}4) \text{ ou } q\equiv 1(\text{mod}4),\\ -1, \text{ se } p\equiv q\equiv 3(\text{mod}4).\end{cases}$$

Corolário A.2.2: Se p e q são primos ímpares distintos, então

$$(p/q)=\begin{cases}(q/p), \text{ se } p\equiv 1(\text{mod}4) \text{ ou } q\equiv 1(\text{mod}4),\\ -(q/p), \text{ se } p\equiv q\equiv 3(\text{mod}4).\end{cases}$$

A partir das identidades acima, e utilizando-se o Teorema Chinês do Resto (Apêndice B) para resolver os sistemas de congruências lineares, os seguintes teoremas podem ser obtidos para o cálculo de (N/p).

Teorema A.3 (*N*=2): Se p é um primo ímpar, então

$$(2/p)=\begin{cases}1, \text{ se } p\equiv 1(\text{mod}8) \text{ ou } p\equiv 7(\text{mod}8),\\ -1, \text{ se } p\equiv 3(\text{mod}8) \text{ ou } p\equiv 5(\text{mod}8).\end{cases}$$

Teorema A.4 (*N*=3): Se $p\neq 3$ é um primo ímpar, então

$$(3/p)=\begin{cases}1, \text{ se } p\equiv \pm 1(\text{mod}12),\\ -1, \text{ se } p\equiv \pm 5(\text{mod}12).\end{cases}$$

Prova: Como $3 \equiv 3(\mathrm{mod}\,4),$ o Corolário A.2.2, do teorema A.2, implica que

$$(3/p) = \begin{cases} (p/3), \text{ se } p \equiv 1(\mathrm{mod}4), \\ -(p/3), \text{ se } p \equiv 3(\mathrm{mod}4). \end{cases}$$

Sabendo-se que $p \equiv 1(\mathrm{mod}\,3)$ ou $p \equiv 2(\mathrm{mod}\,3)$, pelos Teoremas A.1 e A.4, tem-se

$$(p/3) = \begin{cases} 1, \text{ se } p \equiv 1(\mathrm{mod}3), \\ -1, \text{ se } p \equiv 2(\mathrm{mod}3). \end{cases}$$

Assim, $(3/p) = 1$ se e somente se

$p \equiv 1(\mathrm{mod}\,4)$ e $p \equiv 1(\mathrm{mod}\,3)$

ou

$p \equiv 1(\mathrm{mod}\,4)$ e $p \equiv 2(\mathrm{mod}\,3)$. Resolvendo-se essas congruências, chega-se ao resultado desejado.

Teorema A.5 (*N*=4): Se p é um primo ímpar, então $(4/p) = 1$.

Prova: O resultado segue diretamente do Teorema A.1 (b).

Teorema A.6 (*N*=5): Se $p \neq 5$ é um primo ímpar, então

$(5/p) = 1$ se $p \equiv 1 \text{ ou } 4(\mathrm{mod}\,5)$.

Prova: Como $5 \equiv 1(\mathrm{mod}\,4)$, temos

$$(5/p) = \begin{cases} (p/5), \text{ se } p \equiv 1(\mathrm{mod}4), \\ (p/5), \text{ se } p \equiv 3(\mathrm{mod}4). \end{cases}$$

Sabendo-se que $p \equiv 1, 2, 3 \text{ ou } 4(\mathrm{mod}\,5)$, temos

$$(p/5) = \begin{cases} 1, \text{ se } p \equiv 4(\mathrm{mod}5), \\ 1, \text{ se } p \equiv 1(\mathrm{mod}5), \\ (3/5) = -1, \text{ se } p \equiv 3(\mathrm{mod}5), \\ (2/5) = -1, \text{ se } p \equiv 2(\mathrm{mod}5). \end{cases}$$

Assim, $(5/p)=1$ se e somente se

$p \equiv 1(\mathrm{mod}\,5)$ ou $p \equiv 4(\mathrm{mod}\,5)$,

e o resultado segue.

Teorema A.7 (*N*=6): Se p é um primo ímpar, então

$(6/p)=1$ se e somente se $p \equiv 1,5,19,23(\mathrm{mod}\,24)$.

Prova: Sabendo-se que

$$(2/p)=\begin{cases}1, & \text{se } p \equiv 1(\mathrm{mod}8) \text{ ou } p \equiv 7(\mathrm{mod}8),\\ -1, & \text{se } p \equiv 3(\mathrm{mod}8) \text{ ou } p \equiv 5(\mathrm{mod}8).\end{cases}$$

e

$$(3/p)=\begin{cases}1, & \text{se } p \equiv 1(\mathrm{mod}12) \text{ ou } p \equiv \text{-}1(\mathrm{mod}12),\\ -1, & \text{se } p \equiv 5(\mathrm{mod}12) \text{ ou } p \equiv -5(\mathrm{mod}12).\end{cases}$$

tem-se

$$(6/p)=1 \text{ se } \begin{cases} p \equiv 1(\mathrm{mod}8) \text{ e } p \equiv 1(\mathrm{mod}12),\\ p \equiv 1(\mathrm{mod}8) \text{ e } p \equiv \text{-}1(\mathrm{mod}12),\\ p \equiv 7(\mathrm{mod}8) \text{ e } p \equiv 1(\mathrm{mod}12),\\ p \equiv 7(\mathrm{mod}8) \text{ e } p \equiv \text{-}1(\mathrm{mod}12),\\ p \equiv 3(\mathrm{mod}8) \text{ e } p \equiv 5(\mathrm{mod}12),\\ p \equiv 3(\mathrm{mod}8) \text{ e } p \equiv \text{-}5(\mathrm{mod}12),\\ p \equiv 5(\mathrm{mod}8) \text{ e } p \equiv 5(\mathrm{mod}12),\\ p \equiv 5(\mathrm{mod}8) \text{ e } p \equiv \text{-}5(\mathrm{mod}12)\ . \end{cases}$$

e o teorema segue.

Teorema A.8 (*N*=7): Se $p \neq 7$ é um primo ímpar, então

$(7/p)=1$ se e somente se $p \equiv 1,3,9,19,25 \text{ ou } 27(\mathrm{mod}\,28)$.

