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 $Z_{F_n}[i] = \{a + ib \mid a, b \in Z_{F_n}\}$ 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 $(a + ib)(c + id) \equiv (ac - bd)_{F_n} + i(bc + ad)_{F_n}$ 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 $x^2 + 1 \equiv 0 \bmod F_n$ are $s = \pm 2^{2^{n-1}}$

Proof: Since $F_n = 2^{2^n} + 1$, then $2^{2^n} \equiv -1 \bmod 2^{2^n} + 1$. Thus,

$$(\pm 2^{2^{n-1}})^2 \equiv -1 \bmod 2^{2^n} + 1$$

Hence, $s = \pm 2^{2^{n-1}}$ are the solutions of $x^2 + 1 \equiv 0 \bmod F_n$.

Next we map an element $a + ib$ in $Z_{F_n}[i]$ 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 $\{a + sb \mid a, b \in Z_{F_n}\}$ 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 $x^2 + 1 \equiv 0 \bmod F_n$, i.e., $\pm s$ for mapping an element into $(\alpha, \overline{\alpha})$, where $\alpha = (a + sb)_{F_n}$ and $\overline{\alpha} = (a - sb)_{F_n}$, then it is shown in the next theorem that such a mapping is an isomorphic mapping and the set $\{\alpha,\overline{\alpha} \mid \alpha,\overline{\alpha} \in Z_{F_n}\}$ is the direct sum of 2 copies of 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 $Z_{F_n}[i] = \{a + ib \mid a,b \in Z_{F_n}\}$ be the ring with respect to addition and multiplication modulo F_n. Then the direct sum of 2 copies of Z_{F_n}, i.e.,

$$S_{F_n} = Z_{F_n} + Z_{F_n} = \{\alpha,\overline{\alpha} \mid \alpha,\overline{\alpha} \in Z_{F_n}\}$$

where $(\alpha,\overline{\alpha}) + (\beta,\overline{\beta}) = (\alpha + \beta, \overline{\alpha} + \overline{\beta})$ and $(\alpha,\overline{\alpha}) \cdot (\beta,\overline{\beta}) = (\alpha\beta,\overline{\alpha}\overline{\beta})$ is a ring of F_n^2 elements which is isomorphic to the ring $Z_{F_n}[i]$.

Proof: By Lemma 1, integers $s = \pm 2^{2^{n-1}}$ are the solutions of $x^2 + 1 \equiv 0 \bmod F_n$ for $n \geq 1$. If $a + ib \in Z_{F_n}[i]$, then let ϕ be the mapping

$$\phi: a + ib \rightarrow ((a + sb)_{F_n}, (a - sb)_{F_n}) = (\alpha,\overline{\alpha}) \qquad (1)$$

where

$$\alpha = (a + sb)_{F_n}$$

$$\overline{\alpha} = (a - sb)_{F_n}$$

$$s = \pm 2^{2^{n-1}}$$

To show that ϕ is an isomorphism, one must show that ϕ is both one-to-one and onto and that ϕ preserves addition and multiplication. To show that ϕ is onto, one needs to demonstrate that given an arbitrary element, $(\alpha,\overline{\alpha}) \in S_{F_n}$, there exists an element $a + ib \in Z_{F_n}[i]$ such that $\phi(a + ib) = (\alpha,\overline{\alpha})$ is an element of S_{F_n}. Equation (1) implies that

$$a + 2^{2^{n-1}} b \equiv \alpha \bmod F_n \qquad (2a)$$

$$a - 2^{2^{n-1}} b \equiv \overline{\alpha} \bmod F_n \qquad (2b)$$

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

$$2a \equiv \alpha + \overline{\alpha} \bmod F_n$$

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

$$a \equiv 2^{-1} (\alpha + \overline{\alpha}) \equiv -2^{2^n-1} (\alpha + \overline{\alpha}) \bmod F_n$$

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

$$2^{2^{n-1}+1} b \equiv \alpha - \overline{\alpha} \bmod F_n$$

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

$$b \equiv 2^{-2^{n-1}-1} (\alpha - \overline{\alpha}) \equiv -2^{2^{n-1}-1} (\alpha - \overline{\alpha}) \bmod F_n$$

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

$$a \equiv -2^{2^n-1} (\alpha + \overline{\alpha}) \bmod F_n \qquad (3a)$$

$$b \equiv -2^{2^{n-1}-1} (\alpha - \overline{\alpha}) \bmod F_n \qquad (3b)$$

Thus by Eqs. (3a) and (3b) it is seen that $(\alpha,\overline{\alpha}) \in Z_{F_n}$ is the image of $a + ib \in Z_{F_n}[i]$ under the mapping ϕ. This proves that ϕ is an onto mapping.

