The Discrete Fourier Transform in Coding and Cryptography

James L. Massey

Signal & Info. Proc. Lab., Swiss Federal Inst. Tech., ETH-Zentrum, CH-8092, Zürich, Switzerland

Abstract — **Some applications of the Discrete Fourier Transform (DFT) in coding and in cryptography are described. The DFT over general commutative rings is introduced and the condition for its existence given. Blahut's Theorem, which relates the DFT to linear complexity, is shown to hold unchanged in general commutative rings.**

I. The (Usual) Discrete Fourier Transform

Let ξ be a primitive N^{th} root of unity in a field $\mathcal{F}$, i.e., $\xi^N = 1$ but $\xi^i \neq 1$ for $1 \leq i < N$. The (usual) *Discrete Fourier Transform (DFT)* of length N generated by ξ is the mapping $\mathrm{DFT}_\xi(\cdot)$ from $\mathcal{F}^N$ to $\mathcal{F}^N$ defined by $\mathbf{B} = \mathrm{DFT}_\xi(\mathbf{b})$ in the manner

$$B[i] = \sum_{n=0}^{N-1} b[n]\xi^{in} \tag{1}$$

where $\mathbf{b} = (b[0], b[1], \ldots b[N-1])$ is the "time-domain" sequence and $\mathbf{B} = (B[0], B[1], \ldots B[N-1])$ is the "frequency-domain" sequence. As is very well known, the inverse transform is given by

$$b[n] = \frac{1}{N} \sum_{i=0}^{N-1} B[i]\xi^{-in} \tag{2}$$

where N denotes the sum of N 1's in the field $\mathcal{F}$.

II. The DFT in Coding

Coding applications of the DFT rely on the polynomial formulation of the DFT. One identifies the N-tuple $\mathbf{b} = (b[0], b[1], \ldots b[N-1])$ with the polynomial $b(X) = b[0] + b[1]X + \ldots b[N-1]X^{N-1}$ and notes that (1) can then be written as

$$B[i] = b(\xi^i). \tag{3}$$

A cyclic code of length N over a finite field $\mathcal{F}$, or a subfield of $\mathcal{F}$, with generator polynomial $g(X)$ where $g(X)$ must divide $X^N - 1$, is the set of all $\mathbf{b}$ such that $g(X)$ divides $b(X)$. But the zeroes of $X^N - 1$ are all the ξ^i for $0 \leq i < N$ so that $g(X)$ is uniquely characterized by those i for which ξ^i is a zero, say $i \in \mathcal{J}$. It follows that $\mathbf{b}$ is a codeword if and only if $B[i] = 0$ for $i \in \mathcal{J}$. Particularly Blahut [1], [2] has shown the power of this approach for the study of cyclic codes.

What makes the DFT useful in coding is its relation to the linear complexity of sequences. The *linear complexity* of a sequence $s_0, s_1, \ldots s_{n-1}$ [where $n = \infty$ is allowed] is the length L of the shortest linear feedback shift register (LFSR) that, when loaded initially with $s_0, s_1, \ldots s_{L-1}$, produces the entire sequence as its output [3]. The connection to the DFT, which was used implicitly in [1] and is proved in [4], is the following.

Theorem 1 *("Blahut's Theorem") If* $\mathbf{B} = DFT_\xi(\mathbf{b})$ *for the DFT in any field* $\mathcal{F}$*, then the linear complexity of the periodically repeated sequence* $\mathbf{B}, \mathbf{B}, \mathbf{B}, \ldots$ *is equal to* $w_H(\mathbf{b})$*, the Hamming weight of* $\mathbf{b}$*.*

Because a sequence containing a run of $d-1$ consecutive zeroes followed by a non-zero digit has linear complexity at least d, it follows that if $g(X)$ has $d-1$ consecutive powers of ξ as zeroes, then every non-zero codeword in the corresponding cyclic code has Hamming weight at least d so that the minimum distance of the code satisfies $d_{\min} \geq d$. This is the well known BCH bound. All of the known lower bounds on the minimum distance of cyclic codes can be derived in an analogous fashion, cf. [4] for examples.

III. The DFT in Cryptography

Linear complexity plays a very important role in the theory of stream ciphers so it is not surprising that the DFT has been applied to such problems, cf. [5], [6]. More surprisingly perhaps has been the application of the multidimensional DFT over the real numbers with $\xi = -1$ and thus length $N = 2$ in each dimension [i.e., the Walsh-Hadamard transform] to the analysis of a sequences produced by a nonlinear combination of sequences.

