Techniques for Computing the DFT Using the Residue Fermat Number Systems and VLSI

T. K. Truong  
Communications Systems Research Section  
J. J. Chang  
Spacecraft Data Systems Section  
I. S. Hsu, D. Y. Pei, and I. S. Reed  
University of Southern California

In this paper, the integer complex multiplier and adder over the direct sum of two copies of a finite field is specialized to the direct sum of the rings of integers modulo Fermat numbers. Such multiplications and additions can be used in the implementation of a discrete Fourier transform (DFT) of a sequence of complex numbers. The advantage of the present approach is that the number of multiplications needed for the DFT can be reduced substantially over the previous approach. The architectural designs using this approach are regular, simple, expandable and, therefore, naturally suitable for VLSI implementation.

I. Introduction

Recently, the authors (Refs. 1, 2) developed a new method for computing a DFT using the direct sum of two copies of residue number systems. A principal advantage of this algorithm is that a complex integer multiplication can be computed by using similar integer multiplications in two parallel independent residue channels. Using the ideas of Cozzens and Finkelstein (Refs. 1, 2), it is shown in this article that a complex integer DFT can be computed by multiplication, modulo a Fermat number in two parallel independent residue channels. Such a multiplication over the direct sum of two copies of the rings of integers modulo Fermat numbers can be used in the implementation of a systolic array of the DFT as developed by Kung (Ref. 3).

II. Arithmetic Over the Direct Sum of Two Copies of Finite Rings Modulo A Fermat Number

Let \( F_n = 2^{2^n} + 1 \) be a Fermat number and let \( Z_{F_n} \) be the ring of residues of integers modulo \( F_n \). Further, let \((-1)\) denote the negative of integer one and let \( i \) denote the solution of equation \( x^2 = -1 \). Finally define the set \( Z_{F_n}[i] = \{ a + ib | a, b \in Z_{F_n} \} \) of \( F_n^2 \) elements in such a manner that addition is given by \((a + ib) + (c + id) = (a + b)_{F_n} + i(b + d)_{F_n} \) and multiplication is given by \((a + ib)(c + id) = (ac - bd)_{F_n} + i(bc + ad)_{F_n} \), where \((x)_{F_n} \) denotes the residue of a modulo \( F_n \). The set \( Z_{F_n}[i] \) is a commutative ring. (To show that \( Z_{F_n}[i] \) is a commutative ring, it is only necessary to show that any arbitrary three elements of \( Z_{F_n}[i] \) satisfies the postulates of ring [Ref. 4, p. 1].)

**Lemma 1:** Let \( F_n = 2^{2^n} + 1 \) be a Fermat number; where \( n \geq 1 \). The solutions of \( x^2 + 1 \equiv 0 \mod F_n \) are \( s = \pm 2^{2^n-1} \).

**Proof:** Since \( F_n = 2^{2^n} + 1 \), then \( 2^{2^n} \equiv -1 \mod 2^{2^n} + 1 \). Thus,

\[(\pm 2^{2^n-1})^2 \equiv -1 \mod 2^{2^n} + 1\]

Hence, \( s = \pm 2^{2^n-1} \) are the solutions of \( x^2 + 1 \equiv 0 \mod F_n \).
Next we map an element \( a + ib \) in \( \mathbb{Z}_{F^n} [i] \) into \( (a + sb)_{F^n} \). It is easy to show that such a mapping is a homomorphic mapping. It was shown (Ref. 5) that if \( s \) is one of solutions of \( x^2 + 1 \equiv 0 \) modulo \( F_n \), then the set \( \{ a + sb \mid a, b \in \mathbb{Z}_{F^n} \} \) is a field with \( F_n \) elements isomorphic to \( GF(F_n) \), where \( F_n \) is considered as a prime number. If one uses both solutions of \( x^2 + 1 \equiv 0 \mod F_n \), i.e., \( \pm s \) for mapping an element into \( (a, \bar{a}) \), where \( a = (a + sb)_{F^n} \) and \( \bar{a} = (a - sb)_{F^n} \), then it is shown in the next theorem that such a mapping is an isomorphic mapping and the set \( \{ a, \bar{a} \mid a, \bar{a} \in \mathbb{Z}_{F^n} \} \) is the direct sum of 2 copies of \( \mathbb{Z}_{F^n} \) of \( F_n^2 \) elements.

Hence, by an extension of the ideas given in Ref. 5, the following important theorem, a special case of Lemma 2.3 of Ref. 1, can be proved.

**Theorem 1**: Let \( \mathbb{Z}_{F^n} [i] = \{ a + ib \mid a, b \in \mathbb{Z}_{F^n} \} \) be the ring with respect to addition and multiplication modulo \( F_n \). Then the direct sum of 2 copies of \( \mathbb{Z}_{F^n} \), i.e.,

\[
S_{F^n} = \mathbb{Z}_{F^n} + \mathbb{Z}_{F^n} = \{ a, \bar{a} \mid a, \bar{a} \in \mathbb{Z}_{F^n} \}
\]

where \( (a, \bar{a}) + (\beta, \bar{\beta}) = (a + \beta, \bar{a} + \bar{\beta}) \) and \( (a, \bar{a}) \cdot (\beta, \bar{\beta}) = (a\beta, \bar{a}\bar{\beta}) \) is a ring of \( F_n^2 \) elements which is isomorphic to the ring \( \mathbb{Z}_{F^n} [i] \).

**Proof**: By Lemma 1, integers \( s = \pm 2^{n-1} \) are the solutions of \( x^2 + 1 \equiv 0 \mod F_n \) for \( n \geq 1 \). If \( a + ib \in \mathbb{Z}_{F^n} [i] \), then let \( \phi \) be the mapping

\[
\phi: a + ib \to ((a + sb)_{F^n}, (a - sb)_{F^n}) = (a, \bar{a})
\]  

where

\[
a = (a + sb)_{F^n}
\]

\[
\bar{a} = (a - sb)_{F^n}
\]

\[
s = \pm 2^{n-1}
\]

To show that \( \phi \) is an isomorphism, one must show that \( \phi \) is both one-to-one and onto and that \( \phi \) preserves addition and multiplication. To show that \( \phi \) is onto, one needs to demonstrate that given an arbitrary element, \( (a, \bar{a}) \in S_{F^n} \), there exists an element \( a + ib \in \mathbb{Z}_{F^n} [i] \) such that \( \phi(a + ib) = (a, \bar{a}) \) is an element of \( S_{F^n} \). Equation (1) implies that

\[
a + 2^{n-1} b \equiv a \mod F_n
\]  

(2a)

\[
a - 2^{n-1} b \equiv \bar{a} \mod F_n
\]  

(2b)

Summing Eqs. (2a) and (2b) yields

\[
2a \equiv \alpha + \bar{\alpha} \mod F_n
\]

Since \( (2, F_n) = 1 \), one can solve for \( a \), i.e.,

\[
a \equiv 2^{-1} (\alpha + \bar{\alpha}) \equiv -2^{n-1} (\alpha + \bar{\alpha}) \mod F_n
\]

