Fourier Codes

R. M. Campello de Souza
E. S. V. Freire
H. M. de Oliveira

Federal University of Pernambuco - UFPE
Department of Electronic and Systems - DES
Signal Processing Group - GPS

July 2009

Summary

Summary

Introduction

Fourier Number Theoretic Transform - FNTT

- The $GF(p)$-valued sequences $x = (x_0, x_1, \ldots, x_{N-1})$ and $X = (X_0, X_1, \ldots, X_{N-1})$, form an unitary FNTT pair when

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

and

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

where $\alpha \in GF(p)$ has multiplicative order N and $N^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$.

Introduction

Eigensequences of the FNTT

- A sequence x is said to be an eigensequence of the FNTT, with associated eigenvalue $\lambda \in GF(p^2)$, when it satisfies $X = \lambda x$.
- The eigenvalues of the FNTT are the fourth roots of unity $(\pm 1, \pm j)$, where $j^2 \equiv -1 (\mathrm{mod}\ p)$.

Introduction

Eigensequences of the FNTT

- Lemma 1: If x is an FNTT eigensequence, then it has even symmetry (i.e. $x_i = x_{N-i}$) if $\lambda \equiv \pm 1 (\mathrm{mod}\ p)$ and odd symmetry (i.e. $x_i = -x_{N-i}$) if $\lambda \equiv \pm j (\mathrm{mod}\ p)$.

Fourier Codes

FNTT Matrix

$$F = (\sqrt{N})^{-1}(mod p) \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \dots & \alpha^{(N-1)(N-1)} \end{bmatrix}$$

Fourier Codes

Code Construction

- If x is an eigensequence of the linear transform F, then $Fx = \lambda x$.
- $\Rightarrow (F - \lambda I)x = 0 \Rightarrow H^* = (F - \lambda I)$

Fourier Codes

Example: Constructing linear block codes from the FNTT of length $N = 5$, over $GF(41)$. Consider $\alpha = 10$, an element of order 5 in the given field, $\sqrt{5} \equiv 13(mod41)$ and $j \equiv 9(mod41)$. From the transform matrix F one obtains

$$F - \lambda I = \begin{bmatrix} 19-\lambda & 19 & 19 & 19 & 19 \\ 19 & 26-\lambda & 14 & 17 & 6 \\ 19 & 14 & 6-\lambda & 26 & 17 \\ 19 & 17 & 26 & 6-\lambda & 14 \\ 19 & 6 & 17 & 14 & 26-\lambda \end{bmatrix}$$

Fourier Codes

Considering $H = [I_{N-k}|P_\lambda]$ and $G = [-P_\lambda^T|I_k]$, we have the following codes

$F(5,2)$

$$H^{+1} = \begin{bmatrix} 1 & 0 & 0 & 34 & 34 \\ 0 & 1 & 0 & 0 & 40 \\ 0 & 0 & 1 & 40 & 0 \end{bmatrix}; G^{+1} = \begin{bmatrix} 7 & 0 & 1 & 1 & 0 \\ 7 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$F(5,1)$

$$H^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 12 \\ 0 & 1 & 0 & 0 & 40 \\ 0 & 0 & 1 & 0 & 40 \\ 0 & 0 & 0 & 1 & 40 \end{bmatrix}; \quad G^{-1} = \begin{bmatrix} 29 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Fourier Codes

$$F(5,1) \qquad H^{+j} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 31 \\ 0 & 0 & 0 & 1 & 10 \end{bmatrix}; \quad G^{+j} = \begin{bmatrix} 0 & 40 & 10 & 31 & 1 \end{bmatrix}$$

$$F(5,1) \qquad H^{-j} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 37 \\ 0 & 0 & 0 & 1 & 4 \end{bmatrix}; \quad G^{-j} = \begin{bmatrix} 0 & 40 & 4 & 37 & 1 \end{bmatrix}$$

The Code Parameters

- Code block length n: order N of the FNTT matrix;
- Dimension k: Multiplicity of the associated eigenvalue λ;

N	Mult of 1	Mult of -1	Mult of -j	Mult of +j
4m	m+1	m	m	m-1
4m+1	m+1	m	m	m
4m+2	m+1	m+1	m	m
4m+3	m+1	m+1	m+1	m

The multiplicity of λ depends on the value of $\sqrt{N}(mod p)$.

