Efficient DFT of Zadoff-Chu sequences

B.M. Popovic

Closed-form expressions for the discrete Fourier transform (DFT) of cyclically shifted Zadoff-Chu sequences of arbitrary length are presented. These expressions allow for a very efficient DFT implementation based only on the elements of the corresponding already generated basic (non-cyclically-shifted) ZC sequence.

Introduction: Zadoff-Chu (ZC) sequences [1, 2] have been extensively used in various parts of the LTE cellular standard [3]. In particular, the random access (RA) preambles transmitted from the mobile user equipment (UE) are generated from cyclically shifted ZC sequences of a prime length N, by using so-called DFT-S-OFDM modulation ([3], pp. 348 and 438). The first step in generating such RA preambles is to perform an N-point discrete Fourier transform (DFT) of a cyclically shifted ZC sequence characterised by the root index u and the cyclic shift p.

Besides this particular application, a closed-form expression of the DFT of ZC sequences is of general interest for any signal design based on the application of ZC sequences in the Fourier frequency domain. An attempt to obtain such a closed-form representation has been made in [4], but the result is valid for a single, very special combination of the sequence length N and the root index u (N even, $u = 1$). Additionally, this DFT formula does not reveal an efficient DFT implementation structure. Much more general closed-form results, for discrete chirp sequences of arbitrary length, have been obtained in [5]. However, these closed-form expressions still do not reveal the efficient DFT implementation for cyclically shifted ZC sequences.

The efficient DFT structures more suitable for applications of ZC sequences have been derived in [6] and [7] for prime length ZC sequences. However, these formulas are semi-analytical, i.e. contain a constant that is supposed to be computed numerically.

In this Letter, we present compact closed-form expressions for the DFT of cyclically shifted ZC sequences of arbitrary length as a function based only on the elements of the corresponding already generated basic (non-cyclically-shifted) ZC sequence.

Definitions and related prior results: The DFT of a sequence $\{x_u(k)\}$ is defined as

$$X_u(n) = \sum_{k=0}^{N-1} x_u(k) W_N^{nk}, \quad W_N = e^{-j2\pi/N}, \quad j = \sqrt{-1}, N \text{any positive integer} \tag{1}$$

A Zadoff-Chu sequence $\{x_u(k)\}$ has been defined as [1]

$$x_u(k) = W_N^{uk(k+N \bmod 2)/2}, \quad k = 0, 1, \ldots, N-1, \quad N \text{any positive integer} \tag{2}$$

where the root index u is an integer less than and relatively prime to N.

A formula for the DFT of ZC sequences (2) of prime length N has been derived in [6], as

$$X_u(n) = W_N^{-\frac{n(n+u)}{2u}} X_u(0) \tag{3}$$

$$X_u(0) = \sum_{k=0}^{N-1} x_u(k) \tag{4}$$

Eqn. (3) is used in [6] to derive the efficient bank of matched filters for the pair of random access preambles $\{x_{u,p}(k)\}$ and $\{x_{N-u,p}(k)\}$, used in the base station receiver ([3], p.451) where

$$x_{u,p}(k) = x_u((k+p) \bmod N) \tag{5}$$

is a cyclically shifted (by p) version of $\{x_u(k)\}$. Later on, in [7, eqn. (4)], (3) has been put into another form as

$$X_u(n) = x_u^*(u^{-1}n) X_u(0), \quad n = 0, 1, \ldots, N-1, \quad N \text{ prime} \tag{6}$$

where '*' denotes complex conjugation, and $u^{-1} = 1/u$ is the modular multiplicative inverse of u, i.e. an integer such that $u \cdot u^{-1} = 1 \bmod N$.

However, (6) cannot always be used to reduce the number of operations in the transmitter of LTE UE, as the transmitted RA preamble can be a cyclically shifted version of the ZC sequence. Thus it is of interest to find a closed-form expression for

$$X_{u,p}(n) = \sum_{k=0}^{N-1} x_u(k+p) W_N^{nk}, \quad n = 0, 1, \ldots, N-1 \tag{7}$$

where ZC sequence is slightly generalised as [8]

$$x_u(k) = W_N^{uk(k+N \bmod 2+2q)/2}, \quad k = 0, 1, \ldots, N-1, \quad u < N, \ (u, N) = 1 \tag{8}$$

where N is any positive integer and q is any integer, in order to encompass a broader class of sequences with ideal periodic autocorrelation function.