Subtracting Eq. (2b) from Eq. (2a) yields

\[
2^{n-1} b \equiv \alpha - \bar{\alpha} \mod F_n
\]

Since \( (2^{n-1}, F_n) = 1 \), one can solve for \( b \), i.e.,

\[
b \equiv 2^{-2^{n-1} - 1} (\alpha - \bar{\alpha}) \equiv -2^{n-1} (\alpha - \bar{\alpha}) \mod F_n
\]

Hence, the solutions of the system of congruences given in Eqs. (2a) and (2b) are

\[
a \equiv -2^{n-1} (\alpha + \bar{\alpha}) \mod F_n
\]  

(3a)

\[
b \equiv -2^{n-1} (\alpha - \bar{\alpha}) \mod F_n
\]  

(3b)

Thus by Eqs. (3a) and (3b) it is seen that \( (\alpha, \bar{\alpha}) \in \mathbb{Z}_{F^n} \) is the image of \( a + ib \in \mathbb{Z}_{F^n} [i] \) under the mapping \( \phi \). This proves that \( \phi \) is an onto mapping.

In order to show that \( \phi \) is one-to-one, assume \( \phi(a + ib) = \phi(c + id) \). It follows from Eq. (1) that \( ((a + sb)_{F^n}, (a - sb)_{F^n}) = ((c + sd)_{F^n}, (c - sd)_{F^n}) \). This implies that

\[
a + sb \equiv c + sd \mod F_n
\]  

(4a)

\[
a - sb \equiv c - sd \mod F_n
\]  

(4b)

Summing Eqs. (4a) and (4b) yields \( 2a \equiv 2c \mod F_n \). But since \( (2, F_n) = 1 \), \( a \equiv c \mod F_n \). Subtracting Eqs. (4a) from Eq. (4b) yields \( 2ab = 2sd \mod F_n \). Thus, since \( (2, F_n) = 1, b \equiv d \mod F_n \). Hence \( a + ib = c + id \) and \( \phi \) is a one-to-one mapping.

To show that \( \phi \) preserves multiplication and addition, let \( a + ib \) and \( c + id \) be arbitrary elements in \( \mathbb{Z}_{F^n} [i] \). Then

\[
\phi((a + ib) + (c + id)) = \phi(((a + c) + s(b + d)) = \phi((a + c) + s(b + d))
\]

\[
= ((a + c) + s(b + d), (a + c)
\]

\[
- s(b + d))
\]
\[ \phi((a + ib) \cdot (c + id)) = \phi((ac - bd) + (bc + ad)) \]
\[ = ((ac - bd) + s(bc + ad), (ac - bd) - s(bc + ad)) \]
\[ = ((a + sb) \cdot (c + sd), (a - sb) \cdot (c - sd)) \]
\[ = (a + sb, a - sb) \cdot (c + sd, c - sd) \]
\[ = \phi(a + ib) \phi(c + id) \]

Hence, \( \mathbb{Z}_F[i] \) is isomorphic to the ring \( \mathbb{S}_F \) and the theorem is proved.

**Remark 1:** An inverse mapping \( \phi^{-1} \) which maps \( (\alpha, \bar{\alpha}) \in \mathbb{S}_F \) into \( \mathbb{Z}_F[i] \) is defined by

\[ \phi^{-1} : (\alpha, \bar{\alpha}) \rightarrow a + ib \]  
(5)

where \( a \) and \( b \) can be computed by Eq. (3).

It was shown (Ref. 6) that the multiplication by \( e \) powers of two modulo \( F_n \) is accomplished simply by a cyclic shift of \( e \) bits. Thus by Eq. (1) and Eq. (3), the arithmetic needed to compute the mapping \( \phi \) and its inverse \( \phi^{-1} \) requires only cyclic shifts and additions modulo \( F_n \). As a consequence, both mappings are easily implemented with VLSI technology. Also by Theorem 1, the operations needed to perform integer complex multiplication in \( \mathbb{Z}_F[i] \) only require two integer multiplications modulo \( F_n \). Such multiplications modulo \( F_n \) can be implemented by using a new VLSI design of a single chip developed in Ref. 7.

To perform multiplication and addition in \( \mathbb{Z}_F[i] \) or its equivalent \( \mathbb{S}_F \), one must determine an \( F_k \) such that the results of the computations lie in \( \mathbb{Z}_F[i] \). The format number \( F_k \) is sufficiently large for a good many applications. However, for some applications, larger dynamic range is required to keep the results of a computation within \( \mathbb{Z}_F[i] \). This constraint sometimes forces \( F_n \) to be too large to be convenient for computations by VLSI technology. To remedy this situation, using the ideas in Ref. 8, complex multiplications are extended in this section to a ring which is the direct sum of \( \mathbb{Z}_F[i] \), \( \mathbb{Z}_{F_k^1}[i] \), \ldots, and \( \mathbb{Z}_{F_k^r}[i] \), where for each \( j \), \( \mathbb{Z}_{F_k^j}[i] \) is represented by two copies of \( \mathbb{Z}_{F_k^j} \). To achieve this, the following theorems are needed.

**Chinese Remainder Theorem:** If \( m_1, m_2, \ldots, m_r \) are relatively prime in pairs, then the system of congruences, \( x \equiv c_n \mod m_n \) for \( 1 \leq n \leq r \) has a unique solution \( x \) given by

\[ x = \sum_{n=1}^{r} c_n M_n^{-1} \mod M \]  
(6a)

where \( M = m_1 m_2 \ldots m_r = m_1 M_1 = m_2 M_2 = \ldots = m_r M_r \) and \( M_n^{-1} \) uniquely satisfies \( (\mod m_n) \) the congruence

\[ M_n^{-1} \mod M_n = 1 \mod M_n \]  
(6b)

for \( 1 \leq n \leq r \). For a detailed proof, see Ref. 9.

Let \( M = F_k \cdot F_{k+1} \cdot \ldots \cdot F_r = (2^k + 1)(2^{k+1} + 1) \ldots (2^{r-1} + 1) = F_k M_r = F_{k+1} M_k = \ldots = F_r M_1 \), where \( 1 \leq k \leq r \) and \( M_n = \frac{M}{F_n} \). Since \( F_k, F_{k+1}, \ldots, F_r \) are pairwise relatively prime, by the Chinese remainder theorem, it is shown in Appendix A that the congruences

\[ x \equiv c_n \mod F_n \]  
for \( k \leq n \leq r \)  
(7a)

have a unique solution \( x \) given by

\[ x = \sum_{n=k}^{r} c_n M_n^{-1} \mod M = \sum_{n=k}^{r} c_n (M/F_n) M^{-1} \mod M \]  
(7b)

where

\[ M_k^{-1} = 2^{-(r-k)} - 2^{-(r-k) \mod r + k + 1} \]  
(7c)

and

\[ M_n^{-1} = M_k^{-1} 2^{-(r-n)} (2^k - 1) \]
\[ = 2^{(r-n) \mod (r-k+1)} (2^k - 1) \]  
for \( k \leq n \leq r \).