In order to show that ϕ 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

$$a + sb \equiv c + sd \bmod F_n \qquad (4a)$$

$$a - sb \equiv c - sd \bmod F_n \qquad (4b)$$

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

To show that ϕ preserves multiplication and addition, let $a + ib$ and $c + id$ be arbitrary elements in $Z_{F_n}[i]$. Then

$$\begin{aligned} \phi((a + ib) + (c + id)) &= \phi((a + c) + i(b + d)) \\ &= ((a + c) + s(b + d), (a + c) \\ &\quad - s(b + d)) \end{aligned}$$

$$= (a + sb, a - sb) + (c + sd, c - sd)$$

$$= \phi(a + ib) + \phi(c - id)$$

and

$$\phi((a + ib) \cdot (c + id)) = \phi((ac - bd) + i(bc + ad))$$

$$= ((ac - bd) + s(bc + ad), (ac - bd) - s(bc + ad))$$

$$= ((a + sb) \cdot (c + sd), (a - sb) \cdot (c - sd))$$

$$= (a + sb, a - sb) \cdot (c + sd, c - sd)$$

$$= \phi(a + ib)\,\phi(c + id)$$

Hence, $Z_{F_n}[i]$ is isomorphic to the ring S_{F_n} and the theorem is proved.

Remark 1: An inverse mapping ϕ^{-1} which maps $(\alpha, \overline{\alpha}) \in S_{F_n}$ into $Z_{F_n}[i]$ is defined by

$$\phi^{-1}: (\alpha, \overline{\alpha}) \rightarrow a + ib \tag{5}$$

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 ϕ and its inverse ϕ^{-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 $Z_{F_n}[i]$ 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 $Z_{F_n}[i]$ or its equivalent S_{F_n}, one must determine an F_n such that the results of the computations lie in $Z_{F_n}[i]$. The fermat number F_5 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 $Z_{F_n}[i]$. 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 $Z_{F_k}[i]$, $Z_{F_{k+1}}[i]$, ..., and $Z_{F_r}[i]$, where for each j, $Z_{F_{k+j}}[i]$ is represented by two copies of $Z_{F_{k+j}}$. 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, $x \equiv c_n \bmod m_n$ for $1 \leqslant n \leqslant r$ has a unique solution x given by

$$x \equiv \sum_{n=1}^{r} c_n M_n M_n^{-1} \bmod M \tag{6a}$$

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

$$M_n M_n^{-1} \equiv 1 \bmod M_n \tag{6b}$$

for $1 \leqslant n \leqslant r$. For a detailed proof, see Ref. 9.

Let $M = F_k \cdot F_{k+1} \ldots F_r = (2^{2^k} + 1)(2^{2^{k+1}} + 1) \ldots (2^{2^r} + 1) = F_k M_k = F_{k+1} M_{k+1} = \ldots = F_r M_r$, where $1 \leqslant k \leqslant r$ and $M_n = M/F_n$. 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

$$x \equiv c_n \bmod F_n \qquad \text{for } k \leqslant n \leqslant r \tag{7a}$$

have a unique solution x given by

$$x \equiv \sum_{n=k}^{r} c_n M_n M_n^{-1} \equiv \sum_{n=k}^{r} c_n (M/F_n) M_n^{-1} \bmod M \tag{7b}$$

where

$$M_k^{-1} = 2^{-(r-k)} = 2^{(-(r-k)) \bmod 2^{k+1}} \tag{7c}$$

and

$$M_n^{-1} = -2^{-1}\, 2^{-(r-n)} (2^{2^k} - 1)$$

$$= 2^{(2^n - (r-n+1)) \bmod 2^{n+1}} (2^{2^k} - 1) \qquad \text{for } k < n \leqslant r$$

Here M_n^{-1} uniquely satisfies the congruence $M_n M_n^{-1} \equiv 1 \bmod F_n$ for $k \leqslant n \leqslant r$.

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

Theorem 2: Let $M = F_k \cdot F_{k+1} \ldots F_r$ be the product of distinct Fermat numbers. Next let $Z_M[i] = \{a + ib \mid a, b \in Z_M\}$ where Z_M is a set of residues, modulo M. Then the direct sum of finite rings

$$S_M[i] = Z_{F_k}[i] + Z_{F_{k+1}}[i] + \cdots + Z_{F_r}[i]$$

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

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

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

is a ring of M^2 elements which is isomorphic to the ring $Z_M[i]$.

Proof: If $a + ib \in Z_M[i]$, then let θ be the mapping

$$\theta:(a+ib) \to ((a+ib)_{F_k}, (a+ib)_{F_{k+1}}, \ldots, (a+ib)_{F_r})$$

$$= (a_{F_k} + ib_{F_k}, a_{F_{k+1}} + ib_{F_{k+1}}, \ldots, a_{F_r} + ib_{F_r})$$

$$= (\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \tag{8}$$

where $\alpha_n = (a+ib)_{F_n} = a_{F_n} + ib_{F_n}$ for $k \leqslant n \leqslant r$.