Prova: Sabendo-se que $7 \equiv 3(\mathrm{mod}\,4)$,

$$(7/p)=\begin{cases}(p/7), & \text{se } p \equiv 1(\mathrm{mod}4),\\ -(p/7), & \text{se } p \equiv 3(\mathrm{mod}4).\end{cases}$$

tem-se

$$(p/7)=\begin{cases}1, \text{ se } p\equiv 1(\text{mod}7),\\ (2/7)=1, \text{ se } p\equiv 2(\text{mod}7),\\ (3/7)=-1, \text{ se } p\equiv 3(\text{mod}7),\\ (4/7)=1, \text{ se } p\equiv 4(\text{mod}7),\\ (5/7)=-1, \text{ se } p\equiv 5(\text{mod}7),\\ (6/7)=-1, \text{ se } p\equiv 6(\text{mod}4).\end{cases}$$

Portanto,

$$(7/p)=1 \text{ se } \begin{cases}p\equiv 1(\text{mod}4) \text{ e } p\equiv 1(\text{mod}7),\\ p\equiv 1(\text{mod}4) \text{ e } p\equiv 2(\text{mod}7),\\ p\equiv 1(\text{mod}4) \text{ e } p\equiv 4(\text{mod}7),\\ p\equiv 3(\text{mod}4) \text{ e } p\equiv 3(\text{mod}7),\\ p\equiv 3(\text{mod}4) \text{ e } p\equiv 5(\text{mod}7),\\ p\equiv 3(\text{mod}4) \text{ e } p\equiv 6(\text{mod}7).\end{cases}$$

e o teorema segue.

Teorema A.9 (*N*=8): Se p é um primo ímpar, então

$(8/p)=1$ se e somente se $p\equiv \pm 1(\text{mod}\,8)$.

Prova: $(8/p)=(4/p)(2/p)=(2/p)=1$ se $p\equiv \pm 1(\text{mod}\,8)$.

Teorema A.10 (*N*=9): Se p é um primo ímpar, então $(9/p)=1$.

Prova: O resultado segue diretamente do Teorema A.1 (b).

APÊNDICE B
O TEOREMA CHINÊS DO RESTO

O problema de encontrar uma solução simultânea para um sistema de congruências lineares é resolvido pelo Teorema Chinês do Resto [15], como pode ser visto a seguir.

Teorema B.1: Teorema Chinês do Resto. Sejam $n_1, n_2, \ldots, n_r$ inteiros positivos tais que $mdc(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares

$$x \equiv a_1 (\mathrm{mod} n_1)$$
$$x \equiv a_2 (\mathrm{mod} n_2)$$
$$\vdots$$
$$x \equiv a_r (\mathrm{mod} n_r)$$

tem uma solução simultânea, $\bar{x}$, que é única módulo o inteiro $n = n_1 n_2 \ldots n_r$, dada por

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r,$$

em que $N_k = \frac{n}{n_k}$ e $N_k x_k \equiv 1 (\mathrm{mod} n_k)$.

Exemplo B.1: Para o sistema de congruências $p \equiv 3(\mathrm{mod}\, 4)$ e $p \equiv 6(\mathrm{mod}\, 7)$, do Teorema A.8, temos

$n = 4.7 = 28$

e

$N_1 = \frac{n}{4} = 7, \qquad N_2 = \frac{n}{7} = 4.$

As congruências lineares

$7x_1 \equiv 1(\mathrm{mod} 4)$ e $4x_2 \equiv 1(\mathrm{mod} 7)$

são satisfeitas por $x_1 \equiv 3$ e $x_2 \equiv 2,$ respectivamente. Assim, a solução do sistema de equações é dada por $\bar{x} = 3.7.3 + 6.4.2 = 111.$

Módulo 28, temos a solução $\bar{x} = 111 \equiv 27(\mathrm{mod} 28).$

APÊNDICE C
COMPRIMENTOS *N* POSSÍVEIS PARA A FNTT

Como já foi visto no Capítulo 2 dessa dissertação, para que uma FNTT de comprimento N exista sobre $GF(p)$, é necessário que $N \mid (p-1)$ e que N seja um resíduo quadrático módulo p. Usando-se os resultados obtidos no Apêndice A, pode-se gerar a seguinte tabela, contendo valores de $N \leq 9$ e $p < 200$ para os quais a FNTT existe.

Tabela C.1 *Comprimentos N possíveis para a FNTT sobre $GF(p)$*

	N						
	3	**4**	**5**	**6**	**7**	**8**	**9**
	13	5	11	19	29	17	19
	37	13	31	43	113	41	37
	61	17	41	67	197	73	73
	73	29	61	73		89	109
	97	37	71	97		97	127
	109	41	101	139		113	163
	157	53	131	163		137	181
	181	61	151	193		193	199
	193	73	181				
p		89	191				
		97					
		101					
		109					
		113					
		137					
		149					
		157					
		173					
		181					
		193					
		197					

APÊNDICE D

TABELA DE ELEMENTOS UNIMODULARES E SUAS ORDENS

Este apêndice mostra alguns elementos unimodulares, em $GI(p)$, assim como suas respectivas ordens complexas.

Pode-se observar que, de acordo com a Proposição 3.1.2, as ordens dos elementos unimodulares, n, dividem $p+1$. Vale ressaltar também que $p \equiv 3(\mathrm{mod}\,4)$.

Tabela D.1 – *Elementos unimodulares de* $GI(7)$

ζ	*ordem*
1	1
-1	2
j,-j	4
2+2j,2+5j,5+2j,5+5j	8

Tabela D.2 – *Elementos unimodulares de* $GI(11)$

ζ	*ordem*
1	1
-1	2
5+3j,5+8j	3
j,-j	4
6+3j,6+8j	6
3+5j,3+6j,8+5j,8+6j	12

Tabela D.3 – *Elementos unimodulares de* $GI(19)$

ζ	*ordem*
1	1
-1	2
j,-j	4
2+4j,2+15j,7+3j,7+16j	5
12+3j,12+16j,17+4j,17+15j	10

3+7j,3+12j,4+2j,4+17j,15+2j,15+17j,16+7j,16+12j	20

Tabela D.4 – *Elementos unimodulares de* $GI(23)$

ζ	*ordem*
1	1
-1	2
11+8j,11+15j	3
j,-j	4
12+8j,12+15j	6
9+9j,9+14j,14+9j,14+14j	8
8+11j,8+12j,15+11j,15+12j	12
4+10j,4+13j,10+4j,10+19j,13+4j,13+19j,19+10j,19+13j	24

Tabela D.5 – *Elementos unimodulares de* $GI(31)$

ζ	*ordem*
1	1
-1	2
j,-j	4
4+4j,4+27j,27+4j,27+27j	8
7+13j,7+18j,13+7j,13+24j,18+7j,18+24j,24+13j,24+18j	16
2+11j,2+20j,5+10j,5+21j,10+5j,10+26j,11+2j,11+29j,20+2j,20+29j,21+5j,21+26j,26+10j,26+21j,29+11j,29+20j	32