Siegenthaler [7] defined a boolean function of n binary variables to be m^{th}-order correlation immune if, when the inputs are independent balanced binary random variables, the output is independent of every set of m or fewer of the inputs. It was shown in [8] that this is equivalent to the vanishing at all n-dimensional "frequencies" with Hamming weight between 1 and m, inclusive, of the Walsh-Hadamard transform of the function table of the boolean function when the arguments of the function are taken as the "time" indices and the function values treated as the real numbers 0 and 1. A particularly elegant proof of this result was given by Brynielsson [9].

IV. The Discrete Fourier Transform over Commutative Rings

We now enquire into the conditions under which the Discrete Fourier Transform (1) and its inverse (2) can be applied to sequences with components in a commutative ring $\mathcal{R}$ rather than in a field. Hereafter, ξ denotes a primitive N^{th} root of unity in such a ring.

We first note that (1) can be written in matrix form as

$$\mathbf{B} = \mathrm{M}_\xi \, \mathbf{b} \tag{4}$$

where M_ξ is the $N \times N$ matrix

$$\mathrm{M}_\xi = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \xi & \xi^2 & \ldots & \xi^{N-1} \\ 1 & \xi^2 & \xi^{2\cdot 2} & \ldots & \xi^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^{N-1} & \xi^{(N-1)2} & \ldots & \xi^{(N-1)(N-1)} \end{bmatrix}. \tag{5}$$

The matrix equation (4) is uniquely solvable for $\mathbf{b}$ when $\mathbf{B}$ is given, and the inverse is given by (2), just when the determinant of M_ξ, denoted $\Delta(\mathrm{M}_\xi)$, is a *unit* of the ring $\mathcal{R}$, i.e., a ring element having a multiplicative inverse. But M_ξ can

be seen from (5) to be a Vandermonde matrix and hence its determinant is simply

$$\Delta(\mathrm{M}_\xi) = \prod_{j=1}^{N-1}\prod_{i=0}^{j-1}(\xi^j - \xi^i) = \prod_{j=1}^{N-1}\prod_{i=0}^{j-1}\xi^i(\xi^{j-i}-1). \quad (6)$$

But a product of ring elements is a unit if and only if each element is a unit, and ξ itself is a unit since $\xi \cdot \xi^{N-1} = 1$. It follows that $\Delta(\mathrm{M}_\xi)$ is a unit if and only if $\xi^k - 1$ is a unit for $1 \le k < N$. We summarize:

Theorem 2 *If ξ is a primitive N^{th} root of unity in a commutative ring $\mathcal{R}$, then (1) defines an invertible mapping from $\mathcal{R}^N$ to $\mathcal{R}^N$ whose inverse is given by (2) if and only if $\xi^k - 1$ is a unit in $\mathcal{R}$ for $k = 1, 2, \ldots N-1$.*

It follows immediately from Theorem 2 that if ξ generates a DFT of length N in a commutative ring $\mathcal{R}$ and L $(L > 1)$ is a divisor of N, then $\xi^{N/L}$ generates a DFT of length L in $\mathcal{R}$, exactly as for the field case.

For examples, we use the ring of integers modulo m, Z_m. We recall that an element i of Z_m is a unit if and only if $\gcd(m, i) = 1$. If m is a prime, then Z_m is the finite field of m elements so that the DFT in Z_m is novel just when m is composite.

Example 1: $\xi = 2$ is a primitive fourth root of unity in Z_{15} but does not generate a DFT of length $N = 4$ in this ring because, although $\xi - 1 = 1$ is a unit, $\xi^2 - 1 = 3$ is not a unit.

Example 2: $\xi = 8$ is a primitive fourth root of unity in Z_{65} and generates a DFT of length $N = 4$ because $\xi - 1 = 7$, $\xi^2 - 1 = 63$, and $\xi^3 - 1 = 57$ are all units in Z_{65}.

With the aid of Theorem 2 it is an easy matter to prove the following standard result for the DFT over Z_m, which is often referred to as the "Number Theory Transform" or NTT, cf. pp. 211-217 in [10].

Theorem 3 *If $m = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $p_1, p_2, \ldots p_k$ are distinct primes and $e_1, e_2, \ldots e_k$ are positive integers, then there exists a DFT of length N over Z_m if and only if N is a divisor of* $\gcd(p_1 - 1, p_2 - 1, \ldots p_k - 1)$.

V. Blahut's Theorem over Commutative Rings

An immediate question, which we now investigate, is whether Blahut's Theorem holds for the DFT (when it exists) over a general commutative ring.

