Novos Códigos de Bloco Construídos a Partir da Transformada de Fourier de Corpo Finito

Caio Marcelo Fernandes Barros[1]; Hélio Magalhães de Oliveira[2]

[1]Estudante do Curso de Engenharia Eletrônica – CTG – UFPE; E-mail: caio1408@yahoo.com.br,
[2]Docente/pesquisador do Depto de Eletrônica e Sistemas – CTG – UFPE. E-mail: hmo@ufpe.br.

Sumário: Apresentam-se uma nova classe de códigos de bloco baseado na transformada de Fourier de Corpo Finito. Como caso ilustrativo, foram calculadas as matrizes geradoras e de verificação de paridade para códigos desta classe até o comprimento N=36, gerados a partir do campo de Galois GF(37). A distância mínima dos códigos foi apenas determinada para alguns comprimentos de bloco, visto que a complexidade computacional exigida para tais cálculos é não-polinomial (NP).

Palavras–chave: Códigos de Blocos Clássicos; FFFT; Transformada de Fourier de Corpo Finito.

INTRODUÇÃO

Ante ao enorme crescimento nos serviços de telefonia e transmissão de dados, novas técnicas de multiplexação, que reduzam a complexidade computacional (reduzindo assim o tempo de processamento), são sempre bem-vindas. Neste contexto, recentemente, de Oliveira, Campello de Souza e colaboradores [1] desenvolveram uma técnica espectralmente eficiente, denominada por multiplexação por divisão em corpos finitos (GDM). Uma das áreas de enfoque moderno quando se relacionam os serviços telefônicos são as Transformadas. Motivados por amplas aplicações de transformadas – e dentre elas, as transformadas discretas – novas técnicas vêm surgindo aplicando-se com destaque a DFT (*Discrete Fourier Transform)*, em seguida a DHT (*Discrete Hartley Transform)* [2], [3].

Uma alternativa conveniente para aplicação das transformadas discretas no âmbito da comunicação multiusuário é o uso do conceito de autovalor e autovetor [4]. O estudo da aplicação de autoseqüências em sistemas de comunicação em canal real aditivo é uma área que vem merecendo particular atenção [5]. Através de investigações relacionadas com estas aplicações [6], [7], constata-se que esta é uma área rica em inovações. Vislumbrando uma nova contribuição, construiu-se uma nova classe de códigos: códigos projetados a partir de transformadas. Foi particularmente investigada, entre outras transformadas, a transformada de Fourier de Corpo Finito, introduzida por Pollard [8]. A partir desta, foram construídos códigos relacionados a esta transformada. A expectativa reside na esperança de que unidas com as teorias de códigos clássicos, desenvolva-se uma ferramenta atrativa do ponto de vista de complexidade computacional.

MATERIAIS E MÉTODOS

Os principais resultados deste trabalho são fundamentados na estrutura algébrica de códigos clássicos (codificação de canal de Shannon) [9], reticulados [10], transformadas de corpo finito [11], e transformadas discretas [12].

- A plataforma utilizada para a concepção dos aplicativos da simulação foi o Matlab®, construindo assim aplicativos e rotinas específicas. Foi também utilizado outro aplicativo, concebido anteriormente, que foi utilizado no escopo deste trabalho, a saber: Geração de Corpos GF(p^m).
- Concepção da família de códigos, utilizando técnicas de corpo finito [9]. Nesta implementação foi utilizada a transformada de Fourier sob um corpo finito [8] e para isso foram necessárias novas rotinas auxiliares para o *software* original.
- Implementação de um algoritmo que analisa a combinação linear de um dado vetor sobre o espaço de autovalores positivos e negativos, pois este fato pode ser utilizado para analisar um vetor sobre outros espaços dimensionais.

RESULTADOS

Foram projetados e construídos códigos de menor complexidade computacional que pudessem ser utilizados para obter cálculo espectral eficiente em processamento de sinais. Os parâmetros de alguns dos códigos obtidos no caso particular sobre GF(37) encontram-se ilustrados na Tabela 1. Mostram-se em alguns dos casos, as distâncias mínimas obtidas. A dimensão dos subespaços associados aos autovalores positivos e negativos (k^+ e k^-, respectivamente) são mostradas.

Tabela 1. Código de Fourier de Corpo Finito

i	n	k^+	k^-	d^+	d^-
2	36	9	10		
5	36	9	10		
6	4	1	2	4	2
7	9	2	3	6	
9	9	2	3	6	
10	3	1	1	3	3
12	9	2	3	6	
13	36	9	10		
16	9	2	3	6	
17	36	9	10		
23	12	4	3		
24	36	9	10		
26	3	1	1	3	3
29	12	4	3		
31	4	1	2	4	2
32	36	9	10		
33	9	2	3	6	
34	9	2	3	6	
35	36	9	10		

Legenda:

- i o núcleo da Transformada.
- n o comprimento do código.
- k_+ a dimensão do código para o autovalor "p".
- k_- a dimensão do código para o autovalor"p-1".
- d_+ a distância mínima do código para o autovalor "p".
- d_- a distância mínima do código para o autovalor "p-1".