Tabela D.6 – *Elementos unimodulares de* $GI(43)$

ζ	*ordem*
1	1
-1	2
j,-j	4
2+13j,2+30j,7+9j,7+34j,11+3j,11+40j,18+8j,18+35j,26+20j,26+23j	11
17+20j,17+23j,25+8j,25+35j,32+3j,32+40j,36+9j,36+34j,41+13j,41+30j	22
3+11j,3+32j,8+18j,8+25j,9+7j,9+36j,13+2j,13+41j,20+17j,20+26j,23+17j,23+26j,30+2j,30+41j,34+7j,34+36j,35+18j,35+25j,40+11j,40+32j	44

Tabela D.7 – *Elementos unimodulares de* $GI(47)$

ζ	*ordem*
1	1
-1	2
23+6j,23+41j	3
j,-j	4
24+6j,24+41j	6
20+20j,20+27j,27+20j,27+27j	8
6+23j,6+24j,41+23j,41+24j	12
9+22j,9+25j,22+9j,22+38j,25+9j,25+38j,38+22j,38+25j	16
11+16j,11+31j,16+11j,16+36j,31+11j,31+36j,36+16j,36+31j	24
4+19j,4+28j,10+18j,10+29j,18+10j,18+37j,19+4j,19+43j,28+4j,28+43j,29+10j,29+37j,37+18j,37+29j,43+19j,43+28j	48

Tabela D.8 – *Elementos unimodulares de* $GI(59)$

ζ	*ordem*
1	1
-1	2
29+24j,29+35j	3
j,-j	4
42+19j,42+40j,46+3j,46+56j	5
30+24j,30+35j	6
13+3j,13+56j,17+19j,17+40j,	10
24+29j,24+30j,35+29j,35+30j	12
22+15j,22+44j,23+11j,23+48j,49+14j,49+45j,54+25j,54+34j	15
3+13j,3+46j,19+17j,19+42j,40+17j,40+42j,56+13j,56+46j	20
5+25j,5+34j,10+14j,10+45j,36+11j,36+48j,37+15j,37+44j	30
11+23j,11+36j,14+10j,14+49j,15+22j,15+37j,25+5j,25+54j,34+5j,34+54j,44+22j,44+37j,45+10j,45+49j,48+23j,48+36j	60

Tabela D.9 – *Elementos unimodulares de* $GI(67)$

ζ	*ordem*
1	1
-1	2
j,-j	4
7+32j,7+35j,11+9j,11+58j,30+21j,30+46j,40+3j,40+64j,41+14j,41+53j,50+28j,50+39j, 57+13j,57+54j,65+8j,65+59j	17
2+8j,2+59j,10+13j,10+54j,17+28j,17+39j,26+14j,26+53j,27+3j,27+64j,37+21j,37+46j, 56+9j,56+58j,60+32j,60+35j	34
3+27j,3+40j,8+2j,8+65j,9+11j,9+56j,13+10j,13+57j,14+26j,14+41j,21+30j,21+37j, 28+17j,28+50j,32+7j,32+60j,35+7j,35+60j,39+17j,39+50j,46+30j,46+37j,53+26j,53+41j, 54+10j,54+57j,58+11j,58+56j,59+2j,59+65j,64+27j,64+40j	68

Tabela D.10 – *Elementos unimodulares de* $GI(71)$

ζ	*ordem*
1	1
-1	2
35+14j,35+57j	3
j,-j	4
36+14j,36+57j	6
6+6j,6+65j,65+6j,65+65j	8
23+18j,23+53j,56+29j,56+42j,63+24j,63+47j	9
14+35j,14+36j,57+35j,57+36j	12
8+24j,8+47j,15+29j,15+42j,48+18j,48+53j	18
10+16j,10+55j,16+10j,16+61j,55+10j,55+61j,61+16j,61+55j	24
18+23j,18+48j,24+8j,24+63j,29+15j,29+56j,42+15j,42+56j,47+8j,47+63j,53+23j,53+48j	36
13+20j,13+51j,20+13j,20+58j,21+25j,21+46j,25+21j,25+50j,30+33j,30+38j,33+30j, 33+41j,38+30j,38+41j,41+33j,41+38j,46+21j,46+50j,50+25j,50+46j,51+13j,51+58j, 58+20j,58+51j	72

Tabela D.11 – *Elementos unimodulares de* $GI(79)$

ζ	*ordem*
1	1
-1	2
j,-j	4
54+18j,54+61j,64+31j,64+48j	5
35+35j,35+44j,44+35j,44+44j	8
15+31j,15+48j,25+18j,25+61j	10
27+33j,27+46j,33+27j,33+52j,46+27j,46+52j,52+33j,52+46j	16
18+25j,18+54j,31+15j,31+64j48+15j,48+64j,61+25j,61+54j	20
4+8j,4+71j,7+30j,7+49j,8+4j,8+75j,30+7j,30+72j,49+7j,49+72j,71+4j,71+75j,72+30j,72+49, 75+8j,75+71j	40
2+32j,2+47j,5+23j,5+56j,6+26j,6+53j,11+14j,11+65j,14+11j,14+68j,23+5j,23+74j,26+6j,26+73j,32+2j,32+77j,47+2j,47+77j,53+6j,53+3j,56+5j,56+74j,65+11j,65+68j,68+14j,68+65j, 73+26j,73+53j,74+23j,74+56j,77+32j,77+47	80

Tabela D.12 – *Elementos unimodulares de* $GI(83)$

ζ	*ordem*
1	1
-1	2
41+35j,41+48j	3
j,-j	4
42+35j,42+48j	6
5+15j,5+68j,49+16j,49+67j,70+9j,70+74j	7
35+41j,35+42j,48+41j,48+42j	12
13+9j,13+74j,34+16j,34+67j,78+15j,78+68j	14
12+40j,12+43j,31+6j,31+77j,38+36j,38+47j,65+3j,65+80j,66+25j,66+58j,79+20j,79+63j	21
9+13j,9+70j,15+5j,15+78j,16+34j,16+49j,67+34j,67+49j,68+5j,68+78j,74+13j,74+70j	28
4+20j,4+63j,17+25j,17+58j,18+3j,18+80j,45+36j,45+47j,52+6j,52+77j,71+40j,71+43j	42
3+18j,3+65j,6+31j,6+52j,20+4j,20+79j,25+17j,25+66j,36+38j,36+45j,40+12j,40+71j,43+12j,43+71j,47+38j,47+45j,58+17j,58+66j,63+4j,63+79j,77+31j,77+52j,80+18j,80+65j	84