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

$$a \equiv a_{F_n} \bmod F_n \tag{9a}$$

and

$$b = b_{F_n} \bmod F_n \tag{9b}$$

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

$$a \equiv a_{F_k} (M/F_k) \cdot 2^{(-(r-k)) \bmod 2^{k+1}} + \sum_{n=k+1}^{r} a_{F_n} (M/F_n)$$

$$\times 2^{(2^n - (r-n+1)) \bmod 2^{n+1}} (2^{2^k} - 1) \tag{9c}$$

and

$$b = b_{F_k} (M/F_k) \cdot 2^{(-(r-k)) \bmod 2^{k+1}} + \sum_{n=k+1}^{r} b_{F_n} (M/F_n)$$

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

It follows that each element $(a_{F_k} + ib_{F_k}, a_{F_{k+1}} + ib_{F_{k+1}}, \ldots, a_{F_r} + ib_{F_r})$ of S_M is the image of a unique element $a + ib$ of $Z_M[i]$. This proves that θ is one-to-one and onto and hence an isomorphic mapping of $Z_M[i]$ onto $S_M[i]$.

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

$$\theta^{-1}:(\alpha_k, \alpha_{k+1}, \ldots, \alpha_r) \to a + ib \tag{10}$$

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

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

$$S_M = (Z_{F_k} + Z_{F_k}) + (Z_{F_{k+1}} + Z_{F_{k+1}}) + \ldots + (Z_{F_r} + Z_{F_r})$$

$$= \{(\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots,$$

$$(\alpha_r, \overline{\alpha}_r) \mid (\alpha_n, \overline{\alpha}_n) \in (Z_{F_n} + Z_{F_n})\}$$

where addition and multiplication are defined, respectively, by

$$((\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r))$$

$$+ ((\beta_k, \overline{\beta}_k), (\beta_{k+1}, \overline{\beta}_k), \ldots, (\beta_r, \overline{\beta}_r))$$

$$= ((\alpha_k + \beta_k, \overline{\alpha}_k + \overline{\beta}_k), (\alpha_{k+1} + \beta_{k+1}, \overline{\alpha}_{k+1} + \overline{\beta}_{k+1}), \ldots,$$

$$(\alpha_r + \beta_r, \overline{\alpha}_r + \overline{\beta}_r))$$

and

$$((\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r))$$

$$\times ((\beta_k, \overline{\beta}_k), (\beta_{k+1}, \overline{\beta}_{k+1}), \ldots, (\beta_r, \overline{\beta}_r))$$

$$= ((\alpha_k \cdot \beta_k, \overline{\alpha}_k \cdot \overline{\beta}_k), (\alpha_{k+1} \cdot \beta_{k+1}, \overline{\alpha}_{k+1} \cdot \overline{\beta}_{k+1}), \ldots,$$

$$(\alpha_r \cdot \beta_r, \overline{\alpha}_r \cdot \overline{\beta}_r))$$

is a ring of M^2 element which is isomorphic to the ring $Z_M[i]$.

Proof: Let $\hat{\theta} = \phi \cdot \theta$ be the composition of the mapping ϕ given by Eq. (1) and θ given in Eq. (8). If $a + ib \in Z_M[i]$, then $\hat{\theta}$ is

$$\hat{\theta}: a + ib \rightarrow ((\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r)) \quad (11a)$$

where $s_n = \pm 2^{2^{n-1}}$ are the solution of $x^2 + 1 \equiv \bmod F_n$ and $\overline{\alpha}_n = (a + s_n b)_{F_n}$ and $\alpha = (a - s_n b)_{F_n}$, for $k \leq n \leq r$. Some θ and ϕ are an isomorphic mapping of $Z_M[i]$ onto $S_M[i]$ and an isomorphic mapping of $S_{F_n}[i]$ onto S_{F_n}, respectively, it is evident that $\hat{\theta}$ is an isomorphic mapping of $Z_M[i]$ onto S_M. The arithmetic needed to perform the mapping $\hat{\theta}$ given in Eq. (11a) only requires cyclic shifts and addition modulo F_n.

Remark 3: The inverse mapping of $\hat{\theta}$, i.e., $\hat{\theta}^{-1} = \theta^{-1} \cdot \theta^{-1}$ which maps an element in S_M into an element in $Z_M[i]$ is

$$\hat{\theta}^{-1}: ((\alpha_k, \overline{\alpha}_k), (\alpha_{k+1}, \overline{\alpha}_{k+1}), \ldots, (\alpha_r, \overline{\alpha}_r) \rightarrow a + ib \quad (11b)$$

where Eq. (11b) can be computed by the two inverse mapping ϕ^{-1} and θ^{-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 into an element $(a_{F_k} + ib_{F_k}, a_{F_{k+1}} + ib_{F_{k+1}}, \ldots, a_{F_r} + ib_{F_r})$ in $S_M[i]$. Next Eq. (9a) can be used to convert an element $(a_{F_k} + ib_{F_k}, a_{F_{k+1}} + ib_{F_{k+1}}, \ldots, a_{F_r} + ib_{F_r})$ into an element $a + ib \in Z_M[i]$.

