Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Trabalho de Graduação em Engenharia Elétrica

Caio Marcelo Fernandes Barros

Nova Abordagem de Códigos de Bloco Baseados em Autosequências

Orientador : Hélio Magalhães de Oliveira, Docteur

Recife, Junho de 2009.

Agradecimentos

Agradeço, de todo o meu coração, a DEUS pela sua imensa ajuda em todos os momentos difíceis desta caminhada. Aos meus PAIS, Dulcilene e Marcelo, pela dedicação de ambos no decorrer de toda a minha vida, compreensão e apoio em todas as minhas decisões.

A todos vocês os meus mais emocionados agradecimentos

Caio Marcelo Fernandes Barros

Resumo

Um espectador ao observar a evolução dos meios de comunicação, notará um veloz aumento da demanda por sistemas de comunicação, e também memórias, mais eficientes e seguras. Com o advento das conexões de dados em alta velocidade, agora mais do que antes, esses sistemas de comunicação necessitam de artifícios que colaborem para o seu bom funcionamento.

Uma alternativa para esse problema é a codificação de canal, introduzida por *C.E.Shannon* [1]. Ele mostra que uma codificação adequada pode reduzir os erros induzidos por uma fonte de ruído a um nível desejado. As aplicações destas técnicas permeiam todos as esferas sociais que necessitem de um meio de comunicação, das militares às civis.

Motivados por esta crescente demanda, exponho neste trabalho uma nova abordagem de códigos de bloco utilizando o conceito de auto-seqüências.

Sumário

Lista de Figuras

Lista de Tabelas

capítulo 1

Introdução

Ao longo desses últimos anos, verifica-se, em amplas áreas das Telecomunicações, que as Transformadas Discretas vêm proporcionando avanços tecnológicos notáveis em Criptografia[2], Processamento Digital de Sinal[3] e Processamento Digital de Imagem[4].

O crescimento da população, e consequente aumento da demanda, proporcionaram vultosos investimentos nos serviços da telefonia por parte das empresas, que necessitavam atender a essa forte demanda. Nesse cenário, algumas técnicas de aproveitamento de canais físicos de comunicação surgiram, as mais conhecidas são ***FDM***-*Frequency Division Multiplexing* e ***TDM***-*Time Division Multiplexing*.

Nesse contexto, de Oliveira, Campello de Souza e colaboradores, apresentaram uma contribuição eficiente[5], chamada de ***GDM***-*Galois Division Multiplexing*, uma outra alternativa a ser utilizada é a decomposição em wavelets[6].

Seguindo este raciocínio de intensa modificação tecnológica, uma ferramenta permeia todos os campos citados, as Transformadas Discretas. Destacam-se as técnicas da ***DFT***-*Discrete Fourier Transform* e a ***DHT***-*Discrete Hartley Transform*[7][8]. Uma inovação na técnica citada acima foi introduzida por Pollard, a **DFT** de corpo finito[9] e foi usada em avaliações de convoluções discretas com base em aritmética inteira. Um meio de aplicação diferente desta ferramenta é a utilização do conceito das autosequências[10]. Um aprofundamento no conceito de auto-seqüências para uma aplicação em sistemas de comunicação multi-usuário em canal real aditivo é uma área que vem despertando uma atenção particular[11].

Impelido por todos os motivos apresentados e por outros textos científicos[12][13], constata-se que a alternativa apresentada se mostra promissora e satisfatória, haja vista que a complexidade computacional do cálculo da transformada discreta é baixa, tornando-se assim um dos focos de pesquisa do GPS na UFPE[11].

Por fim, as expectativas estão na esperança de que unindo toda a teoria de codificação de canal conhecida, aliada à baixa complexidade computacional do cálculo das transformadas discretas, uma nova ferramenta possa ser apresentada para auxiliar a velocidade de tráfego de dados nas redes de comunicação.

capítulo 2

Histórico

Por volta de 1948, o mundo foi apresentado à primeira formulação matemática completa sobre a teoria de informação[1]. Nesse artigo histórico[1] mostra-se que não importando quão graves são os erros provocados em um meio de transmissão, ou memória, uma codificação de canal eficiente pode baixar os efeitos daqueles, os erros induzidos, a qualquer nível desejado, sem depreciação da taxa de transferência ou armazenamento.

A partir daí, grandes esforços vêm sendo empreendidos para se conseguir uma codificação/decodificação eficiente para um canal de comunicação com ruído bastante atuante. A utilização de códigos para controle e correção de erros se tornou, ao longo do tempo, parte indispensável dos atuais sistemas de comunicação. Essa ferramenta colaborou para a consolidação eficiente e confiável das redes de tráfego de alta velocidade.