Tabela D.13 – *Elementos unimodulares de* $GI(103)$

ζ	*ordem*
1	1
-1	2
j,-j	4
19+19j,19+84j,84+19j,84+84j	8
6+45j,6+58j,22+49j,22+54j,28+12j,28+91j,40+7j,40+96j,71+25j,71+78j,90+48j,90+55j	13
13+48j,13+55j,32+25j,32+78j,63+7j,63+96j,75+12j,75+91j,81+49j,81+54j,97+45j, 97+58j	26
7+40j,7+63j,12+28j,12+75j,25+32j,25+71j,45+6j,45+97j,48+13j,48+90j,49+22j,49+81j, 54+22j,54+81j,55+13j,55+90j,58+6j,58+97j,78+32j,78+71j,91+28j,91+75j,96+40j, 96+63j	52
2+10j,2+93j,5+39j,5+64j,9+34j,9+69j,10+2j,10+101j,20+42j,20+61j,26+47j,26+56j, 30+50j,30+53j,34+9j,34+94j,39+5j,39+98j,42+20j,42+83j,47+26j,47+77j,50+30j,50+73j 53+30j,53+73j,56+26j,56+77j,61+20j,61+83j,64+5j,64+98j,69+9j,69+94j,73+50j,73+53j, 77+47j,77+56j,83+42j,83+61j,93+2j,93+101j,94+34j,94+69j,98+39j,98+64j,101+10j, 101+93j	104

Tabela D.14 – *Elementos unimodulares de* $GI(127)$

ζ	*ordem*
1	1
-1	2
j,-j	4
8+8j,8+119j,119+80j,119+119j	8
21+24j,21+103j,24+21j,24+106j,103+21j,103+106j,106+24j,106+103j	16
25+30j,25+97j,30+25j,30+102j,40+59j,40+68j,59+40j,59+87j,68+40j,68+87j,87+59j, 87+68j,97+25j,97+102j,102+30j,102+97j	32
7+29j,7+98j,15+41j,15+86j,29+7j,29+120j,34+49j,34+78j,41+15j,41+112j,46+60j, 46+67j,49+34j,49+93j,60+46j,60+81j,67+46j,67+81j,78+34j,78+93j,81+60j,81+67j, 86+15j,86+112j,93+49j,93+78j,98+7j,98+120j,112+41j,112+86j,120+29j,120+98j	64
2+39j,2+88j,5+22j,5+105j,9+38j,9+89j,19+23j,19+104j,22+5j,22+122j,23+19j,23+108j, 26+50j,26+77j,27+62j,27+65j,32+45j,32+82j,38+9j,38+118j,39+2j,39+125j,42+53j, 42+74j,45+32j,45+95j,50+26j,50+101j,53+42j,53+85j,62+27j,62+100j,65+77j,65+100j, 74+42j,74+85j,77+26j,77+101j,82+32j,82+95j,85+53j,85+74j,88+2j,88+125j,89+9j,	128

89+118j,95+45j,95+82j,100+62j,100+65j,101+50j,101+77j,104+19j,104+108j,105+50j, 105+122j,108+23j,108+104j,118+38j,118+89j,122+22j,122+105j,125+39j,125+88j	

Tabela D.15 – *Elementos unimodulares de GI*(167)

ζ	*ordem*
1	1
-1	2
83+31j,83+136j	3
j,-j	4
84+31j,84+136j	6
61+11j,61+156j,93+6j,93+161j,96+53j,96+114j	7
77+77j,77+90j,90+77j,90+90j	8
31+83j,31+84j,136+83j,136+84j	12
71+53j,71+114j,74+6j,74+161j,106+11j,106+156j	14
18+41j,18+126j,46+35j,46+132j,56+47j,56+120j,60+24j,60+143j,92+80j,92+87j,146+27j 146+140j	21
4+73j,4+94j,73+4j,73+163j,94+4j,94+163j,163+73j,163+94j	24
6+74j,6+93j,11+61j,11+106j,53+71j,53+96j,114+71j,114+96j,156+61j,156+106j,161+74j 161+93j	28
21+27j,21+140j,75+80j,75+87j,107+24j,107+143j,111+47j,111+120j,121+35j,121+132j, 149+41j,149+126j	42
9+33j,9+134j,19+59j,19+108j,29+50j,29+117j,33+9j,33+158j,50+29j,50+138j,59+19j, 59+148j,108+19j,108+148j,117+29j,117+138j,134+9j,134+158j,138+50j,138+117j, 148+59j,148+108j,158+33j,158+134j	56
24+60j,24+107j,27+21j,27+146j,35+46j,35+121j,41+18j,41+149j,47+56j,47+111j,80+75j 80+92j,87+75j,87+92j,120+56j,120+111j,126+18j,126+149j,132+46j,132+121j,140+21j, 140+146j,143+60j,143+107j	84
12+58j,12+109j,22+39j,22+128j,25+12j,25+85j,34+66j,34+101j,39+22j,39+145j,45+67j, 45+100j,51+78j,51+89j,58+12j,58+155j,66+34j,66+133j,67+45j,67+122j,78+51j,78+116j 82+25j,82+142j,85+25j,85+142j,89+51j,89+116j,100+45j,100+122j,101+34j,101+133j, 109+12j,109+155j,116+78j,116+89j,122+67j,122+100j,128+22j,128+145j,133+66j, 133+101j,142+82j,142+85j,145+39j,145+128j,155+58j,155+109j	168

APÊNDICE E

MATRIZES DE PARIDADE E GERADORAS DE ALGUNS CÓDIGOS FFCT-4P E FFST-4P

Este apêndice mostra todas as matrizes de paridade, H, e matrizes geradoras, G, dos códigos apresentados nas Tabelas 5.1 e 5.2. São indicados também os valores de p, ζ e λ.