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

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

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

$$\begin{aligned} (3 + i2) &\cong (3 + 4 \times 2, 3 - 4 \times 2) = (11, -5) \\ (1 + i4) &\cong (1 + 4 \times 4, 1 - 4 \times 4) = (0, 2) \end{aligned} \quad (12)$$

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 ϕ^{-1} given in Eq. (3) is

$$a \equiv -2^3 (0 + 7) \equiv -8 \cdot 7 \bmod 17 = -5$$

$$b \equiv -2 (0 - 7) \bmod 17 = 14$$

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

Example 2: Compute $(4 + i5) \cdot (17 + i3) \bmod M = F_1 F_2 = 5 \cdot 17 = 85$, where $(4 + i5)$ and $(17 + i3) \in Z_{85}[i]$ by means of the direct sum of $Z_5[i]$ and $Z_{17}[i]$, where $Z_5[i]$ and $Z_{17}[i]$ are represented by 2 copies of Z_5 and Z_{17}, respectively.

From the mapping Eq. (11), one obtains

$$\begin{aligned} (4 + i5)_{85} &\cong (((4 + 2 \cdot 5)_5, (4 - 2 \cdot 5)_5), \\ &\quad ((4 + 2^2 \cdot 5)_{17}, (4 - 2^2 \cdot 5)_{17})) \\ &= ((4, 4)_5, (7, 1)_{17}) \end{aligned} \quad (13)$$

and

$$\begin{aligned} (17 + i3)_{85} &\cong (((17 + 2 \cdot 3)_5, (17 - 2 \cdot 3)_5), \\ &\quad ((17 + 2^2 \cdot 3)_{17}, (17 - 2^2 \cdot 3)_{17}) \\ &= ((3, 1)_5, (12, -12)_{17}) \end{aligned}$$

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

$$\begin{aligned} &((4, 4)_5, (7, 1)_{17}) \cdot ((3, 1)_5, (12, -12)_{17}) \\ &= ((2, -1)_5, (-1, 5)_{17}) \end{aligned}$$

The corresponding elements $a + ib \in Z_5[i]$ and $(c + id) \in Z_{17}[i]$ of $(2, -1)_5$ and $(-1, 5)_{17}$ under the first inverse mapping ϕ^{-1}, given in Eq. (5), are

$$(2, -1)_5 \equiv ((-2)(2 - 1) + i(-1)(2 + 1)) = (-2 - i3)_5$$

and

$$(-1, 5)_{17} = ((-2^3)(-1 + 5) + i(-2)(-1 - 5))_{17} = (2 - i5)_{17}$$

Thus $((2, -1)_5, (-1, 5)_{17}) \cong ((-2 - i3)_5, (2 - i5)_{17})$. Finally, the corresponding element $a + ib \in Z_{85}[i]$ of $((-2 - i3)_5, (2 - i5)_{17})$ under the second inverse mapping θ^{-1} given in Eq. (10) is

$$\begin{aligned} a &\equiv (-2) \cdot 136 + 2 \cdot 120 \\ &\equiv (-272 + 240) \bmod 85 = 53 \end{aligned}$$

and

$$b \equiv (-3) \cdot 136 + (-5) \cdot 120$$

$$\equiv (-408 - 600) \bmod 85 = 12$$

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

III. Discrete Fourier Transform Over $Z_M[i]$

In this section, a d point Fourier transform over ring $Z_M[i]$ 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 $Z_M[i]$, one needs to scale the powers of the dth root of unity from complex numbers to complex integers in $Z_M[i]$. Then the components of the transforms over the ring $Z_M[i]$ 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 $|\alpha_n|, |\beta_n| \leqslant A = 2^{\lambda 1}$, i.e.,

$$A_k = \sum_{n=0}^{d-1} a_n \omega^{n \cdot k}$$

$$= \sum_{n=0}^{d-1} (\alpha_n + i\beta_n) \cdot (x_{n,k} + iy_{n,k}), \qquad 0 \leqslant k \leqslant d-1 \tag{16}$$

where $\omega = \exp(i2\pi/d)$ is a dth root of unity and $\omega^{n \cdot k} = x_{n,k} + iy_{n,k}$.

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

$$\tilde{A}_k = \sum_{n=0}^{d-1} a_n \tilde{\omega}^{n \cdot k}$$

$$= \sum_{n=0}^{d-1} ((\alpha_n \tilde{x}_{n,k} - \beta_n \tilde{y}_{n,k}) + i(\alpha_n \tilde{y}_{n,k} + \beta_n \tilde{x}_{n,k}))$$

$$= \tilde{\gamma}_k + i\tilde{\delta}_k \tag{17}$$

where

$$a_n = \alpha_n + i\beta_n$$

$$\tilde{\omega}^{n \cdot k} = \tilde{x}_{n,k} + i\tilde{y}_{n,k}$$

$$\tilde{\gamma}_k = \sum_{n=0}^{d-1} \alpha_n \tilde{x}_{n,k} - \beta_n \tilde{y}_{n,k}$$

$$\tilde{\delta}_k = \sum_{b=0}^{d-1} \alpha_n \tilde{y}_{n,k} + \beta_n \tilde{x}_{n,k}$$