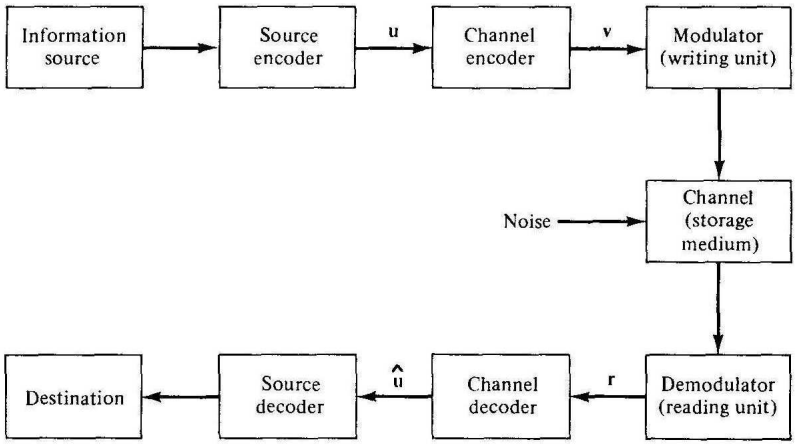

Figura 2.1: Esquema de um sistema de transmissão típico.

O esquema da figura 2.1 mostra um típico canal de comunicação.

A *fonte de informação* pode ser uma pessoa ou uma máquina, ou seja, é toda fonte *emissora* de informação, computador digital por exemplo. A informação de saída pode ser tanto uma onda senoidal ou uma sequência de símbolos discretos.

O *codificador de fonte* tem a função de transformar a informação de saída da *fonte de informação* em uma sequência binária **u** conhecida como *sequência de informação*.

O *codificador de canal* transforma a sequência **u** em uma sequência **v** que pode ou não ser binária. Esta palavra **v** é conhecida como *palavra-código*.

O *modulador* ou *unidade de escrita* é a unidade responsável por transformar a seqüência de dados *v (palavra-código)* em uma onda de duração **T**, pois é conhecido que uma seqüências discretas não são próprias para serem usadas no envio de informação em um meio ruidoso.

O *demodulador* faz o processo inverso ao *modulador*, transforma uma onda de duração **T** em uma sequência de dados conhecida como *r (palavra recebida)*.

O *decodificador de canal*, transforma a palavra recebida r e uma sequência binária $\hat{u}$ *(informação estimada)*. Teoricamente mesmo havendo erros no canal de comunicação, na idealidade, a sequência $\hat{u}$ é uma cópia da informação u.

E por fim o *decodificador de fonte* irá transformar a informação $\hat{u}$ em uma estimativa de informação enviada pela *fonte de informação*.

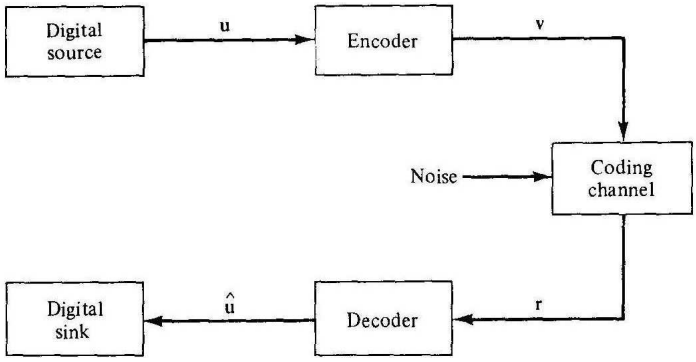

Figura 2.2: Esquema simplificado de um sistema de codificação.

Como o escopo principal deste trabalho versa sobre a codificação de canal é mostrado na figura 2.2 um esquema simplificado de codificação. Neste esquema agrupamos a *fonte de informação* e o *codificador de fonte* em um único bloco nomeado de *fonte digital*. O *codificador de canal* e o *modulador* foram incluídos no bloco *codificador*. O *demodulador* e o *decodificador de canal* foram incluídos no bloco *decodificador*. E por fim os blocos de *decodificador de fonte* e *destinatário* forma substituídos pelo bloco *Digital sink*.

Assim, sempre que nos referirmos a esquemas de codificação/decodificação teremos em mente os esquema da figura 2.2.

capítulo 3

Breve Revisão sobre Fundamentos da Estrutura de Corpos Finitos

Um grupo é uma estrutura algébrica Φ contendo em si elementos e operações que obedecem aos seguintes axiomas:

- Associatividade
- Elemento Identidade
- Elemento Inverso
- Fechamento

Para um grupo tornar-se um corpo finito, existe mais um axioma a ser considerado, a comutatividade, e existem duas operações a serem consideradas, aditiva e multiplicativa (+ e *), todas sobre aritmética modular, que podem ou não ser iguais as usuais. Assim esta estrutura pode formar um corpo de polinômios sobre as operações e axiomas acima citados sendo usada para fins como multiplexação, por meio das transformadas de corpo finito.