Para a Tabela 5.1 as matrizes H e G dos Códigos FFCT-4P de comprimento n, sobre $GI(p)$, são:

Tabela E.1 – *Matrizes* G e H de alguns Códigos $FC_{4P}(n,k,d)$ *para* $\lambda \equiv \pm 1 (\mathrm{mod}\, p)$

n	p	ζ	λ	*Código*	G	H
3	47	24+j41	1	$FC_{4P}(3,1,3)$	$\begin{pmatrix}46 & 13 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 34\end{pmatrix}$
			-1	$FC_{4P}(3,2,2)$	$\begin{pmatrix}44 & 1 & 0\\ 43 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 3 & 4\end{pmatrix}$
4	31	4+j27	1	$FC_{4P}(4,2,3)$	$\begin{pmatrix}7 & 3 & 1 & 0\\ 4 & 24 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 24 & 27\\ 0 & 1 & 29 & 7\end{pmatrix}$
			-1	$FC_{4P}(4,2,3)$	$\begin{pmatrix}20 & 7 & 1 & 0\\ 19 & 11 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 11 & 12\\ 0 & 1 & 24 & 20\end{pmatrix}$
5	79	15+j31	1	$FC_{4P}(5,2,4)$	$\begin{pmatrix}7 & 73 & 27 & 1 & 0\\ 73 & 5 & 71 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 72 & 6\\ 0 & 1 & 0 & 6 & 74\\ 0 & 0 & 1 & 52 & 8\end{pmatrix}$
			-1	$FC_{4P}(5,3,3)$	$\begin{pmatrix}8 & 27 & 1 & 0 & 0\\ 5 & 6 & 0 & 1 & 0\\ 6 & 7 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 71 & 74 & 73\\ 0 & 1 & 52 & 73 & 72\end{pmatrix}$
6	47	6+j23	1	$FC_{4P}(6,3,4)$	$\begin{pmatrix}9 & 37 & 36 & 1 & 0 & 0\\ 8 & 44 & 10 & 0 & 1 & 0\\ 44 & 39 & 9 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 38 & 39 & 3\\ 0 & 1 & 0 & 10 & 3 & 8\\ 0 & 0 & 1 & 11 & 37 & 38\end{pmatrix}$
			-1	$FC_{4P}(6,3,4)$	$\begin{pmatrix}2 & 13 & 7 & 1 & 0 & 0\\ 28 & 16 & 34 & 0 & 1 & 0\\ 34 & 19 & 2 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 45 & 19 & 13\\ 0 & 1 & 0 & 34 & 31 & 28\\ 0 & 0 & 1 & 40 & 13 & 45\end{pmatrix}$

Tabela E.1 – *Matrizes* G e H de alguns Códigos $FC_{4P}(n,k,d)$ *para* $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$

n	p	ζ	λ	*Código*	G	H
7	167	74+j161	1	$FC_{4P}(7,3,5)$	$\begin{pmatrix} 138 & 88 & 116 & 72 & 1 & 0 & 0 \\ 20 & 67 & 46 & 81 & 0 & 1 & 0 \\ 117 & 22 & 71 & 85 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 29 & 147 & 50 \\ 0 & 1 & 0 & 0 & 79 & 100 & 145 \\ 0 & 0 & 1 & 0 & 51 & 121 & 96 \\ 0 & 0 & 0 & 1 & 95 & 86 & 82 \end{pmatrix}$
			-1	$FC_{4P}(7,4,4)$	$\begin{pmatrix} 85 & 86 & 72 & 1 & 0 & 0 & 0 \\ 96 & 46 & 51 & 0 & 1 & 0 & 0 \\ 22 & 100 & 88 & 0 & 0 & 1 & 0 \\ 50 & 20 & 29 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 82 & 71 & 145 & 117 \\ 0 & 1 & 0 & 81 & 121 & 67 & 147 \\ 0 & 0 & 1 & 95 & 116 & 79 & 138 \end{pmatrix}$
8	127	21+j103	1	$FC_{4P}(8,4,4)$	$\begin{pmatrix} 42 & 95 & 55 & 46 & 1 & 0 & 0 & 0 \\ 58 & 2 & 67 & 54 & 0 & 1 & 0 & 0 \\ 73 & 21 & 29 & 58 & 0 & 0 & 1 & 0 \\ 46 & 54 & 95 & 85 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 85 & 69 & 54 & 81 \\ 0 & 1 & 0 & 0 & 32 & 29 & 106 & 73 \\ 0 & 0 & 1 & 0 & 72 & 60 & 98 & 69 \\ 0 & 0 & 0 & 1 & 120 & 55 & 32 & 42 \end{pmatrix}$
			-1	$FC_{4P}(8,4,4)$	$\begin{pmatrix} 117 & 62 & 5 & 117 & 1 & 0 & 0 & 0 \\ 52 & 12 & 73 & 22 & 0 & 1 & 0 & 0 \\ 8 & 59 & 115 & 62 & 0 & 0 & 1 & 0 \\ 33 & 119 & 52 & 10 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 10 & 75 & 119 & 94 \\ 0 & 1 & 0 & 0 & 65 & 115 & 68 & 8 \\ 0 & 0 & 1 & 0 & 22 & 54 & 12 & 75 \\ 0 & 0 & 0 & 1 & 10 & 105 & 65 & 117 \end{pmatrix}$
9	71	8+j24	1	$FC_{4P}(9,4,5)$	$\begin{pmatrix} 31 & 45 & 36 & 13 & 45 & 1 & 0 & 0 & 0 \\ 13 & 18 & 18 & 23 & 18 & 0 & 1 & 0 & 0 \\ 8 & 42 & 38 & 49 & 41 & 0 & 0 & 1 & 0 \\ 37 & 20 & 15 & 59 & 20 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 40 & 58 & 63 & 34 \\ 0 & 1 & 0 & 0 & 0 & 26 & 53 & 29 & 51 \\ 0 & 0 & 1 & 0 & 0 & 35 & 53 & 33 & 56 \\ 0 & 0 & 0 & 1 & 0 & 58 & 48 & 22 & 12 \\ 0 & 0 & 0 & 0 & 1 & 26 & 53 & 30 & 51 \end{pmatrix}$
			-1	$FC_{4P}(9,5,3)$	$\begin{pmatrix} 51 & 41 & 53 & 45 & 1 & 0 & 0 & 0 & 0 \\ 59 & 22 & 23 & 58 & 0 & 1 & 0 & 0 & 0 \\ 56 & 38 & 53 & 36 & 0 & 0 & 1 & 0 & 0 \\ 20 & 29 & 18 & 26 & 0 & 0 & 0 & 1 & 0 \\ 34 & 8 & 58 & 31 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 20 & 12 & 15 & 51 & 37 \\ 0 & 1 & 0 & 0 & 30 & 49 & 33 & 42 & 63 \\ 0 & 0 & 1 & 0 & 18 & 48 & 18 & 53 & 13 \\ 0 & 0 & 0 & 1 & 26 & 13 & 35 & 45 & 40 \end{pmatrix}$
10	79	18+j25	1	$FC_{4P}(10,5,5)$	$\begin{pmatrix} 43 & 65 & 24 & 77 & 49 & 1 & 0 & 0 & 0 & 0 \\ 58 & 58 & 32 & 35 & 2 & 0 & 1 & 0 & 0 & 0 \\ 34 & 63 & 68 & 47 & 24 & 0 & 0 & 1 & 0 & 0 \\ 42 & 69 & 16 & 58 & 14 & 0 & 0 & 0 & 1 & 0 \\ 32 & 37 & 34 & 21 & 43 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 36 & 21 & 45 & 37 & 47 \\ 0 & 1 & 0 & 0 & 0 & 14 & 21 & 16 & 10 & 42 \\ 0 & 0 & 1 & 0 & 0 & 55 & 47 & 11 & 63 & 45 \\ 0 & 0 & 0 & 1 & 0 & 2 & 44 & 32 & 21 & 58 \\ 0 & 0 & 0 & 0 & 1 & 30 & 77 & 55 & 65 & 36 \end{pmatrix}$
			-1	$FC_{4P}(10,5,5)$	$\begin{pmatrix} 66 & 67 & 59 & 32 & 11 & 1 & 0 & 0 & 0 & 0 \\ 73 & 45 & 10 & 77 & 47 & 0 & 1 & 0 & 0 & 0 \\ 67 & 62 & 45 & 69 & 59 & 0 & 0 & 1 & 0 & 0 \\ 72 & 15 & 17 & 45 & 12 & 0 & 0 & 0 & 1 & 0 \\ 70 & 7 & 67 & 6 & 66 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 13 & 6 & 12 & 7 & 9 \\ 0 & 1 & 0 & 0 & 0 & 12 & 34 & 17 & 64 & 72 \\ 0 & 0 & 1 & 0 & 0 & 20 & 69 & 34 & 62 & 12 \\ 0 & 0 & 0 & 1 & 0 & 47 & 2 & 10 & 34 & 73 \\ 0 & 0 & 0 & 0 & 1 & 68 & 32 & 20 & 67 & 13 \end{pmatrix}$