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 $\tilde{\omega}^{n \cdot k}$. That is,

$$|\tilde{\gamma}_k| = \left| \sum_{n=0}^{d-1} (\alpha_n \tilde{x}_{n,k} - \beta_n \tilde{y}_{n,k}) \right|$$

$$\leqslant \sum_{n=0}^{d-1} (|\alpha_n| \cdot |\tilde{x}_{n,k}| + |\beta_n| \, |\tilde{y}_{n,k}|)$$

$$\leqslant (M-1)/2 \tag{18}$$

and

$$|\tilde{\delta}_k| = \left| \sum_{n=0}^{d-1} (\alpha_n \tilde{y}_{n,k} + \beta_n \tilde{x}_{n,k}) \right|$$

$$\leqslant \sum_{n=0}^{d-1} (|\alpha_n| \, |\tilde{y}_{n,k}| + |\beta_n| \cdot |\tilde{x}_{n,k}|)$$

$$\leqslant (M-1)/2$$

To satisfy Eq. (18) for all complex integer valued sequences a_n and $\tilde{\omega}^{n \cdot k}$ such that $|\alpha_n|, |\beta_n| \leqslant A = 2^{\lambda 1}$ and $|x_{n,k}|, |y_{n,k}| \leqslant B = 2^{\lambda 2}$, it is sufficient to set

$$2dA \cdot B \leqslant (M-1)/2 \tag{19}$$

if $A = B$, then

$$A = \left[\sqrt{\frac{n-1}{4d}} \right] \tag{20}$$

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 $Z_{F_k}[i]$, $Z_{F_{k+1}}[i]$, ..., and $Z_{F_r}[i]$, where $Z_{F_{k+j}}[i]$ is represented by two copies of $Z_{F_{k+j}}$. Finally, the $\tilde{A}_k$'s are scaled back to the scale of original complex numbers by B^{-1} for $1 \leqslant k \leqslant d-1$. 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 $\tilde{A}_k$'s is this truncation error. The error analysis of the DFT caused by $\tilde{\omega}^{n\cdot k}$ 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

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

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

$$\begin{aligned} \tilde{A}_k &= \sum_{n=0}^{4-1} a_n \tilde{\omega}^{n\cdot k} \bmod 17 \\ &= \tilde{\gamma}_k + i\tilde{\delta}_k \qquad \text{for } 0 \leqslant k \leqslant 3 \end{aligned} \tag{22}$$

The corresponding elements in S_{17} of a_0 and $\tilde{\omega}^{n\cdot j}$ in $Z_{17}[i]$ under the mapping ϕ defined in Eq. (1) is

$$a_0 = 1 + i1 \cong (1 + 2^2 \cdot 1, 1 - 2^2 \cdot 1) = (5, -3)$$

where $\pm 2^2$ is the solution of $x^2 + 1 \equiv 0 \bmod 17$. Similarly, one has $a_1 = 1 + i1 = (5, -3)$, $a_2 = a_3 = 0 \cong (0, 0)$, $\tilde{\omega}^0 = 1 \cong (1, 1)$, $\tilde{\omega}^1 = 1 \cong (4, -4)$, $\tilde{\omega}^2 = -1 \cong (-1, -1)$, and $\tilde{\omega}^3 = -i \cong (-4, 4)$.

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

$$\begin{aligned} \tilde{A}_k &= (5, -3)\,\tilde{\omega}^0 + (5, -3)\,\tilde{\omega}^k + (0, 0)\,\tilde{\omega}^{2\cdot k} + (0, 0)\,\tilde{\omega}^{3\cdot k} \\ &= (5, -3)\,\tilde{\omega}^0 + (5, -3)\,\tilde{\omega}^k \end{aligned} \tag{23a}$$

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

$$\left.\begin{aligned} \tilde{A}_0 &= (5, -3)\,\tilde{\omega}^0 + (5, -3)\,\tilde{\omega}^0 \\ &= (5, -3)(1, 1) + (5, -3)(1, 1) \\ &= (5, -3) + (5, -3) = (10, 6) \\ \tilde{A}_1 &= (5, -3)\,\tilde{\omega}^0 + (5, -3)\,\tilde{\omega}^1 \\ &= (5, -3)(1, 1) + (5, -3)(4, -4) \\ &= (5, -3) + (3, 12) = (8, 9) \\ \tilde{A}_2 &= (0, 0) \\ \tilde{A}_3 &= (5, -3)\,\omega^0 + (5, -3)\,\omega^3 \\ &= (5, -3) + (-3, 5) = (2, 2) \end{aligned}\right\} \tag{23b}$$