Here \( M_n^{-1} \) uniquely satisfies the congruence \( M_n M_n^{-1} = 1 \mod F_n \) for \( k \leq n \leq r \).

The number of additions and multiplications modulo \( F_n \) needed to compute Eq. (7b) are \( r - k \) and \( r - k + 1 \).

**Theorem 2:** Let \( M = F_k \cdot F_{k+1} \cdot \ldots \cdot F_r \) be the product of distinct Fermat numbers. Next let \( Z_M[i] = \{a + ib \mid a, b \in \mathbb{Z}_M\} \) where \( Z_M \) is a set of residues, modulo \( M \). Then the direct sum of finite rings
\[ S_M \left[ i \right] = Z_{F_k} \left[ i \right] + Z_{F_{k+1}} \left[ i \right] + \cdots + Z_{F_r} \left[ i \right] \]

where addition and multiplication are defined, respectively, by

\[
(\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) + (\beta_k, \beta_{k+1}, \ldots, \beta_r) = (\alpha_k + \beta_k, \alpha_{k+1} + \beta_{k+1}, \ldots, \alpha_r + \beta_r)
\]

and

\[
(\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \cdot (\beta_k, \beta_{k+1}, \ldots, \beta_r) = (\alpha_k \cdot \beta_k, \alpha_{k+1} \cdot \beta_{k+1}, \ldots, \alpha_r \cdot \beta_r)
\]

is a ring of \(M^2\) elements which is isomorphic to the ring \(Z_M \left[ i \right]\).

**Proof:** If \(a + ib \in Z_M \left[ i \right]\), then let \(\theta\) be the mapping

\[
\theta : (a + ib) \rightarrow \left( (a + ib) \right)' \left( a + ib \right)' \left( a + ib \right)' \left( a + ib \right)'
\]

\[
= (a_k + ib_k, a_{k+1} + ib_{k+1}, \ldots, a_r + ib_r)
\]

\[
= (a_k, a_{k+1}, \ldots, a_r)
\]

where \(a_k = (a + ib) = aF_n + ibF_n\) for \(k \leq n \leq r\).

It is easy to show that \(\theta\) preserves addition and multiplication. To show that \(\theta\) is onto and one-to-one, it suffices to show that given an arbitrary element \((\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \in S_M \left[ i \right]\), there exists an unique element \(a + ib \in Z_{F_k} \left[ i \right]\) such that \(\phi(a + ib) = (\alpha_k, \alpha_{k+1}, \ldots, \alpha_r)\). Equation (8) implies that

\[
a \equiv aF_n \mod F_n
\]

and

\[
b \equiv bF_n \mod F_n
\]

for \(k \leq n \leq r\). By Eq. (7), the unique solution of the systems of congruences in Eqs. (9a) and (9b), are

\[
a \equiv aF_k \left( M/F_k \right) \cdot 2^{(n-k) \mod 2^{k+1}} + \sum_{n=k+1}^{r} aF_n \left( M/F_n \right) \times 2^{(n-(n+1)) \mod 2^{n+1}} \left( 2^k - 1 \right)
\]

and

\[
b \equiv bF_k \left( M/F_k \right) \cdot 2^{(n-k) \mod 2^{k+1}} + \sum_{n=k+1}^{r} bF_n \left( M/F_n \right) \times 2^{(n-(n+1)) \mod 2^{n+1}} \left( 2^k - 1 \right)
\]

It follows that each element \((a_k, a_{k+1}, a_{k+1}, \ldots, a_r + ib_{k+1}, ib_{k+1}, \ldots, a_r + ib_r)\) of \(S_M\) is the image of a unique element \(a + ib \in Z_M \left[ i \right]\). This proves that \(\theta\) is one-to-one and onto and hence an isomorphic mapping of \(Z_M \left[ i \right]\) onto \(S_M \left[ i \right]\).

**Remark 2:** An inverse mapping \(\theta^{-1}\) which maps \((\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \in S_M\) into \(a + ib \in Z_M \left[ i \right]\) is defined by

\[
\theta^{-1} : (\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \rightarrow a + ib
\]

where \(a\) and \(b\) can be computed by Eqs. (9c).

**Theorem 3:** Let \(M = F_k \cdot F_{k+1} \cdots F_r\), where \((F_p, F_r) = 1\). Next let \(Z_{M \left[ i \right]} = \{a + ib \mid a, b \in Z_M\}\) be the ring in Theorem 2. Then the direct sum of \(Z_{F_k \left[ i \right]}\), \(Z_{F_{k+1} \left[ i \right]}\), \ldots, and \(Z_{F_r \left[ i \right]}\), where for each \(j, Z_{F_j} \left[ i \right]\) is represented by two copies of \(Z_{F_k \left[ i \right]}\), is

\[
S_M = \left( Z_{F_k} + Z_{F_k} \right) + \left( Z_{F_{k+1}} + Z_{F_{k+1}} \right) + \ldots + \left( Z_{F_r} + Z_{F_r} \right)
\]

where addition and multiplication are defined, respectively, by

\[
((\alpha_k, \alpha_{k+1}, \alpha_{k+1}, \ldots, \alpha_r, \alpha_{k+1}))
\]

\[
+ ((\beta_k, \beta_{k+1}, \beta_{k+1}, \ldots, \beta_r, \beta_{k+1}))
\]

\[
= ((\alpha_k + \beta_k, \alpha_{k+1} + \beta_{k+1}, \ldots, \alpha_r + \beta_r))
\]

\[
= ((\alpha_k, \alpha_{k+1}, \alpha_{k+1}, \ldots, \alpha_r + \beta_r))
\]

\[
+ ((\beta_k, \beta_{k+1}, \beta_{k+1}, \ldots, \beta_r, \beta_{k+1}))
\]

\[
= ((\alpha_k + \beta_k, \alpha_{k+1} + \beta_{k+1}, \ldots, \alpha_r + \beta_r))
\]

\[
+ ((\beta_k, \beta_{k+1}, \beta_{k+1}, \ldots, \beta_r, \beta_{k+1}))
\]

\[
= ((\alpha_k, \alpha_{k+1}, \alpha_{k+1}, \ldots, \alpha_r + \beta_r))
\]

\[
+ ((\beta_k, \beta_{k+1}, \beta_{k+1}, \ldots, \beta_r, \beta_{k+1}))
\]

\[
= ((\alpha_k + \beta_k, \alpha_{k+1} + \beta_{k+1}, \ldots, \alpha_r + \beta_r))
\]

is a ring of \(M^2\) element which is isomorphic to the ring \(Z_M \left[ i \right]\).
Proof: Let \( \widehat{\theta} = \phi \cdot \theta \) be the composition of the mapping \( \phi \) given by Eq. (1) and \( \theta \) given in Eq. (8). If \( a + ib \in \mathbb{Z}_M[i] \), then \( \widehat{\theta} \) is

\[
\widehat{\theta}: a + ib \rightarrow (\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r) \tag{11a}
\]

where \( s_n = \pm 2^n \) are the solution of \( x^2 + 1 \equiv 0 \mod F_n \) and \( \overline{\alpha}_n = (a - s_n b)F_n + a = (a - s_n b)F_n \), for \( k < n < r \). Some \( \theta \) and \( \phi \) are isomorphic mapping of \( \mathbb{Z}_M[i] \) onto \( S_M[i] \) and an isomorphic mapping of \( S_F[i] \) onto \( S_F[i] \), respectively, it is evident that \( \widehat{\theta} \) is an isomorphic mapping of \( \mathbb{Z}_M[i] \) onto \( S_M[i] \). The arithmetic needed to perform the mapping \( \widehat{\theta} \) given in Eq. (11a) only requires cyclic shifts and addition modulo \( F_n \).