Definição 3.1. *Um polinômio p(x) de grau m é dito irredutível sobre um determinado corpo quando ele não é divisível por nenhum outro polinômio de grau inferior a m ou superior a 0, ou seja, quando ele não tem fatores com coeficientes pertencentes ao corpo.*

Definição 3.2. *Chama-se campo de Galois e representa-se por GF(q^m) um corpo com q^m elementos, q uma potência de primo p ($q = p^s$).*

É de interesse definir uma aritmética utilizando os q^m elementos do corpo. Para isso deve-se partir de um polinômio primitivo que é o único capaz de gerar os q^m elementos distintos pertencentes ao corpo.

Definição 3.3. *Define-se como polinômio primitivo, um polinômio p(x) irredutível de grau m tal que p(ζ) = 0, em que ζ é um elemento cujas potências são capazes de gerar todos os elementos diferentes de zero de GF(q^m). ζ é dito ser, então, um elemento primitivo do corpo. Se um polinômio p(x) é dito primitivo, então seu polinômio recíproco p'(x) também é primitivo, em que p'(x) = x^m * p (1/x).*

Depois de apresentar os conceitos e características que envolvem a teoria dos corpos finitos, vamos agora introduzir algumas propriedades abstratas estruturais dos corpos finitos. Com esta finalidade, alguns teoremas serão enunciados (sem apresentar as demonstrações), considerando a existência de um corpo finito com q elementos.

Teorema 3.1. *O número de elementos q de um corpo finito corresponde a uma potência p^m, em que p é um número primo. Ou seja, $q = p^m$, com p primo. Para o caso dos campos de Galois associados à estrutura binária, tem-se p=2, assim, q=2^m.*

Definição 3.4. *Chama-se ordem de θ, e indica-se por ord(θ), o menor inteiro $t \geq 1$ em que θ^t =1. Em linhas gerais, pode-se dizer que θ é o elemento gerador de um grupo com t elementos ou um corpo com t+1 elementos. Dessa forma, este corpo possui como elementos 0, 1, θ, θ^2 , θ^3 ,..., θ^{t-1} .*

Teorema 3.2. *Se um elemento θ de um corpo possui ordem t ($t > 1$), implica que q-1 é divisível por t, em que q é o número de elementos do corpo.*

capítulo 4

Atividades Realizadas

Todas as simulações realizadas neste trabalho utilizaram a plataforma *Matlab*®. A grande parte dos assuntos abordados neste trabalho foram ministrados em aulas presencias do curso de engenharia eletrônica com ênfase em telecomunicações:

- Álgebra Linear
- Sistemas Discretos
- Processamento Digital de Sinais
- Códigos Corretores de Erro

Outros assuntos requeridos neste trabalho, os quais não podiam ser obtidos em aulas presencias, foram abordados com o Profº orientador (Hélio Magalhães de Oliveira) e com alunos do lab. de Criptografia(Juliano Bandeira (Orientador: Profº Ricardo Campello), Eduarda Simões (Orientador: Profº Ricardo Campello)).

As especificações dos computadores digitais utilizados são:

- Processador: *Intel*® *Celeron*®
- Sistema Operacional: *WindowsXP*®
- Memória : 1Gb
- HD : 120GB
- Clock : 1.87GHz

Neste trabalho foi necessário implementar rotinas de *Matlab*® para a criação de corpos de extensão (GF(q^m)). Foram de extrema importância as realizações de rotinas para geração das matrizes *Geratriz* e *Paridade* dos códigos considerados e consequêntemente de rotinas de cálculo de distância mínima. Mais informações e detalhes serão abordados oportunamente no capítulo 5.

capítulo 5

Resultados

Considere a matriz da DFT, $[W]_N \triangleq \left(exp(\frac{2\pi}{N} kn) \right)$, em que k,n=0,1,2,...,N-1. Sabemos pois que se um sinal x[n] é uma autosequência da DFT, então o seu espectro será dado por:

$$[W]_N x[n] = \lambda x[n]; \lambda = \pm\sqrt{N}, \pm j\sqrt{N}. \tag{5.1}$$

Nesta configuração 4 autovalores são possíveis[11][14], considerando um bloco de comprimento N, como mostrado acima. Cada um dos autovalores está associado a um subespaço vetorial,estes são mutuamente exclusivos, que juntos varrem todo o espaço vetorial de autosequências. Denotaremos esses espaços vetoriais por $V_N^+, V_N^-, V_N^{+j}, V_N^{-j}$,respectivamente. Como iremos trabalhar com códigos convencionais sobre os reais, conhecidos como *reticulados*[15][16], só há interesse nos autovalores reais, $\pm\sqrt{N}$. Assim a equação 5.1 será modificada por:

$$[W]_N x[n] = \pm\sqrt{N}. \tag{5.2}$$

A partir da equação 5.2, aplicando algumas modificações algébricas resultamos na equação abaixo:

$$x[n]([W]_N \mp \sqrt{N} I_N)^T = 0. \tag{5.3}$$

Da teoria convencional de códigos sabe-se que a matriz de paridade H é o espaço nulo das palavras-código gerados a partir da matriz geradora G. Assim definimos a matriz de paridade do código como segue abaixo:

$$H^T \triangleq [W]_N \mp \sqrt{N} I_N. \tag{5.4}$$

Lembrando que o sinal da equação acima depende do autovalor da equação 5.2. Para por a matriz de paridade na forma convencional e retirar as linhas que sejam linearmente independentes aplicamos a forma escalonada padrão. Aplicando o procedimento anterior obtemos os parâmetros N e $K^{+,-}$ (comprimento e dimensão do código, este último depende do sinal do autovalor). Assim $N - K^{+,-} = rank([W]_N \mp \sqrt{N} I_N)$, resultando nas equações abaixo:

$$H^T \triangleq [I_{N-K} \vdots P_\lambda] \leftrightarrows G \triangleq [-P_\lambda^T \vdots I_K]. \tag{5.5}$$

A partir da equação 5.5, há a possibilidade de obter dois códigos, $[N, K^+]$ e $[N, K^-]$, um utilizando o autovalor positivo e outro utilizando o autovalor negativo, respectivamente. Podemos obter a dimensão do código através de manipulações algébricas temos:

$$K^{sgn(\lambda)} = N - rank([W]_N - \lambda I_N), \lambda = \pm\sqrt{N}. \tag{5.6}$$

Para exemplificação mostra-se abaixo o caso para a transformada discreta de Fourier de comprimento 4:

$$[W]_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & j \end{pmatrix}. \tag{5.7}$$

Os possíveis autovalores são $\lambda = \pm\sqrt{N}$, considerando o caso de sinal positivo para o autovalor, temos $\lambda = 2$, assim a exemplificação prossegui:

$$([W]_4 - 2I_4) = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & (-2+j) & -1 & j \\ 1 & -1 & -1 & -1 \\ 1 & j & -1 & (-2+j) \end{pmatrix}. \tag{5.8}$$

Pela equação 5.6 podemos ver que a dimensão dos espaço vetorial V_4^+ é dois (K^+=2), assim a forma escalonada padrão da equação 5.8 será:

$$H^T = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 0 & -1 \end{pmatrix} \tag{5.9}$$

A partir da equação da matriz de paridade acima podemos obter a matriz geradora do código F:[4,2], a letra 'F' indica que foi obtida a partir da matriz de transformação de Fourier:

$$G^+ = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \mid F[4,2] \; ; \; G^- = \begin{pmatrix} -1 & 1 & 1 & 1 \end{pmatrix} \mid F[4,1] \tag{5.10}$$

Para o caso da transformada discreta de Hartley, só há possibilidade de dois autovalores ($\lambda = \pm\sqrt{N}$), não havendo os autovalores complexos. Desta forma, todo o raciocínio que foi apresentado até o presente momento pode ser repetido para a transformada discreta de Hartley. Assim a matriz geradora do código para a transformada discreta de Hartley é:

$$G^+ = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \mid H[4,3] \; ; \; G^- = \begin{pmatrix} -1 & 1 & 1 & 1 \end{pmatrix} \mid H[4,1] \tag{5.11}$$

Considerando as matrizes geradoras apresentadas acima, casualmente vemos que elas representam os reticulados *D3* e *A1*, os melhores reticulados de dimensão 3 e 1[15][17]. Segue abaixo uma tabela

que apresenta os parâmetros dos códigos oriundos da transformada de Fourier, foram testados, para fins de resultado e análise, as transformadas de comprimento até 24.

Nas tabelas 5.1 e 5.3 os termos $'\Delta'$ *e* $'\mu'$ significam, respectivamente, a densidade e a distância mínima dos reticulados considerados.

Tabela 5.1: Códigos de Fourier no espaço euclideano N-dimensional

N	K^+	μ^+	Δ^+	K^-	μ^-	Δ^-
3	1	9.4641	1	1	2.5359	1
4	2	2	0.55536	4	1	1
5	2	4	0.82582	1	5.5279	1
6	2	3.5505	0.56921	2	3.5505	0.56921
7	2	2.8931	0.37722	2	2.4577	0.44763
8	3	3	0.26029	2	2.3431	0.42505
9	3	2.7852	0.26073	2	2.5014	0.43446
10	3	2.7906	0.25213	3	6.8377	0.40055
11	3	2.9203	0.2483	3	5.4021	0.42541
12	4	4	0.11577	3	4.906	0.44661
13	4	3.4628	0.12822	3	4.2503	0.39718
14	4	3.5376	0.15731	3	3.8717	0.30403
15	4	3.4413	0.15837	4	7.418	0.21238
16	4	4.2625	0.1412	3	3.2543	0.27218
17	5	5.3824	0.089659	4	2.9451	0.063149
18	5	4.8172	0.096808	4	3.0745	0.069407
19	5	4.7151	0.11403	4	3.304	0.088451
20	5	5.0325	0.13599	4	4.1055	0.15164
21	5	4.9701	0.10052	4	3.6455	0.14034
22	6	7.2991	0.071307	5	8.387	0.10898
23	6	5.0715	0.034921	5	8.6131	0.15042
24	6	4.0909	0.021066	5	5.777	0.1134