Let ξ generate a DFT of length N in the commutative ring $\mathcal{R}$. Then, because $1 - \xi^i D$ has a unit of $\mathcal{R}$ as its constant term and hence is a unit in the ring $\mathcal{R}((D))$ of formal power series in the indeterminate D, we can write

$$\frac{1 - D^N}{1 - \xi^i D} = 1 + \xi^i D + \xi^{2i} D^2 + \ldots + \xi^{(N-1)i} D^{N-1}. \quad (7)$$

Let $\mathbf{B} = (B[0], B[1], \ldots B[N-1])$ be arbitrary in $\mathcal{R}^N$ and consider the (modified) partial fraction expansion

$$B[0] + B[1]D + \ldots + B[N-1]D^{N-1} = \sum_{n=0}^{N-1} b[n]\frac{1 - D^N}{1 - \xi^n D}. \quad (8)$$

Using (7) and equating coefficients of like powers of D on both sides in (8) yields the matrix equation

$$\mathbf{B} = \mathrm{M}_\xi \ \mathbf{b} \quad (9)$$

where $\mathbf{b} = (b[0], b[1], \ldots b[N-1])$ and where M_ξ is the matrix in (4). It follows that $\mathbf{B}$ is the DFT of $\mathbf{b}$ and hence that (8) is uniquely solvable for the coefficients in the (modified) partial fraction expansion. Writing the right side of (8) as

$$\frac{P(D)}{C(D)} = \sum_{\substack{n=0 \\ b[n]\neq 0}}^{N-1} b[n]\frac{1 - D^N}{1 - \xi^n D}, \quad (10)$$

where

$$C(D) = \prod_{\substack{n=0 \\ b[n]\neq 0}}^{N-1} (1 - \xi^n D) \quad (11)$$

is a polynomial of degree $w_H(\mathbf{b})$ in the ring $\mathcal{R}[D]$ of polynomials in the indeterminate D and where the polynomial $P(D)$ has degree strictly less than that of $C(D)$, and dividing by $1 - D^N$, which is a unit in $\mathcal{R}((D))$, we obtain

$$\frac{P(D)}{C(D)} = (B[0] + B[1]D + \ldots + B[N-1]D^{N-1})\frac{1}{1 - D^N}. \quad (12)$$

The right side of (12) is the power series corresponding to the periodically repeated sequence $\mathbf{B}, \mathbf{B}, \mathbf{B}, \ldots$ and hence (12) shows that $C(D)$ as given by (11) is the connection polynomial of the shortest LFSR with feedback coefficients in $\mathcal{R}$ that can generate this semi-infinite sequence, cf. [3]. This shortest LFSR has length $\max\{\deg[C(D)], 1 + \deg[P(D)]\}$, which by definition is the linear complexity of the sequence, and thus we have the following result.

Theorem 4 *("Blahut's Theorem for Commutative Rings") If ξ generates a DFT of length N in a commutative ring $\mathcal{R}$ and $\mathbf{B} = DFT_\xi(\mathbf{b})$, then the linear complexity of the periodically repeated sequence $\mathbf{B}, \mathbf{B}, \mathbf{B}, \ldots$ is equal to $w_H(\mathbf{b})$, the Hamming weight of $\mathbf{b}$.*

References

[1] R. E. Blahut, "Transform Techniques for Error Control Codes," *IBM J. Res. Dev.*, vol. 63, pp. 550-560, 1979.

[2] R. E. Blahut, *Theory and Practice of Error Control Codes.* Reading, MA: Addison-Wesley, 1983.

[3] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. on Info. Th.*, Vol. IT-15, pp. 122-127, Jan. 1969.

[4] J. L. Massey and T. Schaub, "Linear Complexity in Coding Theory," in *Coding Theory and Applications* (Eds G. Cohen and Ph. Godlewski), Lecture Notes in Computer Science, No. 311. Heidelberg and New York: Springer, 1988, pp. 19-32.

[5] J. L. Massey and S. Serconek, "A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences," *Advances in Cryptology-CRYPTO '94* (Ed. Y. G. Desmedt), Lecture Notes in Computer Science No. 839. New York: Springer, pp. 322-340, 1994.

[6] J. L. Massey and S. Serconek, "Linear Complexity of Periodic Sequences: A General Theory," in Advances in Cryptology-CRYPTO'96 (Ed. N. Koblitz), Lecture Notes in Computer Science No. 1109. New York: Springer, 1996, pp. 358-371.

[7] T. Siegenthaler, "Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications," *IEEE Trans. Info. Th.*, vol. IT-30, pp. 776-780, Oct. 1984.

[8] G. Z. Xiao and J. L. Massey, "A Spectral Chracterization of Correlation-Immune Combining Functions," IEEE Trans. Info. Th., Vol. IT-34, pp. 569-571, May 1988.

[9] L. Brynielsson, "A Short Proof of the Xiao-Massey Lemma," IEEE Trans. Info. Th., vol. IT-35, p. 1344, Nov. 1989.

[10] H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms.* Berlin: Springer, 1982.