Remark 3: The inverse mapping of \( \widehat{\theta} \), i.e., \( \widehat{\theta}^{-1} = \theta^{-1} \cdot \phi^{-1} \) which maps an element in \( S_M[i] \) into an element in \( \mathbb{Z}_M[i] \) is

\[
\widehat{\theta}^{-1}: (\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r) \rightarrow a + ib \tag{11b}
\]

where Eq. (11b) can be computed by the two inverse mapping \( \phi^{-1} \) and \( \theta^{-1} \). In other words, Eq. (5) can be used first to convert an element \( (\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r) \) in \( S_M[i] \) into an element \( (aF_k + ibF_k, aF_{k+1} + ibF_{k+1}, \ldots, aF_r + ibF_r) \) in \( S_F[i] \). Next Eq. (9a) can be used to convert an element \( (aF_k + ibF_k, aF_{k+1} + ibF_{k+1}, \ldots, aF_r + ibF_r) \) into an element \( a + ib \in \mathbb{Z}_M[i] \).

In the following, some examples are given to illustrate how the above mappings can be used to efficiently perform complex multiplication.

Example 1: Compute \((3 + i2) \cdot (1 + i4) \mod 17\), where \( 3 + i2 \) and \( 1 + i4 \in \mathbb{Z}_{17}[i] \) by means of the direct sum of two copies of \( \mathbb{Z}_{17} \).

Consider now this operation in the image ring \( S_{F_2} \). The solution of \( x^2 + 1 \equiv 0 \mod F_2 \) are \( \pm 2^{2^n - 1} = \pm 2^4 = \pm 4 \). Thus, by the mapping \( \phi \) given in Eq. (1), one obtains

\[
(3 + i2) \cong (3 + 4 \times 2, 3 - 4 \times 2) = (11, -5) \tag{12}
\]

\( (1 + i4) \cong (1 + 4 \times 4, 1 - 4 \times 4) = (0, 2) \)

Multiplying two images given in Eq. (12) yields

\[(11, -5) \cdot (0, 2) = (0, 7)\]

The corresponding element \( a + ib \) of \( (0, 7) \) under the inverse mapping \( \phi^{-1} \) given in Eq. (3) is

\[a \equiv -2^3 (0 + 7) \equiv 8 \cdot 7 \mod 17 = -5\]

The final result is \(-5 + i14\) which is verified readily to be the correct answer.

Example 2: Compute \((4 + i5) \cdot (17 + i3) \mod M = F_1F_2 = 5 \cdot 17 = 85\), where \((4 + i5) \in \mathbb{Z}_{85}[i] \) and \((17 + i3) \in \mathbb{Z}_{85}[i] \) by means of the direct sum of \( \mathbb{Z}_5[i] \) and \( \mathbb{Z}_{17}[i] \), where \( \mathbb{Z}_5[i] \) and \( \mathbb{Z}_{17}[i] \) are represented by 2 copies of \( \mathbb{Z}_5 \) and \( \mathbb{Z}_{17} \), respectively.

From the mapping Eq. (11), one obtains

\[\begin{align*}
(4 + i5)_{85} & \cong (((4 + 2 \cdot 5)_5, (4 - 2 \cdot 5)_5), \\
((4 + 2^2 \cdot 5)_{17}, (4 - 2^2 \cdot 5)_{17})) \\
& \Rightarrow ((4, 4), (7, 1)_{17}) \tag{13}
\end{align*}\]

and

\[\begin{align*}
(17 + i3)_{85} & \cong (((17 + 2 \cdot 3)_5, (17 - 2 \cdot 3)_5), \\
((17 + 2^2 \cdot 3)_{17}, (17 - 2^2 \cdot 3)_{17})) \\
& \Rightarrow ((3, 1), (12, -12)_{17})
\end{align*}\]

where \( \pm 2 \) and \( \pm 2^2 \) are the solutions of \( x^2 + 1 \equiv 0 \mod 5 \) and the solutions of \( x^2 + 1 \equiv 0 \mod 17 \), respectively. Multiplying two images given in Eq. (13) yields

\[(4, 4), (7, 1)_{17} \cdot ((3, 1), (12, -12)_{17}) \Rightarrow ((2, -1), (-1, 5)_{17})\]

The corresponding elements \( a + ib \in \mathbb{Z}_5[i] \) and \((c + id) \in \mathbb{Z}_{17}[i] \) of \((2, -1)_{5}\) and \((-1, 5)_{17}\) under the first inverse mapping \( \phi^{-1} \), given in Eq. (5), are

\[\begin{align*}
(2, -1)_{5} & \cong ((-2) (2 - 1) + i (-1) (2 + 1)) = (-2 - i3)_{5} \\
(-1, 5)_{17} & \cong ((-2^3) (-1 + 5) + i (-2) (-1 - 5))_{17} = (-2 - i5)_{17}
\end{align*}\]

Thus \((2, -1), (-1, 5)_{17} \cong ((-2 - i3)_{5}, (2 - i5)_{17})\). Finally, the corresponding element \( a + ib \in \mathbb{Z}_{85}[i] \) of \((-2 - i3)_{5}, (2 - i5)_{17}\) under the second inverse mapping \( \theta^{-1} \) given in Eq. (10) is

\[\begin{align*}
a & \equiv (-2) \cdot 136 + 2 \cdot 120 \\
& \equiv (-272 + 240) \mod 85 = 53
\end{align*}\]
\[ b \equiv (-3) \cdot 136 + (-5) \cdot 120 \]
\[ \equiv (-408 - 600) \text{ mod } 85 = 12 \]

The final result is \( a + ib = 53 + i12 \) which is verified readily to be the correct answer.