Nas tabelas 5.2, 5.4, 5.5, 5.6 os termos $'\delta'$ *e* $'det\Lambda'$ significam, respectivamente, a densidade de centro e o determinante da matriz de graminiano dos reticulados considerados.

Como foi mencionado, os códigos de Hartley podem ser obtidos da mesma maneira que os códigos de Fourier, assim segue:

Considere a matriz de transformação discreta de Hartley $[H]_N \triangleq \left(cas(\frac{2\pi}{N}kn) \right)$ n,k=0,1,2,...,N-1, em que o núcleo da transformada discreta de Hartley é a função $\text{cas}(x) \triangleq \cos(x) + \sin(x)$. A partir de um autovalor da transformada discreta de Hartley chega-se a expressão : $[H]_N x[n] = \lambda x[n]$; $\lambda = \pm\sqrt{N}$, após algumas manipulações algébricas : $x[n]([H]_N \mp \sqrt{N} I_N)^T = 0$. Por fim : $N - K^{+,-} = rank([H]_N \mp \sqrt{N} I_N)$.

Através de análises de simulações do código gerado a partir da transformada discreta de Hartley,

Tabela 5.2: Códigos de Fourier no espaço euclideano N-dimensional (Outros Parâmetros)

N	K^+	δ^+	$det\Lambda^+$	K^-	δ^-	$det\Lambda^-$
3	1	0.5	3.0764	1	0.5	1
4	2	0.17678	2.8284	4	0.5	1
5	2	0.26287	3.8042	1	0.5	1
6	2	0.18119	4.899	2	0.18119	0.56921
7	2	0.12007	6.0237	2	0.14249	0.44763
8	3	0.06214	10.453	2	0.1353	0.42505
9	3	0.062245	9.3343	2	0.13829	0.43446
10	3	0.060192	9.6812	3	0.095625	0.40055
11	3	0.059278	10.524	3	0.10156	15.454
12	4	0.023459	42.628	3	0.10662	12.74
13	4	0.025982	28.844	3	0.094819	11.552
14	4	0.031878	24.536	3	0.072582	13.12
15	4	0.032093	23.062	4	0.043038	79.91
16	4	0.028614	39.685	3	0.064979	11.294
17	5	0.017033	123.31	4	0.012797	42.364
18	5	0.018391	86.543	4	0.014065	42.005
19	5	0.021663	69.642	4	0.017924	38.066
20	5	0.025835	68.723	4	0.030728	34.283
21	5	0.019096	90.122	4	0.028438	29.207
22	6	0.013799	440.35	5	0.020704	307.47
23	6	0.0067576	301.61	5	0.028577	238.09
24	6	0.0040764	262.42	5	0.021544	116.35

a dimensão do código gerado pode ser expressa por:

$$K^{+} = \left\lceil \frac{N}{2} \right\rceil + \delta_{Nmod4,0} \; ; \; K^{-} = \left\lfloor \frac{N}{2} \right\rfloor - \delta_{Nmod4,0} \tag{5.12}$$

Em que $\delta_{k,l}$ representa o símbolo de *Kronecker*. Vale mencionar que a complexidade computacional requerida para calcular os parâmetros do código gerado a partir da transformada discreta de Hartley é maior que complexidade computacional requerida para calcular os parâmetros do código gerado a partir da transformada discreta de Fourier.

Para uma notação mais apurada , denotaremos as matriz geradora e de paridade do código gerado a partir das transformadas discretas de Fourier e Hartley de comprimento N, associado ao autovalor λ por ${}_{s}G_{N}^{sgn(\lambda)}$ e ${}_{s}H_{N}^{sgn(\lambda)}$, em que s denota a transformada discreta usada, $s \in \{F, H\}$ e $sgn(\lambda) \in \{+, -\}$. As tabelas 5.3 e 5.4estão apresentados os parâmetros para o código gerado a partir da DHT.