The Code Parameters

- Proposition 1: Let $H^{\lambda} = [I_{n-k}|P]$ be the parity-check matrix of an $F^{\lambda}(n, k, d)$ Fourier Code over $GF(p)$. Then the submatrix P contains a secondary diagonal matrix D_s, of order k, with entries m, where $m = p - 1$ if $\lambda = \pm 1(modp)$ and $m = 1$ if $\lambda = \pm j(modp)$.

for $\lambda = \pm 1$, $m = p - 1$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 3 & 5 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 16 \\ 0 & 0 & 1 & 0 & 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 1 & 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 14 & 5 & 14 \end{bmatrix}$$

for $\lambda = \pm j$, $m = 1$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 11 & 16 \end{bmatrix}$$

The Code Parameters

The Minimum Distance

Proposition 2 (An upper bound on the minimum distance): The minimum distance of a Fourier code $F^{\lambda}(n, k, d)$ satisfies $d \leq n - 2k + 2$.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 3 & 5 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 16 \\ 0 & 0 & 1 & 0 & 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 1 & 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 14 & 5 & 14 \end{bmatrix}$$

The Code Parameters

The Minimum Distance

Corollary: For $F^{\lambda}(n, k, d)$, with $\lambda = \pm j$, the code minimum distance satisfies $d \leq n - 2k$.

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 11 & 16 \end{bmatrix}$$

Parameters of some Fourier codes

N	k^{+1}	d^{+1}	k^{-1}	d^{-1}	k^{+j}	d^{+j}	k^{-j}	d^{-j}
3	1	3	1	3	-	-	1	2
4	2	2	1	4	-	-	1	2
5	2	3	1	5	1	4	1	4
6	2	4	2	4	1	4	1	4
7	2	5	2	5	1	6	2	4
8	3	4	2	4	1	6	2	4
9	3	3	2	6	2	6	2	6
10	3	6	3	6	2	6	2	6
11	3	7	3	7	2	8	3	6
12	4	4	3	6	3	4	2	6

Error Control based on the FNTT Eigenstructure

Syndrome Computation

$$S = Fr - \lambda I$$

- $r = x + e$ is the received sequence
- S is zero if, and only if, r is a codeword

Single Error Correction - The symmetric case

$$r = (r_0, r_1, r_2, r_i, \ldots, r_{N-i} \ldots, r_{N-1})$$

According to Definition 1, if N is odd, r_0 must satisfy

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

$$r = (r_0, r_1, r_2, r_i, \ldots, r_{N/2}, \ldots, r_{N-i} \ldots, r_{N-1})$$

If N is even, the possible error occurred at position r_0 or $r_{N/2}$.

$$r_{N/2} = r_0(\lambda\sqrt{N} - 1)(r_1 + \ldots + r_{N/2-1} + r_{N/2+1} + \ldots + r_{N-1})$$

Double Error Correction - The nonsymmetric case

3 possible options:

1. Errors in symbols r_0 and r_i, $i \neq 0$
2. Errors r_i and r_{N-i}
3. Error in r_i, $i \neq 0$ and in r_j, $j \neq N - i$

Decoding algorithms for double errors

Decoding algorithm 2: $r = (r_0, r_1, r_2, r_i, \ldots, r_{N-i} \ldots, r_{N-1})$

- Make $r_i = \frac{1}{2}(\lambda\sqrt{N}r_0 - \sum_{\substack{j=0 \\ j\neq i, N-i}}^{N-1} r_j)$ and $r_{N-i} = r_i$;
- If the sequence is an eigensequence, decoding is complete. Otherwise, more than two errors have occurred.

Decoding algorithm 2 - Example 1

Consider the double-error correcting code $F^1(7, 2, 5)$ over $GF(19)$, with $\alpha = 7$, $\sqrt{7} \equiv 6(mod 29)$, generator matrix

$$G = \begin{bmatrix} 16 & 0 & 1 & 10 & 10 & 1 & 0 \\ 20 & 1 & 0 & 20 & 20 & 0 & 1 \end{bmatrix},$$

and received sequence $r = (16, 2, 1, 10, 10, 1, 3)$.

$r_i = \frac{1}{2}(\lambda\sqrt{N}r_0 - \sum_{\substack{j=0 \\ j\neq i, N-i}}^{N-1} r_j) \Longrightarrow r^{(1)} = (16, 0, 1, 10, 10, 1, 0)$ and

$R^{(1)} = (16, 0, 1, 10, 10, 1, 0). \Longrightarrow$ Decoding is complete!

Final Remarks

- We have introduced a new family of nonbinary linear block codes, the Fourier codes.
- The codewords of a Fourier code $F^{\lambda}(n, k, d)$ are the eigensequences of the Fourier number theoretic transform, associated with a given eigenvalue λ.

Final Remarks

- Strategies for single and double error control based on the FNTT eigenstructure were examined.
- The approach described can be extended to other families of finite field transforms
- The restrictions on the code parameters can be removed if arbitrary linear transforms are considered.