### III. Discrete Fourier Transform Over \( \mathbb{Z}_M \) \([i]\)

In this section, a \( d \) point Fourier transform over ring \( \mathbb{Z}_M \) \([i]\) or its equivalent \( S_M \) is developed to compute the usual digital Fourier transform of complex numbers. It will not be necessary for the transform length to be a power of two. For the Fourier transform of complex integer numbers in \( \mathbb{Z}_M \) \([i]\), one needs to scale the powers of the \( d \)th root of unity from complex numbers to complex integers in \( \mathbb{Z}_M \) \([i]\). Then the components of the transforms over the ring \( \mathbb{Z}_M \) \([i]\) or its equivalent \( S_M \) are required to remain in the interval \(-(M - 1)/2\) to \((M - 1)/2\). These results can then be scaled back from the complex integers to the original complex numbers to give a DFT of complex numbers without round-off error. For example, to compute a \( d \) point DFT of integer complex numbers \( a_n = \alpha_n + i\beta_n \) with \(|\alpha_n|, |\beta_n| \ll A = 2^{k_1/2} \), i.e.,

\[
A_k = \sum_{n=0}^{d-1} a_n \omega^{n \cdot k} \\
= \sum_{n=0}^{d-1} (\alpha_n + i\beta_n) \cdot (\chi_{n,k} + i\psi_{n,k}), \quad 0 \leq k \leq d - 1
\]

where \( \omega = \exp (i2\pi/d) \) is a \( d \)th root of unity and \( \omega^{n \cdot k} = \chi_{n,k} + i\psi_{n,k} \).

The components of the truncated complex number \( \omega^{n \cdot k} \) are first converted to integers with the dynamic range \( B = 2^{k_2} \), i.e., \(-B \ll \chi_{n,k}, \psi_{n,k} \ll B\). Here \( \omega^{n \cdot k} = \chi_{n,k} + i\psi_{n,k} \) denotes the scaled original complex number \( \omega^{n \cdot k} \). Next, let the DFT of \( a_n \) using the scaled truncated sequence \( \omega^{n \cdot k} \) be denoted by \( \tilde{A}_k \). Thus, \( \tilde{A}_k \) is defined by

\[
\tilde{A}_k = \sum_{n=0}^{d-1} a_n \omega^{n \cdot k} \\
= \sum_{n=0}^{d-1} (\alpha_n \chi_{n,k} - \beta_n \psi_{n,k}) + i(\alpha_n \psi_{n,k} + \beta_n \chi_{n,k}) \\
= \tilde{\gamma}_k + i\tilde{\delta}_k
\]

where

\[
a_n = \alpha_n + i\beta_n \\
\omega^{n \cdot k} = \chi_{n,k} + i\psi_{n,k} \\
\tilde{\gamma}_k = \sum_{n=0}^{d-1} \alpha_n \chi_{n,k} - \beta_n \psi_{n,k} \\
\tilde{\delta}_k = \sum_{n=0}^{d-1} \alpha_n \psi_{n,k} + \beta_n \chi_{n,k}
\]

To compute Eq. (17), one requires the final DFT in Eq. (17) to lie in the same "dynamic range" as the complex integers \( a_n \) and \( \omega^{n \cdot k} \). That is,

\[
|\tilde{\gamma}_k| = \left| \sum_{n=0}^{d-1} (\alpha_n \chi_{n,k} - \beta_n \psi_{n,k}) \right| \\
\leq \sum_{n=0}^{d-1} (|\alpha_n| \cdot |\chi_{n,k}| + |\beta_n| \cdot |\psi_{n,k}|) \\
\leq (M - 1)/2 \quad (18)
\]

and

\[
|\tilde{\delta}_k| = \left| \sum_{n=0}^{d-1} (\alpha_n \psi_{n,k} + \beta_n \chi_{n,k}) \right| \\
\leq \sum_{n=0}^{d-1} (|\alpha_n| \cdot |\psi_{n,k}| + |\beta_n| \cdot |\chi_{n,k}|) \\
\leq (M - 1)/2
\]

To satisfy Eq. (18) for all complex integer valued sequences \( a_n \) and \( \omega^{n \cdot k} \) such that \(|\alpha_n|, |\beta_n| \ll A = 2^{k_1/4} \) and \(|\chi_{n,k}|, |\psi_{n,k}| \ll B = 2^{k_2/2} \), it is sufficient to set

\[
2dA \cdot B \ll (M - 1)/2 \quad (19)
\]

if \( A = B \), then

\[
A = \left[ \sqrt{\frac{m-1}{4d}} \right] \quad (20)
\]

where \([x]\) denotes the greatest integer less than \( x \). The transform \( \tilde{A}_k \) in Eq. (17) can be computed by using the direct sum.
of $Z_{F_1}[l]$, $Z_{F_{k+1}}[l]$, $\ldots$, and $Z_{F_r}[l]$, where $Z_{F_{k+1}}[l]$ is represented by two copies of $Z_{F_{k+1}}[l]$. Finally, the $A^{\prime}_k$'s are scaled back to the scale of original complex numbers by $B^{-1}$ for $1 \leq k \leq d - 1$. By Eq. (17), one observes that the powers of roots of unity always have a truncation error due to approximating the powers of roots of unity. Evidently, the only error made in this computation of $A^{\prime}_k$'s is this truncation error. The error analysis of the DFT caused by $\omega^m$ is illustrated in the following section.

**Example 3:** Compute a 4-point DFT of $a_n$ by means of the direct sum of two copies of $Z_{F_2}$, where $a_0 = a_1 = 1 + i$ and $a_2 = a_3 = 0$.

The 4-point DFT of complex number of $a_n$

$$A_k = \sum_{n=0}^{4-1} a_n \omega^{n \cdot k} = \gamma_k + i\delta_k$$ (21)

where $\omega = i$ is the 4th root of unity and $a_n = \alpha_n + i\beta_n$. Since $d = 4$, $F_2 = 17$, $|\alpha_n|, |\beta_n| \leq A = 2^4 - 1 = 1$, then by Eq. (19) the dynamic range constraint of the components of $\omega^{n \cdot k}$ is $B = 2^{2^2} = 2^4 (4 \cdot 4 \cdot 1) = 1$. Thus, in this example, $\omega^{n \cdot k} = \omega^{n \cdot k}$. This implies that $|\gamma_k| = |x_{n \cdot k}| \leq B$ and $|\delta_k| = |y_{n \cdot k}| \leq B$, where $\gamma_k = x_{n \cdot k} + j y_{n \cdot k}$ and $\omega^{n \cdot k} = x_{n \cdot k} + j y_{n \cdot k}$. That is, $\omega^0 = \omega^0 = 1$, $\omega^1 = \omega = i$, $\omega^2 = \omega^{-1} = \omega^3 = \omega^3 = -i$. Hence, the 4-point DFT of $a_n$ becomes

$$\hat{A}_k = \sum_{n=0}^{4-1} a_n \omega^{n \cdot k} \mod 17$$

$$= \gamma_k + i\delta_k$$ for $0 \leq k \leq 3$ (22)

The corresponding elements in $S_{17}$ of $a_0$ and $\omega^{n \cdot k}$ in $Z_{F_1}[l]$ under the mapping $\psi$ defined in Eq. (1) is

$$a_0 = 1 + i = (1 + 2^2 \cdot 1, 1 - 2^2 \cdot 1) = (5, -3)$$

where $2^2$ is the solution of $x^2 + 1 \equiv 0 \mod 17$. Similarly, one has $a_1 = 1 + i = (5, -3), a_2 = a_3 = 0 \equiv (0, 0), \omega^1 = 1 \equiv (1, 1), \omega^3 = -1 \equiv (-1, -1),$ and $\omega^3 = -i \equiv (-4, 4)$.