Tabela 5.3: Códigos de Hartley no espaço euclidiano N-dimensional

N	K^{+}	μ^{+}	Δ^{+}	K^{-}	μ^{-}	Δ^{-}
3	2	2	0.7221	1	2.5359	1
4	3	2	0.74048	1	4	1
5	3	4	0.42552	2	1.5814	0.4614
6	3	4.9148	0.21497	3	1.3924	0.24623
7	4	3.3937	0.19977	3	1.5515	0.22407
8	5	2	0.062949	3	2.3431	0.30672
9	5	3	0.054289	4	1.7306	0.12155
10	5	5.2063	0.075916	5	1.8957	0.077169
11	6	3.7751	0.052394	5	2.6115	0.14192
12	7	2.5744	0.014886	5	2.2205	0.066449
13	7	3.0709	0.0099451	6	1.8702	0.024582
14	6	2	0.010263	7	2.2839	0.02135
15	8	4.1987	0.015084	7	2.1276	0.014352
16	9	2.7463	0.0022665	7	2.2606	0.012029
17	9	3.3358	0.0021189	8	1.9687	0.00391907
18	9	4.7288	0.0033659	9	2.5477	0.0047677
23	12	-	-	11	-	-

Após uma análise mais apurada da técnica apresentada, vê-se que esta é universal, desde que a transformada discreta considerada tenha autovalores e consequentemente autovetores. Assim considerando a transformada discreta do cosseno tipo 1 com simetria par[3] como se segue, autovalores possíveis ± 1:

$$\left[C_{t1,par}\right]_{N} \triangleq 2\left(\alpha[n]\cos\left(\frac{\pi * k * n}{N-1}\right)\right) \; ; \; 0 \leq k, n \leq N-1. \tag{5.13}$$

Em que a função $\alpha[n]$ é definida como segue: $\alpha[n] \triangleq \begin{cases} \frac{1}{2}, & n = 0, N-1 \\ 1, & 1 \leq n \leq N-2 \end{cases}$

Tabela 5.4: Códigos de Hartley no espaço euclideano N-dimensional (Outros Parâmetros)

N	K^+	δ^+	$det\Lambda^+$	K^-	δ^-	$det\Lambda^-$
3	2	0.22985	2.1753	1	0.5	1.5925
4	3	0.17678	2	1	0.5	2
5	3	0.10159	9.8438	2	0.14687	2.6919
6	3	0.051319	26.54	3	0.058782	3.494
7	4	0.040483	17.781	3	0.053494	4.5157
8	5	0.011959	14.782	3	0.073223	6.1229
9	5	0.010314	47.233	4	0.024631	7.5998
10	5	0.014422	134.01	5	0.01466	10.547
11	6	0.010139	82.915	5	0.026962	12.774
12	7	0.0031505	67.882	5	0.012624	18.189
13	7	0.0021049	188.36	6	0.0047569	21.488
14	6	0.001986	62.94	7	0.0045188	31.127
15	8	0.003716	326.64	7	0.030375	36.13
16	9	0.00068728	267.95	7	0.0025442	53.298
17	9	0.00064239	687.59	8	0.00006449	60.769
18	9	0.00000161	2081.2	9	0.00005246	90.866
23	12	-	-	11	-	-

Na tabela 5.5, mostra-se os parâmetros para a transformada do cosseno tipo1 par.

Pode-se aplicar a mesma técnica de geração de códigos de bloco sobre os reais para a transformada discreta do cosseno tipo 2 par[3], obtendo-se os parâmetros da tabela 5.6.

$$\left[C_{t2,par}\right]_N \triangleq 2\left(\cos\left(\frac{\pi * k * (2n+1}{N-1}\right)\right) \; ; \; 0 \leq k, n \leq N-1. \tag{5.14}$$

O deslocamento desta técnica para as transformadas de corpo finito foi inicialmente proposta em reuniões com o orientador, foi usada a transformada de fourier de corpo finito, como é conhecido, só foram usados os parâmetros que obtinham autovalor que não pertencia aos inteiros Gaussianos. A tabela 5.7 mostra os parâmetros obtidos na simulação.

Tabela 5.5: Códigos do Cosseno tipo1 par no espaço euclidiano N-dimensional

N	K^+	μ^+	Δ^+	K^-	μ^-	Δ^-
4	2	14,899	0,7294	2	1,5051	0,7294
5	3	2	0,21609	2	5,1716	0,46609
6	3	38,646	0,91417	3	1,3793	0,22139
7	4	2	0,031435	2	2	0,064615
8	3	7,9449	0,14624	4	2,0461	0,091736
9	5	4	0,015553	3	2	0,082357
10	4	20,486	0,68831	5	4,1715	0,073251
11	5	3,423	0,088435	4	2	0,046787
12	4	2	0,010245	5	2	0,063664
13	5	2	0,069374	4	2	0,010487
14	4	2	0,0010786	6	2,8455	0,0088372
15	6	7,4749	0,011159	4	2	0,0032571
16	5	2	0,00074003	6	2	0,0061624
17	7	2	4,06E-05	5	2	0,00017059
18	6	2	4,35E-05	7	6,2464	0,0043464
19	7	2	0,00026577	5	2	0,0022748
20	6	2	0,00039572	7	5,4193	0,0061939