Taking the inverse mapping ϕ^{-1} defined in Eq. (5) yields

$$\begin{aligned} \tilde{A}_0 &= (10, -6) \\ &\cong (-2^{2^2-1}(10 - 6) - i2^{2^{2-1}-1}(10 + 6)) \\ &= ((-8)(4) + i(-2)(16)) \\ &= (-32 - i32) = 2 + i2 \\ A_1 &= (8, 9) \\ &= ((-8)(8 + 9) + i(-2)(8 - 9)) = 2i \end{aligned}$$

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

Example 4: Compute a 4-point DFT of a_n by means of the direct sum of $Z_{F_1}[i]$ and $Z_{F_2}[i]$, where $Z_{F_1}[i]$ and $Z_{F_2}[i]$ are represented by two copies 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 $a_n = \alpha_n + i\beta_n \in Z_M[i]$ for $M = F_1 \cdot F_2$.

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

In this example, $|x_{n,k}|$, $|y_{n,k}| \leqslant B = 2^2$, where $\omega^{n\cdot k} = x_{n,k} + iy_{n,k}$. Thus $\tilde{\omega}^{n\cdot k} = \omega^{n\cdot k}$. That is, $\tilde{\omega} = \omega = i$, $\tilde{\omega}^2 = \omega^2 = -1$, $\tilde{\omega}^3 = \omega^3 = -i$ and $\tilde{\omega}^0 = \omega^0 = 1$. Hence, a 4-point transform DFT of a_n due to the scaled truncated sequence $\omega^{n\cdot k}$ is

$$\tilde{A}_k = \sum_{n=0}^{4-1} a_n \tilde{\omega}^{n \cdot k} \bmod 85$$

$$= \tilde{\gamma}_k + i\tilde{\delta} \quad \text{for } 0 \leqslant k \leqslant 3 \tag{23c}$$

Taking the mapping $\hat{\theta}$ defined in Eq. (11) yields

$$a_0 = a_1 = (1 + i)$$

$$\cong ((1 + 2 \cdot 1, 1 - 2 \cdot 1)_5, (1 + 2^2 \cdot 1, 1 - 2^2 \cdot 1)_{17})$$

$$\cong ((3, -1)_5, (5, -3)_{17})$$

where 2 and 4 are the solutions of $x^2 + 1 \equiv 0 \bmod 5$ and 17, respectively. Similarly, one has $a_2 = a_3 = 0 \cong ((0, 0)_5, (0, 0)_{17})$, $\tilde{\omega}^0 = 1 \cong ((1, 1)_5, (1, 1)_{17})$, $\tilde{\omega}^1 = i \cong ((2, -2)_5, (4, -4)_{17})$, $\tilde{\omega}^2 = -1 \cong ((-1, -1)_5, (-1, -1)_{17})$, and $\tilde{\omega}^3 = -i \cong ((-2, 2)_5, (-4, 4)_{17})$. Thus, Eq. (23c) in S_{85} becomes

$$\tilde{A}_k = ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0 + ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^k + ((0, 0)_5, (0, 0)_{17})\, \tilde{\omega}^{2k} + ((0, 0)_5, (0, 0)_{17})\, \tilde{\omega}^{3 \cdot k}$$

$$= ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0 + ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^k \tag{24a}$$

For $k = 0, 1, 2, 3$, Eq. (24a) becomes

$$\tilde{A}_0 = ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0 + ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0$$

$$= ((3, -1)_5, (5, -3)_{17}) \cdot ((1, 1)_5, (1, 1)_{17}) + ((3, -1)_5, (5, -3)_{17}) \cdot ((1, 1)_5, (1, 1)_{17})$$

$$= ((1, -2)_5, (10, -6)_{17}) \tag{24b}$$

$$\tilde{A}_1 = ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0 + (3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^1$$

$$= ((3, -1)_5, (5, -3)_{17}) \cdot ((1, 1)_5, (1, 1)_{17}) + ((3, -1)_5, (5, -3)_{17}) \cdot ((2, -2)_5, (4, -4)_{17})$$

$$= ((4, 1)_5, (8, 5)_{17})$$

$$\tilde{A}_2 = ((0, 0)_5, (0, 0)_{17})$$

$$\tilde{A}_3 = ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^0 + ((3, -1)_5, (5, -3)_{17})\, \tilde{\omega}^3$$

$$= ((2, 2)_5, (2, 2)_{17})$$

Taking the first inverse mapping ϕ^{-1} defined in Eq. (5) yields

$$\tilde{A}_0 = ((1, -2)_5, (10, -6)_{17})$$

$$= (((-2^{2-1})(1 - 2) + i(-2^{2^{1-1}-1})(1 + 2)), ((-2^{2^2-1})(10 - 6) + i(-2^{2^{2-1}-1})(10 + 6))$$