Then Eq. (22) over $S_{17}$ becomes

$$\hat{A}_k = (5, -3) \omega^0 + (5, -3) \omega^1 + (0, 0) \omega^2 + (0, 0) \omega^3$$

$$= (5, -3) \omega^0 + (5, -3) \omega^1$$ (23a)

For $k = 0, 1, 2, 3$, Eq. (23a) becomes

$$\hat{A}_0 = (5, -3) \omega^0 + (5, -3) \omega^0$$

$$= (5, -3) (1, 1) + (5, -3) (1, 1)$$

$$= (5, -3) + (5, -3) = (10, 6)$$

$$\hat{A}_1 = (5, -3) \omega^1 + (5, -3) \omega^2$$

$$= (5, -3) (1, 1) + (5, -3) (4, -4)$$

$$= (5, -3) + (3, 12) = (8, 9)$$

$$\hat{A}_2$$

$$= (0, 0)$$

$$\hat{A}_3 = (5, -3) \omega^3 + (5, -3) \omega^3$$

$$= (5, -3) + (-3, 5) = (2, 2)$$

Taking the inverse mapping $\psi$ defined in Eq. (5) yields

$$\hat{A}_0 = (10, -6)$$

$$= (-2^2 \cdot 10 + 6) = (16)$$

$$\hat{A}_1 = (8, 9)$$

$$\hat{A}_2 = ((-8) (4) + (-2) (16)) = (-32 - 32) = 2i$$

$$\hat{A}_3 = ((-8) (8) + (-2) (-9)) = 2i$$

Similarly, one has $\hat{A}_2 = (0, 0) = 0$ and $\hat{A}_3 = (2, 2) = 2$.

**Example 4:** Compute a 4-point DFT of $a_n$ by means of the direct sum of $Z_{F_1}[l]$ and $Z_{F_2}[l]$, where $Z_{F_1}[l]$ and $Z_{F_2}[l]$ are represented by two copies of $Z_{F_1}$ and $Z_{F_2}$, respectively. Let the input values be $a_0 = a_1 = 1 + i$ and $a_2 = a_3 = 0$ where $a_n = a_n + i\beta_n \in Z_{F_1}[l]$ for $M = F_1 \cdot F_2$.

Since $d = 4, M = 85$ and $|\alpha_n|, |\beta_n| \leq A = 2^{4} - 1 = 1$, then by Eq. (19), the dynamic range constraint of the components of $\omega^{n \cdot k}$ is $B = 2^{2^2} = 85 (4 \cdot 4 \cdot 1) \equiv 2^2$.

In this example, $|\alpha_n|, |\beta_n| \leq B = 2^2$, where $\omega^{n \cdot k} = x_{n \cdot k} + j y_{n \cdot k}$. Thus $\omega^{n \cdot k} = \omega^{n \cdot k}$. That is, $\omega^0 = \omega^0 = \omega^1 = \omega = i$, $\omega^3 = \omega^3 = -i$ and $\omega^3 = \omega^3 = 1$. Hence, a 4-point transform DFT of $a_n$ due to the scaled truncated sequence $\omega^{n \cdot k}$ is
\[ \tilde{A}_k = \sum_{n=0}^{4-k} a_n \tilde{\omega}^{n+k} \mod 85 \]
\[ = \tilde{\gamma}_k + i\tilde{\delta} \quad \text{for } 0 \leq k \leq 3 \quad (23c) \]

Taking the mapping \( \tilde{\theta} \) defined in Eq. (11) yields
\[ a_0 = a_1 = (1 + i) \]
\[ \approx ((1 + 2 \cdot 1, 1, 1 - 2 \cdot 1)_{\tilde{\omega}}, (1 + 2^2 \cdot 1, 1, 1 - 2^2 \cdot 1)_{17}) \]
\[ \approx ((3, -1), (5, -3)_{17}) \]

where 2 and 4 are the solutions of \( x^2 + 1 \equiv 0 \mod 5 \) and \( 17 \), respectively. Similarly, one has \( a_2 = a_3 = 0 \approx ((0, 0), (0, 0), (0, 0), (0, 0)_{17}) \).
\[ \tilde{\gamma}_0 = 1 \approx ((1, 1)_{\tilde{\omega}}, (1, 1)_{17}), \tilde{\gamma}_1 = i \approx ((2, -2), (4, -4)_{17}), \tilde{\gamma}_2 = -1 \approx ((-1, 1), (-1, 1)_{17}), \text{ and } \tilde{\gamma}_3 = -i \approx ((-2, 2), (4, 4)_{17}). \]

Thus, Eq. (23c) in \( S_{85} \) becomes
\[ \tilde{A}_k = ((3, -1), (5, -3)_{17}) \tilde{\omega}^0 \]
\[ + ((0, 0), (0, 0)_{17}) \tilde{\omega}^{2k} \]
\[ + ((0, 0), (0, 0)_{17}) \tilde{\omega}^{4k} \]
\[ = ((3, -1), (5, -3)_{17}) \tilde{\omega}^0 \]
\[ + ((0, 0), (0, 0)_{17}) \tilde{\omega}^{2k} \]
\[ \approx ((3, -1), (5, -3)_{17}) \tilde{\omega}^k \quad (24a) \]

For \( k = 0, 1, 2, 3 \), Eq. (24a) becomes
\[ \tilde{A}_0 = ((3, -1), (5, -3)_{17}) \tilde{\omega}^0 + ((3, -1), (5, -3)_{17}) \tilde{\omega}^0 \]
\[ = ((3, -1), (5, -3)_{17}) \cdot ((1, 1), (1, 1)_{17}) \]
\[ + ((3, -1), (5, -3)_{17}) \cdot ((1, 1), (1, 1)_{17}) \]
\[ = ((-2, 2), (10, -6)_{17}) \quad (24b) \]

\[ \tilde{A}_1 = ((3, -1), (5, -3)_{17}) \tilde{\omega}^0 + ((3, -1), (5, -3)_{17}) \tilde{\omega}^1 \]
\[ = ((3, -1), (5, -3)_{17}) \cdot ((1, 1), (1, 1)_{17}) \]
\[ + ((3, -1), (5, -3)_{17}) \cdot ((2, -2), (4, -4)_{17}) \]
\[ = ((4, 1), (8, 5)_{17}) \]

For \( k = 0 \), the corresponding element \( \tilde{A}_0 = \tilde{\gamma}_0 + i\tilde{\delta}_0 \) of \( \tilde{A}_0 = ((1, -2), (10, -6)_{17}) \) under the second inverse mapping \( \tilde{\theta}^{-1} \) given in Eq. (10) is
\[ \tilde{\gamma}_0 \equiv 2 \cdot 17 \cdot 2^{6(2-1)} \mod 4 \cdot 2 \cdot 3 \]
\[ \times 2(2^2 - 2) \equiv 2 \cdot 17 \times 8 + 2 \cdot 5 \times 8 \times 3 \equiv 2 \mod 85 \]
\[ \equiv (-3) \cdot (17) \times 8 + (2) \cdot 5 \cdot 8 \cdot 3 \equiv 2 \mod 85 \]

Thus,
\[ \tilde{A}_0 = ((1, -2), (10, -6)_{17}) \equiv 2 + i2 \]
Using the same procedure for \( A_k \) for \( k = 1, 2, 3 \), one has finally \( A_1 = 2 + i2 \) and \( A_2 = A_3 = 0 \).