Para a Tabela 5.2 as matrizes H e G dos Códigos FFST-4P de tamanho n, sobre $GI(p)$, são:

Tabela E.2 – *Matrizes* G e H de alguns Códigos $FS_{4P}(n,k,d)$ *para* $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$

n	p	ζ	λ	*Código*	G	H
3	47	24+j41	1	$FS_{4P}(3,1,3)$	$\begin{pmatrix}46 & 34 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 13\end{pmatrix}$
			-1	$FS_{4P}(3,2,2)$	$\begin{pmatrix}34 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 13 & 46\end{pmatrix}$
4	31	4+j27	1	$FS_{4P}(4,2,3)$	$\begin{pmatrix}7 & 29 & 1 & 0\\ 27 & 24 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 24 & 4\\ 0 & 1 & 2 & 7\end{pmatrix}$
			-1	$FS_{4P}(4,2,3)$	$\begin{pmatrix}20 & 23 & 1 & 0\\ 12 & 11 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 11 & 19\\ 0 & 1 & 7 & 20\end{pmatrix}$
5	79	15+j31	1	$FS_{4P}(5,2,4)$	$\begin{pmatrix}65 & 66 & 25 & 1 & 0\\ 66 & 67 & 44 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 14 & 13\\ 0 & 1 & 0 & 13 & 12\\ 0 & 0 & 1 & 54 & 35\end{pmatrix}$
			-1	$FS_{4P}(5,3,3)$	$\begin{pmatrix}35 & 25 & 1 & 0 & 0\\ 67 & 13 & 0 & 1 & 0\\ 13 & 65 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 44 & 12 & 66\\ 0 & 1 & 54 & 66 & 14\end{pmatrix}$;
6	47	6+j23	1	$FS_{4P}(6,3,4)$	$\begin{pmatrix}45 & 13 & 40 & 1 & 0 & 0\\ 28 & 31 & 34 & 0 & 1 & 0\\ 13 & 34 & 45 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 2 & 19 & 34\\ 0 & 1 & 0 & 34 & 16 & 28\\ 0 & 0 & 1 & 7 & 13 & 2\end{pmatrix}$
			-1	$FS_{4P}(6,3,4)$	$\begin{pmatrix}38 & 37 & 11 & 1 & 0 & 0\\ 8 & 3 & 10 & 0 & 1 & 0\\ 3 & 39 & 38 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 9 & 39 & 44\\ 0 & 1 & 0 & 10 & 44 & 8\\ 0 & 0 & 1 & 36 & 37 & 9\end{pmatrix}$
7	167	74+j161	1	$FS_{4P}(7,3,5)$	$\begin{pmatrix}15 & 34 & 117 & 70 & 1 & 0 & 0\\ 121 & 86 & 128 & 56 & 0 & 1 & 0\\ 135 & 119 & 79 & 55 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 0 & 152 & 46 & 32\\ 0 & 1 & 0 & 0 & 133 & 81 & 48\\ 0 & 0 & 1 & 0 & 50 & 39 & 88\\ 0 & 0 & 0 & 1 & 97 & 111 & 112\end{pmatrix}$
			-1	$FS_{4P}(7,4,4)$	$\begin{pmatrix}55 & 111 & 70 & 1 & 0 & 0 & 0\\ 88 & 128 & 50 & 0 & 1 & 0 & 0\\ 119 & 81 & 34 & 0 & 0 & 1 & 0\\ 32 & 121 & 152 & 0 & 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 112 & 79 & 48 & 135\\ 0 & 1 & 0 & 56 & 39 & 86 & 46\\ 0 & 0 & 1 & 97 & 117 & 133 & 15\end{pmatrix}$