$$= ((-2)(-1) + i(-1)(3), (-8)(4) + i(-2)(-1))$$

$$= ((2 - i3)_5, (2 + i2)_{17})$$

$$\tilde{A}_1 = ((4, 1)_5, (8, 5)_{17})$$

$$\cong ((-2)(4 + 1) + i(-1)(4 - 1), (-8)(8 + 5) + i(-2)(8 - 5))$$

$$\cong ((0 + i2)_5, (-2 - 6i)_{17})$$

$$\tilde{A}_2 = ((0 + i0)_5, (0 + i0)_{17})$$

$$\tilde{A}_3 = ((2 + i0)_5, (2 + i0)_{17})$$

For $k = 0$, the corresponding element $\tilde{A}_0 = \tilde{\gamma}_0 + i\tilde{\delta}_0$ of $\tilde{A}_0 = ((1, -2)_5, (10, -6)_{17})$ under the second inverse mapping θ^{-1} given in Eq. (10) is

$$\tilde{\gamma}_0 \equiv 2 \times 17 \cdot 2^{(-(2-1)) \bmod 4} + 2 \cdot 3 \times 2^{(2^2-(2-2+1)) \bmod 2^3} (2^2 - 1)$$

$$\equiv 2 \times 17 \times 8 + 2 \cdot 5 \times 8 \cdot 3 = 2 \bmod 85$$

and

$$\tilde{\delta}_0 \equiv (-3)(17) \times 8 + (2) \cdot 5 \cdot 8 \cdot 3 \equiv 2 \bmod 85$$

Thus,

$$\tilde{A}_0 = ((1, -2)_5, (10, -6)_{17}) \cong 2 + i2$$

Using the same procedure for $\tilde{A}_k$ for $k = 1, 2, 3$, one has finally $\tilde{A}_1 = 2 + i2$ and $\tilde{A}_2 = \tilde{A}_3 = 0$.

IV. Error Analysis of DFT Over S_M

In Eq. (17), let $|a_n| \leqslant \sqrt{2} \cdot A = \sqrt{2} \cdot 2^{\lambda_1}$, where $a_n = \alpha_n + i\beta_n$ such that $|\alpha_n|, |\beta_n| \leqslant A = 2^{\lambda_1}$. 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., $|\alpha_n|, |\beta_n| \leqslant 2^{\lambda_1}$, where $0 \leqslant \lambda_1 \leqslant 8$. Also let

$$\mathrm{Re}\{\omega^{n \cdot k}\} = x_{n,k} = \frac{x_1}{2} + \frac{x_2}{2^2} + \cdots + \frac{x_{\lambda_2}}{2^{\lambda_2}} + \cdots$$

$$\mathrm{Im}\{\omega^{n \cdot k}\} = y_{n,k} = \frac{y_1}{2} + \frac{y_2}{2^2} + \cdots + \frac{y_{\lambda_2}}{2^{\lambda_2}} + \cdots$$

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

$$\mathrm{Re}\{\tilde{\omega}^{n \cdot k}\} = \tilde{x}_{n,k} = \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x_3}{2^3} + \cdots + \frac{x_{\lambda_2}}{2^{\lambda_2}}$$

$$\mathrm{Im}\{\tilde{\omega}^{n \cdot k}\} = \tilde{y}_{n,k} = \frac{y_1}{2} + \frac{y_2}{2^2} + \frac{y_3}{2^3} + \cdots + \frac{y_{\lambda_2}}{2^{\lambda_2}}$$

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

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

$$\leqslant \sum_{n=0}^{d-1} |a_n| \cdot |\omega^{n \cdot k} - \tilde{\omega}^{n \cdot k}| \qquad (25)$$

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

$$|A_k - \tilde{A}_k| \leqslant d \cdot \sqrt{2} \cdot 2^{\lambda_1} \cdot \sqrt{2} \cdot 2^{\lambda_2}$$

$$= d \cdot 2^{\lambda_1 + 1} \cdot 2^{-\lambda_2}$$

$$= \epsilon \qquad (26)$$

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

$$d 2^{\lambda_1 + 1} \cdot 2^{\lambda_2} \leqslant \frac{(M-1)}{2} \qquad (27a)$$

Thus,

$$2^{\lambda_2} \cong \frac{(M-1)}{2^{\lambda_1 + 1} \cdot 2d} \qquad (27b)$$

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

$$\epsilon \cong \frac{(d \cdot 2^{\lambda_1 + 1})^2}{(M-1)/2} \qquad (28)$$

Example 5: Let $M = F_5 \cdot F_4 = (2^{2^5+1}) \cdot (2^{2^4} + 1)$ and $d = 2^6$ and $\lambda_1 = 8$. Then $(d \cdot 2^{\lambda_1 + 1})^2 = (2^6 \cdot 2^9)^2 = 2^{30}$. By Eq. (19), the dynamic range of the components of $\tilde{\omega}^{n \cdot k}$ is

$$B = 2^{\lambda_2} \cong \frac{(2^{32} + 1)(2^{16} + 1)}{2^9 \cdot 2^7} \cong 2^{32}$$

where $\lambda_1 = 31$. 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

$$\epsilon \cong \frac{2^{30}}{((2^{32} + 1)(2^{16} + 1) - 1)/2} \cong \frac{2^{30}}{2^{47}} \cong 2^{-17}$$