Além dos códigos cujos parâmetros são mostrados, diversos outros códigos para outros corpos finitos foram também obtidos (e.g. p=7, 11, 13, 17, 19, 23, 29, 31).
Para todos estes códigos, foram determinadas as matrizes geradoras e de verificação de paridade, as quais são geradas por programa desenvolvido, e não foram incluídas aqui tendo em vista a grandes dimensões envolvidas (c.f. Tabela 1). Houve também a implementação computacional de um algoritmo de mapeamento de uma seqüência genérica no espaço gerado pelo autovalor "positivo" e que mostra potencialmente interessante na avaliação de desempenho das redes de serviço.

DISCUSSÃO & CONCLUSÕES

Esses códigos mostraram-se interessante por envolverem algoritmos de baixa complexidade aritmética para o cálculo espectral. É bem verdade que estes não apresentam alta distância mínima comparada ao tamanho do bloco, mas o seu desempenho sobre um canal real aditivo ainda deve ser analisado. O uso das auto-seqüências para comunicação de multiusuário é um ponto que ainda falta por ser investigado e que vem se revelando atrativo. Em suma, não houve conflito entre as simulações realizadas e nem entre essas e a teoria estudada, e o embasamento teórico para estes novos códigos foi bem fundamentado. Os novos códigos revelam-se promissores para as redes de dados com múltiplos usuários, particularmente graças à baixa complexidade dos algoritmos envolvidos.

AGRADECIMENTOS

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq): CMFB por bolsa de PIBIC-I; HMdO por apoio financeiro parcial CNPq#301996. Eles também agradecem ao Prof. Ricardo M. Campello de Souza (UFPE) e Juliano Bandeira (Pós-Graduação) (PPGEE-UFPE).

REFERÊNCIAS

[1] OLIVEIRA, Hélio Magalhães de; SOUZA, Ricardo Menezes Campello de; KAUFFMAN, André N.. Efficient Multiplex for Band-Limited Channels: Galois-Field Multiple Access. **Proc. Of The Workshop On Coding And Cryptography'99**, Paris, p.235-241, Set. 1999.

[2] BRACEWELL, R. N.. Discrete Hartley transform. **Journal Of The Optical Society Of America,** Usa, vol. 73, p. 1832-1835. Dec. 1983.

[3] BRACEWELL, R. N.. **The Hartley transform.** Ny: Oxford University Press, 1986.

[4] LIPSCHUTZ, S.. **Schaum's outline of theory and problems of linear algebra.** Usa: Makron Books, 1994.

[5] SOUZA, Ricardo Menezes Campello de; OLIVEIRA, Hélio Magalhães de. Eigensequences for Multiuser Communication over the Real Adder Channel. In: IV INTERNATIONAL TELECOMMUNICATIONS SYMPOSIUM (ITS2006), 2006, Fortaleza, Brazil. **Anais... .** Fortaleza: Ieee, 2006. p. xx - xx.

[6] PEI, Soo-chang; DING, Jian-jiun. Eigenfunctions of linear canonical transform. **Ieee Transactions On Signal Processing,** Usa, p. 11-26. jan. 2002.

[7] TSENG, Chien-cheng. Eigenvalues and eigenvectors of generalized DF, generalized DHT,DCT-IV and DST-IV matrices. **Ieee Transactions On Signal Processing,** Usa, p. 866-877. Apr. 2002.

[8] POLLARD, J. M. The Fast Fourier Transform in a Finite Field. **American Mathematical Society,** Usa, p. 365-374. Apr. 1971.

[9] LIN, Shu. **Error Control Coding Fundamentals and Applications.** Usa: Prentice Hall, 1983.

[10] CONWAY, John Horton; SLOANE, N. J. A.; BANNAI, Etsuko. **Sphere Packings, Lattices and Groups.** 3º Usa: Springer, 1998..

[11] OLIVEIRA, Hélio Magalhães de; SOUZA, Ricardo Menezes Campello de; KAUFFMAN, André N.. The Hartley Transform over a Finite Field. **Revista da Sociedade Brasileira de Telecomunicações**, São Paulo, n. , p.46-54, set. 1999.

[12] OPPENHEIM, A. V.. **Discrete-Time Signal Processing.** Usa: Prentice Hall, 1989.