Tabela E.2 – *Matrizes* G e H de alguns Códigos $FS_{4P}(n,k,d)$ *para* $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$

n	p	ζ	λ	*Código*	G	H
8	127	21+j103	1	$FS_{4P}(8,4,4)$	$\begin{pmatrix} 7 & 88 & 17 & 104 & 1 & 0 & 0 & 0 \\ 45 & 26 & 10 & 110 & 0 & 1 & 0 & 0 \\ 36 & 7 & 101 & 88 & 0 & 0 & 1 & 0 \\ 30 & 91 & 45 & 120 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 120 & 82 & 91 & 97 \\ 0 & 1 & 0 & 0 & 39 & 101 & 120 & 36 \\ 0 & 0 & 1 & 0 & 110 & 117 & 26 & 82 \\ 0 & 0 & 0 & 1 & 23 & 17 & 39 & 7 \end{pmatrix}$
			-1	$FS_{4P}(8,4,4)$	$\begin{pmatrix} 41 & 120 & 26 & 16 & 1 & 0 & 0 & 0 \\ 29 & 31 & 24 & 101 & 0 & 1 & 0 & 0 \\ 42 & 47 & 96 & 120 & 0 & 0 & 1 & 0 \\ 87 & 85 & 29 & 86 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 86 & 98 & 85 & 40 \\ 0 & 1 & 0 & 0 & 7 & 96 & 80 & 42 \\ 0 & 0 & 1 & 0 & 101 & 103 & 31 & 98 \\ 0 & 0 & 0 & 1 & 111 & 26 & 7 & 41 \end{pmatrix}$
9	71	8+j24	1	$FS_{4P}(9,5,3)$	$\begin{pmatrix} 58 & 23 & 36 & 43 & 1 & 0 & 0 & 0 & 0 \\ 56 & 23 & 51 & 29 & 0 & 1 & 0 & 0 & 0 \\ 40 & 12 & 27 & 24 & 0 & 0 & 1 & 0 & 0 \\ 58 & 22 & 36 & 43 & 0 & 0 & 0 & 1 & 0 \\ 24 & 62 & 9 & 7 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 13 & 15 & 31 & 13 & 47 \\ 0 & 1 & 0 & 0 & 48 & 48 & 59 & 49 & 9 \\ 0 & 0 & 1 & 0 & 35 & 20 & 44 & 35 & 62 \\ 0 & 0 & 0 & 1 & 28 & 42 & 47 & 28 & 64 \end{pmatrix}$
			-1	$FS_{4P}(9,4,5)$	$\begin{pmatrix} 7 & 28 & 24 & 42 & 43 & 1 & 0 & 0 & 0 \\ 62 & 36 & 44 & 51 & 35 & 0 & 1 & 0 & 0 \\ 62 & 49 & 12 & 48 & 23 & 0 & 0 & 1 & 0 \\ 47 & 58 & 31 & 56 & 13 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 64 & 9 & 9 & 24 \\ 0 & 1 & 0 & 0 & 0 & 43 & 35 & 22 & 13 \\ 0 & 0 & 1 & 0 & 0 & 47 & 27 & 59 & 40 \\ 0 & 0 & 0 & 1 & 0 & 29 & 20 & 23 & 15 \\ 0 & 0 & 0 & 0 & 1 & 28 & 36 & 48 & 58 \end{pmatrix}$
10	79	18+j25	1	$FS_{4P}(10,5,5)$	$\begin{pmatrix} 55 & 56 & 13 & 72 & 17 & 1 & 0 & 0 & 0 & 0 \\ 16 & 0 & 17 & 68 & 7 & 0 & 1 & 0 & 0 & 0 \\ 1 & 59 & 26 & 62 & 13 & 0 & 0 & 1 & 0 & 0 \\ 15 & 36 & 20 & 0 & 23 & 0 & 0 & 0 & 1 & 0 \\ 43 & 64 & 1 & 63 & 55 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 24 & 63 & 78 & 64 & 36 \\ 0 & 1 & 0 & 0 & 0 & 23 & 0 & 20 & 43 & 15 \\ 0 & 0 & 1 & 0 & 0 & 66 & 62 & 53 & 59 & 78 \\ 0 & 0 & 0 & 1 & 0 & 7 & 11 & 17 & 0 & 16 \\ 0 & 0 & 0 & 0 & 1 & 62 & 72 & 66 & 56 & 24 \end{pmatrix}$
			-1	$FS_{4P}(10,5,5)$	$\begin{pmatrix} 12 & 12 & 47 & 0 & 39 & 1 & 0 & 0 & 0 & 0 \\ 5 & 40 & 23 & 7 & 0 & 0 & 1 & 0 & 0 & 0 \\ 72 & 12 & 56 & 56 & 47 & 0 & 0 & 1 & 0 & 0 \\ 6 & 14 & 67 & 40 & 67 & 0 & 0 & 0 & 1 & 0 \\ 58 & 73 & 72 & 74 & 12 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 67 & 74 & 7 & 73 & 21 \\ 0 & 1 & 0 & 0 & 0 & 67 & 39 & 67 & 65 & 6 \\ 0 & 0 & 1 & 0 & 0 & 32 & 56 & 23 & 12 & 7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 72 & 23 & 39 & 5 \\ 0 & 0 & 0 & 0 & 1 & 40 & 0 & 32 & 12 & 67 \end{pmatrix}$

REFERÊNCIAS

[1] J. M. Pollard, The Fast Fourier Transform in a Finite Field, *Mathematics of Computation*, v. 25, n. 114, p. 365-374, April, 1971.

[2] M. M. Campello de Souza, H. M. de Oliveira, R. M. Campello de Souza and M. M. Vasconcelos, The Discrete Cosine Transform over Prime Finite Fields, In: **Proceedings of the 11th International Conference on Telecommunications**, ser. Lecture Notes in Computer Science, J. N. de Souza, P. Dini, and P. Lorentz, Eds. Berlin: Springer, 2004, p. 482-487.

[3] R. M. Campello de Souza, H. M. de Oliveira, M. M. Campello de Souza e M. M. Vasconcelos, A Transformada Discreta do Seno em um Corpo Finito, In: **Anais do XXVIII Congresso Nacional de Matemática Aplicada e Computacional**, São Paulo, Brasil, 2005.

[4] J. B. Lima, *Trigonometria sobre Corpos Finitos: Novas Definições e Cenários de Aplicação*. Recife, 2008. Tese (Doutorado em Engenharia Elétrica) – Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco.

[5] J. B. Lima and R. M. Campello de Souza, New Trigonometric Transforms over Prime Finite Fields for Image Filtering, In: **Proceedings of the International Telecommunications Symposium**, Fortaleza, Brasil, 2006.

[6] J. B. Lima and R. M. Campello de Souza, Uma Marca D'água Digital Baseada na Transformada do Cosseno sobre Corpos Finitos, In: **Anais do XXII Simpósio Brasileiro de Telecomunicações**, Campinas, Brasil, 2005.