Tabela 5.6: Códigos do Cosseno tipo2 par normalizado no espaço euclidiano N-dimensional

N	K^+	μ^+	$det\Lambda^+$	K^-	μ^-	$det\Lambda^-$
3	3	1	1	1	3,4091	1,8464
4	4	1	1	4	1	1
5	1	4,7564	2,1809	5	1	1
6	1	7,3638	2,7136	1	4,6817	2,1637
7	7	1	1	1	6,4375	2,5372
8	8	1	1	8	1	1
9	1	8,7579	2,9594	9	1	1
10	1	10,693	3,27	1	8,5142	2,9179
11	11	1	1	1	9,8689	3,1415
12	12	1	1	12	1	1
13	1	12,82	3,5805	13	1	1
14	1	14,274	3,778	1	12,428	3,5253
15	15	1	1	1	13,416	3,6628
16	16	1	1	16	1	1
17	1	16,901	4,1111	17	1	1
18	1	17,952	4,237	1	16,376	4,0468
19	19	1	1	1	17,028	4,1265
20	20	1	1	20	1	1

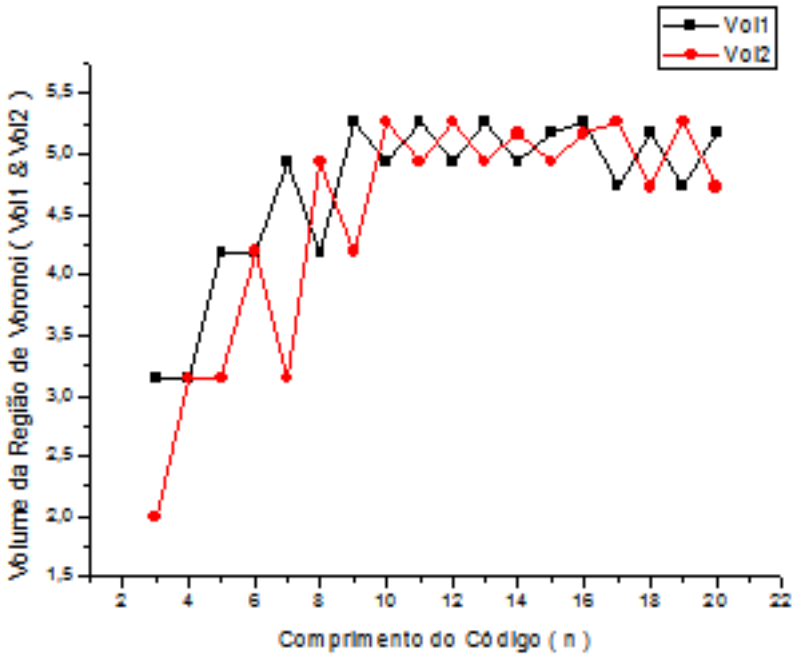

Figura 5.1: Gráfico do Vol. da região de Voronoi para a DCT tipo 1 normalizado

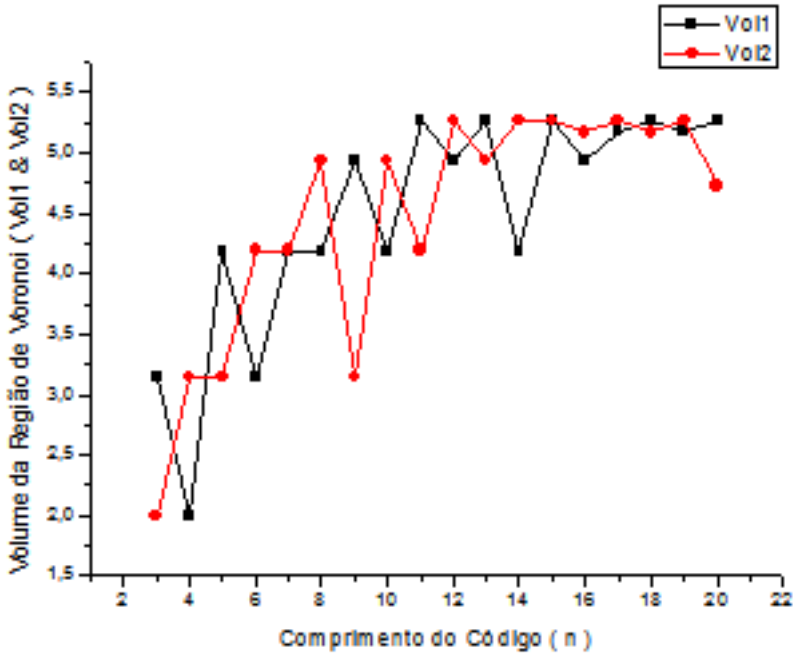

Figura 5.2: Gráfico do Vol. da região de Voronoi para a DCT tipo 4

Tabela 5.7: Parâmetros do código gerado a partir da Transformada de Fourier de Corpo Finito