Efficient DFT: To obtain the structure of an efficient DFT of a cyclically shifted ZC sequence, we start by rewriting (7) as

$$X_{u,p}(n) = \sum_{l=0}^{N-1} x_u(l) W_N^{ud(l-p)}, \quad n = 0, 1, \ldots, N-1 \tag{9}$$

where $l = k + p$, $d = u^{-1} n \bmod N$. Then we note that the ZC sequences (8) have the following property:

$$x_u(a+b) = x_u(a) x_u(b) W_N^{uab} \tag{10}$$

By applying (10) to (9) we obtain

$$\begin{aligned} X_{u,p}(n) &= W_N^{-udp} x_u^*(d) \sum_{l=0}^{N-1} x_u(l+d) \\ &= x_u^*(d+p) x_u(p) X_u(0) \\ &= x_u^*(u^{-1}n + p) x_u(p) X_u(0) \end{aligned} \tag{11}$$

From (11) it follows that, for a given root u and the cyclic shift p of a ZC sequence of any length N, the corresponding DFT is cyclically delayed (by p) and then cyclically sampled (by integer increment u^{-1}) complex-conjugated version of already generated ZC sequence, multiplied by a constant, consisting of two factors: the $(p+1)$th element of the ZC sequence, and the sum of all the elements of the ZC sequence. Thus, the DFT can be calculated by $N-1$ complex additions and $N+1$ complex multiplications, by using only the elements of already generated ZC sequence (8). The constant $X_u(0)$ can be expressed in closed-form as

$$X_u(0) = \begin{cases} \left(\frac{2N}{u}\right) W_{2N}^{-uq^2} e^{j\frac{\pi}{4}(u-2)} \sqrt{N}, & \text{for } N \text{ even} \\ \left(\frac{u\alpha}{N}\right) x_u(\beta) \frac{1+j^N}{1+j} \sqrt{N}, & \text{for } N \text{ odd} \end{cases} \tag{12}$$

$$\alpha = \frac{N+1}{2}, \quad \beta = \left(\frac{N-1}{2} - q\right) \bmod N$$

where $(2N/u)$ and $(u\alpha/N)$ denote Jacobi symbols. A Jacobi symbol (a/b) can have values 0, +1 or −1, and is defined for any integer a, and any positive odd integer b, as

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k} \tag{13}$$

where $p_1, p_2, \ldots p_k$ are primes, $e_1, e_2, \ldots e_k$ are positive integers, such that $b = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, and (a/p_l) is a Legendre symbol, defined for any integer a and any prime p_l as

$$\left(\frac{a}{p_l}\right) = \begin{cases} 0, & \text{if } a = 0 \bmod p_l \\ +1, & \text{if } a \neq 0 \text{ is a square mod } p_l \\ -1, & \text{if } a \neq 0 \text{ is a nonsquare mod } p_l \end{cases} \tag{14}$$

A Jacobi symbol can be efficiently iteratively calculated without actual calculation of Legendre symbols.

With closed-form expressions for $X_u(0)$ according to (12), the number of operations for obtaining the DFT coefficients for ZC sequences might be reduced, as $N-1$ complex additions are replaced by a multiplication and a sign calculation. If the $X_u(0)$ has been prestored for each root index u and each sequence length N, the formula (12) enables reduction of the corresponding look-up table size. If N is a prime, as it is in the LTE system, the lookup table should contain $(N-1)$ complex values of $X_u(0)$ for each N; by using (12), this lookup table for each N can be reduced to a single real value $\sqrt{N}$, and $(N-1)/2$ binary values of the Legendre

symbol $(a/N) = (-1)^{(N-1)/2}(N-a/N) = \pm 1, \quad a = 1, 2, \ldots, (N-1)/2$, so that $(u\alpha/N) = (u/N)(\alpha/N)$ can be obtained by addressing this table with u and α. The remaining two values in (12) can be easily obtained: $x_u(\beta)$ is the element of already available ZC sequence, while the value of $(1+j^N)/(1+j)$ is either 1 or j, depending on whether Nmod4 is 1 or 3, respectively. The proof of (12) is given below.

Proof of (12): For N even, as a ZC sequence is periodic with period N, we can rewrite (4) as

$$\begin{aligned} X_u(0) &= \frac{1}{2}\sum_{k=0}^{2N-1} W_{2N}^{uk(k+2q)} \\ &= \frac{1}{2} W_{2N}^{-uq^2} \sum_{k=0}^{2N-1} W_{2N}^{u(k+q)^2} \\ &= \frac{1}{2} W_{2N}^{-uq^2} G(u, 2N)^* \end{aligned} \tag{15}$$

where $G(m, L)^*$ is the complex conjugate of the quadratic Gauss sum $G(m, L) = \sum_{k=0}^{L-1} W_L^{-mk^2}$, equal to [9]

$$G(m, L) = \begin{cases} \left(\frac{m}{L}\right)\sqrt{L}, & L = 1 \bmod 4 \\ \left(\frac{m}{L}\right) j\sqrt{L}, & L = 3 \bmod 4 \\ \left(\frac{L}{m}\right)(1+j^m)\sqrt{L}, & L = 0 \bmod 4 \\ 0, & L = 2 \bmod 4 \end{cases} \tag{16}$$

where (m/L) and (L/m) denote Jacobi symbols defined by (13), and $(m, L) = 1$.