[7] J. B. Lima, R. M. Campello de Souza and D. Panario, Blind Sequence Separation Based on the Eigenstructure of Finite Field Transforms, In: **Anais do XXVI Simpósio Brasileiro de Telecomunicações**, Rio de Janeiro, Brasil, 2008.

[8] R. E. Blahut, Transform Techniques for Error-Control Codes, *IBM J. Res. Dev.*, v. 23, p.299-315, 1979.

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

[10] R. G. F. Távora, *Algoritmos Rápidos para Transformadas em Corpos Finitos*. Recife, 2001. Dissertação (Mestrado em Engenharia Elétrica) – Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco.

[11] J. W. Cooley and J. W. Tukey, An Algorithm for the Machine Calculation of Complex Fourier Series, *Math Comp.* 19, p. 297-301, 1965.

[12] T. I. Good, The Interaction Algorithm and Practical Fourier Analysis, *J. Roy. Statis. Soc.*, series B20, p. 361-375, 1958; addendum series 22, p. 372-375, 1960.

[13] G. Goertzel, An Algorithm for the Evaluation of Finite Trigonometric Series, *The American Mathematical Monthly*, v. 65, n. 1, p.34-35, 1958.

[14] R. M. Campello de Souza, E. S. V. Freire and H. M. de Oliveira, Fourier Codes, In: **Proceedings of the Tenth International Symposium on Communication Theory and Applications, ISCTA'09**, Ambleside, Lake District, UK, 2009, p. 370-375.

[15] D. M. Burton, *Elementary Number Theory*, 7th edition, McGraw Hill, 2005.

[16] R. E. Blahut, *Theory and Practice of Error Control codes*, Addison-Wesley, 1985.

[17] D. F. Elliott and K. R. Rao, *Fast Transforms - Algorithms Analyses Applications*, Academic Press, 1982.

[18] H. Alaedine, E. H. Baghious, G. Madre and G. Burel, Realization of Block Robust Adaptive Filters Using Generalized Sliding Fermat Number Transform, In: **Proceedings of the 14th European Signal Processing Conference**, EUSIPCO'2006, Florence, Italy, 2006.

[19] T. Toivonen and J. Heikkilä, Video Filtering with Fermat Number Theoretic Transforms Using Residue Number System, *IEEE Transactions on Circuits and Systems for Video Technology*, v. 16, n. 1, January, 2006.

[20] S. Gudvangen and H. Buskerud, Practical Applications of Number Theoretic Transforms, In: **Proceedings of the Norwegian Signal Processing Symposium**, NORSIG'99, Asker, Norway, 1999.

[21] H. Tamori, N. Aoki and T. Yamamoto, A Fragile Digital Watermarking Technique by Number Theoretic Transform, *IEICE Trans. Fundamentals*, v. E85-A, n. 8, p. 1902-1904, August, 2002.

[22] D. T. Birtwistle, The Eigenstructure of the Number Theoretic Transforms, *Signal Processing 4*, p. 287-294, 1982.

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

[24] R. M. Campello de Souza, H. M. de Oliveira, Eigensequences for Multiuser Communication over the Real Adder Channel, In: **Proceedings of the VI International Telecommunications Symposium**, Fortaleza, Brasil, 2006, p. 711-716.

[25] D. F. Elliott and K. R. Rao, *Fast Transforms – Algorithms, Analyses, Applications*, Academic Press, 1982.

[26] L. H. Thomas, Using a Computer to Solve Problems in Physics, In: **Applications of Digital Computers**, Ginn and Co., Boston, MA, 1963.

[27] W. Pennebaker and B. Mitchell, *JPEG Still Image Data Compression Standard*, New York: Van Nostrand Heinhold, 1993.

[28] T. Sikora, MPEG Digital Video-Coding Standards, *IEEE Signal Processing Magazine*, v.14, n.5, p. 82-100, September, 1997.

[29] M. A. Suhail and M. S. Obaidat, Digital Watermarking-based DCT and JPEG Model, *IEEE Trans. on Instrumentation and Measurement*, v. 52, n. 5, p. 1640-1647, October, 2003.

[30] S. A. Martucci, Symmetric Convolution and the Discrete Sine and Cosine Transforms, *IEEE Trans. on Signal Processing*, v. 42, n. 5, p. 1038-1051, May, 1994.

[31] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, Trigonometry in Finite Fields and a New Hartley Transform, In: **Proceedings of the 1998 IEEE International Symposium on Information Theory**, Boston, MA, 1998, p.293.

[32] A. N. Kauffman, *A Transformada de Hartley em um Corpo Finito e Aplicações*. Recife, 1999. Dissertação (Mestrado em Engenharia Elétrica) - DES, Universidade Federal de Pernambuco.

[33] R. M. Campello de Souza, H. M. de Oliveira and D. Silva, The Z Transform over Finite Fields, In: **Proceedings of the International Telecommunications Symposium**, Natal, Brasil, 2002.

[34] H. S. Stone, *Discrete Mathematical Structures*, Science Research Associates, 1973.

[35] C. C. Tseng, Eigenvalues and Eigenvectors of Generalized DFT, Generalized DHT and DST-IV Matrices, *IEEE Trans. on Signal Processing*, v. 50, n. 4, p. 866-877, April, 2002.

[36] G. J. da Silva Jr., R. M. Campello de Souza and H. M. de Oliveira, New Algorithms for Computing a Single Component of the Discrete Fourier Transform, In: **Proceedings of the Tenth International Symposium on Communication Theory and Applications, ISCTA '09**, Ambleside, Lake District, UK, 2009, p. 151-154.

[37] Adler, Andrew and Coury, John E., *The Theory of Numbers: A Text and Source Book of Problems*, Chapter 5, 1995, p. 125-137.

[38] R. M. Campello de Souza, H. M. de Oliveira and M. M. Campello de Souza, Hartley Number Theoretic Transforms, In: **Proceedings of the 2001 IEEE International Symposium on Information Theory**, Washington, D.C., USA, 2001, p. 210.

TRABALHOS PUBLICADOS

R. M. Campello de Souza, E. S. V. Freire and H. M. de Oliveira, Fourier Codes, In: **Proceedings of the Tenth International Symposium on Communication Theory and Applications, ISCTA'09**, Ambleside, Lake District, UK, 2009, p. 370-375.

E. S. V. Freire, R. M. Campello de Souza and J. B. Lima, Códigos Corretores de Erros Baseados na Transformada do Cosseno de Corpo Finito, In: **Anais do XXVII Simpósio Brasileiro de Telecomunicações, SBrT 2009**, Blumenau, SC, Brasil, 2009.