IV. Error Analysis of DFT Over \( S_M \)

In Eq. (17), let \( |a_n| \leq \sqrt{2} \cdot A = \sqrt{2} \cdot 2^{\lambda_1} \), where \( a_n = \alpha_n + 2^{\beta_n} \) such that \( |\alpha_n|, |2^{\beta_n}| \leq A = 2^{\lambda_1} \). In most digital signal processing applications, the input data \( a_n \) is an integer complex number, each component of \( a_n \) is represented, say, to at most 8 bit accuracy, i.e., \( |\alpha_n|, |\beta_n| \leq 2^{\lambda_1}, \) where \( 0 \leq \lambda_1 \leq 8 \). Also let

\[
\text{Re} \{\omega^{n \cdot k}\} = x_{n,k} = \frac{x_1}{2^1} + \frac{x_2}{2^2} + \cdots + \frac{x_{2^{\lambda_2}}}{2^{2^{\lambda_2}}} + \cdots
\]

\[
\text{Im} \{\omega^{n \cdot k}\} = y_{n,k} = \frac{y_1}{2^1} + \frac{y_2}{2^2} + \cdots + \frac{y_{2^{\lambda_2}}}{2^{2^{\lambda_2}}} + \cdots
\]

If one truncates both \( x_{n,k} \) and \( y_{n,k} \) by \( 2^{-\lambda_2} \) digits, then the truncated sequences for \( \omega^{n \cdot k} \) become

\[
\text{Re} \{\omega^{n \cdot k}\} = \tilde{x}_{n,k} = \frac{x_1}{2^1} + \frac{x_2}{2^2} + \cdots + \frac{x_{2^{\lambda_2}}}{2^{2^{\lambda_2}}}
\]

\[
\text{Im} \{\omega^{n \cdot k}\} = \tilde{y}_{n,k} = \frac{y_1}{2^1} + \frac{y_2}{2^2} + \cdots + \frac{y_{2^{\lambda_2}}}{2^{2^{\lambda_2}}}
\]

The error of \( A_k \) in Eq. (16) due to the truncated sequence \( \omega^{n \cdot k} \) is

\[
|A_k - \tilde{A}_k| = \left| \sum_{n=0}^{d-1} a_n (\omega^{n \cdot k} - \omega^{n \cdot k}) \right|
\]

\[
\leq \sum_{n=0}^{d-1} |a_n| \cdot |\omega^{n \cdot k} - \omega^{n \cdot k}| \leq |A_k| \leq 2^{\lambda_1} - \lambda_2
\]

But \( \text{Re} \{\omega^{n \cdot k} - \omega^{n \cdot k}\}, \text{Im} \{\omega^{n \cdot k} - \omega^{n \cdot k}\} \leq B^{-1} = 2^{-\lambda_2} \). Thus, \( |\omega^{n \cdot k} - \omega^{n \cdot k}| \leq \sqrt{2} \cdot 2^{-\lambda_2} \). Hence since \( |a_n| \leq \sqrt{2} \cdot 2^{\lambda_1} \), Eq. (25) becomes

\[
|A_k - \tilde{A}_k| \leq d \cdot \sqrt{2} \cdot 2^{\lambda_1} \cdot \sqrt{2} \cdot 2^{\lambda_2}
\]

\[
= d \cdot 2^{\lambda_1 + 1} \cdot 2^{\lambda_2}
\]

\[
= \varepsilon
\]

(26)

where \( \varepsilon \) is the desired error. Since \( |\alpha_n|, |\beta_n| \leq 2^{\lambda_1} \), then, from Eq. (19), the product of the dynamic range \( A = 2^{\lambda_1} \) and \( B = 2^{\lambda_2} \) is

\[
d^{2^{\lambda_1 + 1}} \cdot 2^{\lambda_2} \leq \frac{(M-1)}{2}
\]

(27a)

Thus,

\[
2^{\lambda_2} \leq \frac{(M-1)}{2^{\lambda_1 + 1} \cdot 2d}
\]

(27b)

The substitution of Eq. (27b) into Eq. (26) yields

\[
\varepsilon \leq \frac{(d \cdot 2^{\lambda_1 + 1})^2}{(M-1)/2}
\]

(28)

Example 5: Let \( M = F_k \cdot F_k = (2^{2^k + 1}) \cdot (2^{2^k} + 1) \) and \( d = 2^8 \) and \( \lambda_1 = 8 \). Then \( (d \cdot 2^{\lambda_1 + 1})^2 = (2^8 \cdot 2^9)^2 = 2^{30} \). By Eq. (19), the dynamic range of the components of \( \omega^{n \cdot k} \) is

\[
B = 2^{\lambda_2} \approx \frac{(2^{32} + 1)(2^{16} + 1)}{2^9 \cdot 2^7} \approx 2^{32}
\]

where \( \lambda_2 = 31 \). By Eq. (28), the desired error of \( A_k \) due to the scaled truncated sequence \( \omega^{n \cdot k} \) by \( 2^{-\lambda_2} = 2^{32} \) is

\[
\varepsilon \approx \frac{2^{30}}{(2^{32} + 1)(2^{16} + 1) - 1}/2 \approx \frac{2^{30}}{2^{47}} \approx 2^{-17}
\]

V. A VLSI Design for Computing the DFT Over \( S_M \)

In this section, a VLSI architecture is developed for computing the \( d \)-point DFT over the direct sum of \( Z_{F_k^j}^d \) using two copies of the finite ring \( Z_{F_k^j} \) for all \( j \). This VLSI processor for computing Eq. (17) is composed of \( d \) basic cells. Each basic cell performs a sum and product operation over \( S_M \), where \( M = F_k \cdot F_k \cdot \ldots \cdot F_r \). That is,

\[
(a_1, a_2, \ldots, a_d) \leftarrow (a_1, a_2, \ldots, a_d) + (b_1, b_2, \ldots, b_d) \cdot (c_1, c_2, \ldots, c_d)
\]
where "×" denotes the operation "is replaced by." The VLSI architecture of the DFT, using the Fermat residue number system with computations in $\mathbb{Z}_M[i]$ is illustrated in the following two simple examples.