p	α	η	K^+	K^-	μ^+	μ^-
7	6	2	1	1	2	2
11	3	5	1	2	5	3
	4	5	1	2	5	3
	5	5	2	1	3	5
	9	5	2	1	3	5
13	3	3	1	1	3	3
	5	4	1	2	4	2
	6	12	4	3	-	6
	7	12	3	4	6	-
	8	4	1	2	4	2
	9	3	1	1	3	3
	11	12	-	3	-	6
17	2	8	2	3	4	4
	3	16	4	5	-	-
	4	4	1	2	4	2
	5	16	4	5	-	-
	6	16	4	5	-	-
	7	16	4	5	-	-
	8	8	3	2	4	4
	9	9	2	3	4	4
	10	16	4	5	-	-
	11	16	4	5	-	-
	12	16	4	5	-	-
	13	4	1	2	4	2
	14	16	4	5	-	-
	15	8	3	2	4	4
	16	2	1	1	2	2

capítulo 6

Conclusão

Concluí-se que a técnica utilizada para geração de códigos, em que as palavras desse código são as autosequências da transformada discreta considerada, é consistente, promissora e universal, caso a transformada considerada apresente o par autosequência-autovalor. Essas autosequências são associadas a autovalores, esses por suas vez irão separar todo o espaço de autosequências utilizados em conjuntos disjuntos.

Quanto ao trabalho realizado pelo aluno, este foi de grande esclarecimento e motivação, impulsionando o aluno a ingressar na pós-graduação em engenharia eletrônica pela sua estrutura de pesquisa, foi requerido habilidade em programação em plataforma *Matlab*® e técnicas avançadas de processamento de sinais e teoria dos códigos.

Referências Bibliográficas

[1] Shannon,C.E., **A Mathematical Theory of Communication**, *Bell, Syst. Tech. J.* 27, pag.379-423(Part I),623-656(Part II), Julho 1948

[2] Shneier, B., **Applied Cryptography**, *John Wiley e Sons*, 1996

[3] Oppenheim,A. **Discrete-Time Signal Processing**, *Prentice Hall*, 1989

[4] Pitas, I. **Digital Image Processing Algorithms and Applications**, *JohnWiley e Sons*, 2000

[5] de Oliveira,H.M., Campello de Souza,R.M.,Kauffman, A.N. **Efficient Multiplex for Band-Limited Channels: Galois-Field Multiple Access. WCC.INRIA.**, Paris, *Proc. of the Workshop on Coding and Cryptography'99*,1999, pp. 235-241

[6] Bouton, E., **Multiplexação por divisão em multirresolução : um novo sistema baseado em wavelets**, 2006, Dissertação (Mestrado), - Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife

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

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

[9] Pollard,J. M.,**The Fast Fourier Transform in a Finite Field**, Math. Comput., vol.25, n.114, pp. 365-374, Apr. 1971.

[10] Lipschtz, S., **Schaum's outline of theory and problems of linear algebra**, *Makron Books*, 1994.

[11] Campello de Souza,R.M.,de Oliveira,H.M.**Eigensequences for Multiuser Communication over the Real Adder Channel**. *IEEE VI International Telecommunications Symposium (ITS2006)*.Sept. 3-6.Fortaleza. Brazil.

[12] Pei,S.-C.,Ding,J.-J., **Eigenfunctions of Linear Canonical Transforms**, *IEEE Trans. on Signal Proc.*,vol.50, n.1, Jan.,pp.11-26, 2002.

[13] Tseng,C.-C.,**Eigenvalues and Eigenvectors of Generalized DFT, Generalized DHT, DCT-IV and DST-IV Matrices**, *IEEE Trans. on Signal Process.*, vol.50, April, pp.866-877, 2002.

[14] L.R. Soares, H.M. de Oliveira, R.J.S. Cintra, R.M.C.Souza. **Fourier Eigenfunctions, Uncertainty Gabor Principle and Isoresolution Wavelets**,*XX Simpósio Bras. de Telecomunicações*,Rio de Janeiro, 5-8 Oct.,2003

[15] J.H. Conway. N.J.A. Sloane. **Sphere Packings. Lattices and Groups**. NY: *Springer-Verlag*, 1988.

[16] N.J.A. Sloane, **The Sphere Packing Problem**, *Shannon Lecture*, 1998.

[17] T.M. Thompson. **From Error-Correcting Codes Through Sphere Packings to Simple Groups**. *The Math. Assoc. of America*, 1983.