The expression for $G(u, 2N)$ is given by (16) for $L = 0 \bmod 4$ ($2N = 0 \bmod 4$ for any N even), so when it is inserted in (15) it follows that

$$\begin{aligned} X_u(0) &= W_{2N}^{-uq^2}\left(\frac{2N}{u}\right)(1-j^u)\sqrt{\frac{2N}{4}} \\ &= \left(\frac{2N}{u}\right) W_{2N}^{-uq^2} e^{j\frac{\pi}{4}(u-2)}\sqrt{N} \end{aligned}$$

For N odd, $\alpha = (N+1)/2$ is an integer, so we can rewrite (4) as

$$X_u(0) = \sum_{k=0}^{N-1} W_N^{u\alpha k(k+1+2q)} \tag{17}$$

where we have used the fact

$$W_N^{u(N/2)k(k+1+2q)} = e^{-j2\pi uk(k+1)/2} = 1$$

as $k(k+1)/2$ is an integer for any integer k.

By introducing an additional integer $\beta = \{(N-1)/2 - q\} \bmod N$, we can rewrite (17) as

$$X_u(0) = \sum_{k=0}^{N-1} W_N^{u\alpha[(k-\beta)^2 - \beta^2]} \tag{18}$$

Before we proceed with (18), it will be useful to note that

$$\begin{aligned} \beta(q+\alpha N)/2 &= \beta[q + (\beta+1+q)N]/2 \\ &= \beta q(N+1)/2 + N\beta(\beta+1)/2 \\ &= \alpha\beta q \bmod N \end{aligned} \tag{19}$$

as $\beta(\beta+1)/2$ is always an integer. Now we can continue from (18) as

$$\begin{aligned} X_u(0) &= W_N^{-u\alpha\beta^2} \sum_{k=0}^{N-1} W_N^{u\alpha k^2} \\ &= W_N^{u\alpha\beta/2} W_N^{-u(N/2)\alpha\beta} W_N^{u\alpha\beta q} G(u\alpha, N)^* \\ &= x_u(\beta)\ W_N^{-u\beta q/2} W_N^{-u(N/2)\alpha\beta} W_N^{u\alpha\beta q} G(u\alpha, N)^* \\ &= x_u(\beta)\ W_N^{-u\beta(q+\alpha N)/2} W_N^{u\alpha\beta q} G(u\alpha, N)^* \\ &= x_u(\beta)\ G(u\alpha, N)^* \end{aligned} \tag{20}$$

where we used the identity (19), and where $G(u\alpha, N)$ is given by (16) for L odd. By replacing (16) into (20) we complete the proof of (12).

Conclusions: Compact closed-form expressions for the DFT of cyclically shifted ZC sequences of arbitrary length are presented. These expressions allow for a very efficient DFT implementation based only on the elements of the corresponding already generated basic (non-cyclically-shifted) ZC sequence.

© The Institution of Engineering and Technology 2010
21 December 2009
doi: 10.1049/el.2010.3510

B.M. Popovic (*Huawei Technologies Sweden, PO Box 54, SE-164 94 Kista, Stockholm, Sweden*)

E-mail: branislav.popovic@huawei.com

References

1 Chu, C.: 'Polyphase codes with good periodic correlation properties', *IEEE Trans. Inf. Theory*, 1972, **18**, pp. 531–532
2 Frank, R.L.: 'Comments on polyphase codes with good periodic correlation properties', *IEEE Trans. Inf. Theory*, 1973, **19**, p. 244
3 Sesia, S., Toufik, I., Baker, M. (Eds.): 'LTE – the UMTS long term evolution: from theory to practice' (John Wiley & Sons Ltd, Chichester, UK, 2009)
4 Li, C., and Huang, W.: 'A constructive representation for the Fourier dual of the Zadoff-Chu sequences', *IEEE Trans. Inf. Theory*, 2007, **53**, pp. 4221–4224
5 Brodzik, A.: 'On the Fourier transform of finite chirps', *IEEE Signal Process. Lett.*, 2006, **13**, (9), pp. 541–544
6 Popovic, B.M., and Mauritz, O.: 'Efficient matched filters for paired root Zadoff-Chu sequences'. 3GPP RAN1#48bis meeting, source: Huawei, tdoc number R1-071409, St. Julian's, Malta, March 2007
7 Beyme, S., and Leung, C.: 'Efficient computation of DFT of Zadoff-Chu sequences', *Electron. Lett.*, 2009, **45**, (9), pp. 461–463
8 Popovic, B.M.: ''Generalized chirp-like polyphase sequences with optimum correlation properties,'', *IEEE Trans. Inf. Theory*, 1992, **38**, (4), pp. 1406–1409
9 Berndt, B.C., Evans, R.J., and Williams, K.S.: 'Gauss and Jacobi sums'' (Wiley-Interscience, New York, USA, 1998)