The calculations of the first example were illustrated in example 3 in Section IV. A VLSI architecture structure for computing a 4-point DFT over $\mathbb{Z}_{85}[i]$ for this example is shown in Fig. 1. This figure contains 4 basic cells. The function of each basic cell is

$$(u, \overline{a}) \rightarrow (u, \overline{a}) + (b, \overline{b}) (c, \overline{c}) = ((a + b \cdot c)_1, \overline{(a + b \cdot c)}_1)_1$$  \hspace{1cm} (29)$$

Equation (29) is computed by using the direct sum of two copies of $\mathbb{Z}_{17}$. The $\omega^{n \cdot \cdot n \cdot \cdot k}$ is first scaled by $B = 2^5$. In this example, $\omega^{n \cdot \cdot n \cdot \cdot k} = \omega^{n \cdot \cdot n \cdot \cdot k}$. First the integer complex number sequence $a_i$ under the mapping $\phi$ is converted from $\mathbb{Z}_{85}[i]$ into $(a_i, \overline{a}_i) \in S_{17}$ for $1 \leq i \leq 4$ and are sent to all of the cells simultaneously. Each register in Fig. 1 is composed of two 5-bit subregisters $a$ and $\overline{a}$ of $(a, \overline{a}) \in S_{17}$. $(a, \overline{a})$ is stored in these two 5-bit subregisters.

Assume initially that all registers are set to zero. After the input data are entered completely, the components of $A_k$ in $S_{17}$ given by Eq. (23b) are contained in registers $B_k$ for $0 \leq k \leq 3$. The values computed in this manner are shifted sequentially out of register $R_k$. Next these values are converted by the inverse mapping $\phi^{-1}$ into $\tilde{A}_k = \tilde{a}_k + i\tilde{b}_k$ for $0 \leq k \leq 3$. Finally, these $\tilde{A}_k$ are scaled back to the scale of the original complex numbers $A_k$ by $B^{-1} = 1$ for $1 \leq k \leq 4$.

The second example in this section illustrates in example 4 for the application of theorem 3 to the VLSI design of a DFT. A structure for computing the 4-point DFT over $\mathbb{Z}_{85}[i]$ is shown in Fig. 2. In this figure, the function of each cell is

$$(a_1, \overline{a}_1)_5, (a_2, \overline{a}_2)_17) \rightarrow ((a_1, \overline{a}_1)_5, (a_2, \overline{a}_2)_17)$$

$$+ ((b_1, \overline{b}_1)_5, (b_2, \overline{b}_2)_17)$$

$$\times ((c_1, \overline{c}_1)_5, (c_2, \overline{c}_2)_17)$$

$$= ((a_1 + b_1 c_1, \overline{a}_1 + \overline{b}_1 c_1)_5, (a_2 + b_2 c_2, \overline{a}_2 + \overline{b}_2 c_2)_17)$$  \hspace{1cm} (30)$$

Equation (30) is computed by using the direct sum of two copies of $\mathbb{Z}_{5}$ and $\mathbb{Z}_{17}$. The $\omega^{n \cdot \cdot n \cdot \cdot k}$ is first scaled by $B = 2^5$. In this example $\omega^{n \cdot \cdot n \cdot \cdot k} = \omega^{n \cdot \cdot n \cdot \cdot k}$. The complex integer number sequence $a_i$ under the mapping $\tilde{\phi} = \phi \cdot \theta$ is converted from $\mathbb{Z}_{85}[i]$ to $((a_1, \overline{a}_1), (a_2, \overline{a}_2)) \in S_{2 \cdot \cdot 5} = S_5 + S_{17}$ and is transferred to all of the cells simultaneously. Each register in Fig. 2 is composed of four subregisters, where the first two are 3-bit subregisters and the last two are 5-bit subregisters. $(a_1, \overline{a}_1), (a_2, \overline{a}_2)$ are stored in two 3-bit and 5-bit subregisters, respectively. Assume initially that all registers are set to zero. After the input data is entered completely, the results given in Eq. (24b) are stored in register $R_k$ for $0 \leq k \leq 3$. The above results computed in this manner are shifted sequentially out of register $R_k$. Using inverse mapping $\tilde{\phi}^{-1}$ these values are converted then to $\tilde{A}_k = \tilde{a}_k + i\tilde{b}_k$ for $0 \leq k \leq 3$. Finally, these $\tilde{A}_k$ are scaled back to the scale of the original complex numbers $A_k$ by $B^{-1} = 1$ for $0 \leq k \leq 3$. 

References


Fig. 1. The systolic array to compute a 4-point DFT over the direct sum of two copies of $\mathbb{Z}_{17}$.

Fig. 2. The systolic array to compute a 4-point DFT over the direct sum of $\mathbb{Z}_6[i]$ and $\mathbb{Z}_{17}[i]$, where $\mathbb{Z}_6[i]$ and $\mathbb{Z}_{17}[i]$ are represented by two copies of $\mathbb{Z}_6$ and $\mathbb{Z}_{17}$, respectively.
Appendix A

To show that $M_{n}^{-1}$ in Eq. (7c) satisfies the congruence $M_{n} \cdot M_{n}^{-1} \equiv 1 \mod F_{n}$ for $k \leq n \leq r$, consider first the case for $n = k$.

Substituting $M_{k}^{-1}$ in Eq. (7c) into $M_{k} \cdot M_{k}^{-1}$ yields

$$M_{k} \cdot M_{k}^{-1} \equiv (2^{k+1} + 1) (2^{k+2} + 1) \ldots (2^{r} + 1) \cdot 2^{-(r-k)}$$

$$\equiv (2 \cdot 2 \ldots 2) \cdot 2^{-(r-k)}$$

$$\equiv 2^{r-k} \cdot 2^{-(r-k)} \equiv 1 \mod 2^{k} + 1$$

Next consider the case for $n = k + i + 1$, where $k + 1 \leq n \leq r$. Substituting $M_{n}^{-1}$ in (7c) into $M_{n} \cdot M_{n}^{-1}$ yields the following:

$$M_{n} \cdot M_{n}^{-1} \equiv (2^{k} + 1) (2^{k+1} + k) \ldots (2^{k+i} + k) \cdot (2^{k+i+2} + 1) \ldots (2^{r} + 1) \cdot (-2)^{-1}$$

$$\times 2^{-(r-(k+i+1))} \cdot (2^{k} - 1)$$

$$= [(2^{k} - 1) \cdot (2^{k} + 1) \ldots (2^{k+i+2} - 1)] \cdot (2^{k+i+2} + 1) \ldots (2^{r} + 1) \cdot (-2)^{-1}$$

$$\times 2^{-(r-(k+i+1))}$$

$$\equiv (2^{k+i+1} - 1) \cdot (2^{k+i+2} + 1) \ldots (2^{r} + 1) (-2)^{-1} \cdot 2^{-(r-(k+i+1))}$$

$$\equiv (-2) (2 \cdot 2 \ldots 2) (-2)^{-1} \cdot 2^{-(r-(k+i+1))}$$

$$\equiv (-2) 2^{-(r-(k+i+1))} (-2)^{-1} \cdot 2^{-(r-(k+i+1))}$$

$$\equiv 1 \mod 2^{k+i+1} \text{ for } k + 1 \leq n \leq r$$

where $n = k + i + 1$. 

30