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 $Z_{F_{k+j}}[i]$ 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 $M = F_k \cdot F_{k+1} \cdots F_r$. That is,

$$(a_1, a_2, \ldots, a_r) \leftarrow (a_1, a_2, \ldots, a_r)$$

$$+ (b_1, b_2, \ldots, b_r) \cdot (c_1, c_2, \ldots, c_r)$$

where "←" denotes the operation "is replaced by." The VLSI architecture of the DFT, using the Fermat residue number system with computations in $Z_M[i]$ 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 $Z_{17}[i]$ for this example is shown in Fig. 1. This figure contains 4 basic cells. The function of each basic cell is

$$(a, \overline{a}) \leftarrow (a, \overline{a}) + (b, \overline{b})\,(c, \overline{c})$$

$$= ((a + b \cdot c)_{17}, (\overline{a} + \overline{b} \cdot \overline{c})_{17}) \tag{29}$$

Equation (29) is computed by using the direct sum of two copies of Z_{17}. The $\omega^{n \cdot k}$ is first scaled by $B = 2^0$. In this example, $\tilde{\omega}^{n \cdot k} = \omega^{n \cdot k}$. First the integer complex number sequence a_n under the mapping ϕ are converted from $Z_{17}[i]$ into $(a_i, \overline{a}_i) \in S_{17}$ for $1 \leqslant i \leqslant 4$ and are sent to all of the cells simultaneously. Each register in Fig. 1 is composed of two 5-bit subregisters α and $\overline{\alpha}$ of $(\alpha, \overline{\alpha}) \in S_{17}$. $(\alpha, \overline{\alpha})$ 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 $0 \leqslant k \leqslant 3$. The values computed in this manner are shifted sequentially out of register R_0. Next these values are converted by the inverse mapping ϕ^{-1} into $\tilde{A}_k = \tilde{a}_k + i\tilde{b}_k$ for $0 \leqslant k \leqslant 3$. Finally, these $\tilde{A}_k$ are scaled back to the scale of the original complex numbers A_k by $B^{-1} = 1$ for $1 \leqslant k \leqslant 4$.

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 $Z_{85}[i]$ is shown in Fig. 2. In this figure, the function of each cell is

$$(a_1, \overline{a}_1)_5, (a_2, \overline{a}_2)_{17}) \leftarrow ((a_1, \overline{a}_1)_5, (a_2, \overline{a}_2)_{17})$$

$$+ ((b_1, \overline{b}_1)_5, (b_2, \overline{b}_2)_{17})$$

$$\times ((c_1, \overline{c}_1)_5, (c_2, \overline{c}_2)_{17})$$

$$= ((a_1 + b_1\, c_1, \overline{a}_1 + \overline{b}_1 \cdot \overline{c}_1)_5,$$

$$(a_2 + b_2 \cdot c_2, \overline{a}_2 + \overline{b}_2 \cdot \overline{c}_2)_{17} \tag{30}$$

Equation (30) is computed by using the direct sum of two copies of Z_5 and Z_{17}. The $\omega^{n \cdot k}$ is first scaled by $B = 2^0$. In this example $\tilde{\omega}^{n \cdot k} = \omega^{n \cdot k}$. The complex integer number sequence a_n under the mapping $\hat{\theta} = \phi \cdot \theta$ is converted from $Z_{85}[i]$ to $((a_{1,n}, \overline{a}_{1,n})_5, (a_{2,n}, \overline{a}_{2,n})_{17}) \in S_{85} = S_5 + S_{17}$ 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. $(a_{1,n}, \overline{a}_{1,n})_5$ and $(a_{2,n}\, \overline{a}_{2,n})_{17}$ 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 $0 \leqslant k \leqslant 3$. The above results computed in this manner are shifted sequentially out of register R_0. Using inverse mapping $\hat{\theta}^{-1}$ these values are converted then to $\tilde{A}_k = \tilde{\gamma}_k + i\tilde{\delta}_k$ for $0 \leqslant k \leqslant 3$. Finally, these $\tilde{A}_k$ are scaled back to the scale of the original complex numbers A_k by $B^{-1} = 1$ for $0 \leqslant k \leqslant 3$.

References

1. Cozzens, J. H. and Finkelstein, L. A., "Computing the Discrete Fourier Transform Using Residue Number Systems in a Ring of Algebraic Integers," to be published in *IEEE Information Theory*.

2. Despain, A. M., Peterson, A. M., Rothaus, O. S., and Wold, E. "Fast Fourier Transform Processors Using Complex Residue Arithmetic," to appear in the *Journal of Parallel and Distributed Processing*.

3. Mead, C. and Conway, L., *Introduction to VLSI Systems*, Addison-Wesley Publishing Company, California, 1980, Chapter 8.

4. McCoy, N. H., *Rings and Ideas*, George Banta Company, Inc., Wisconsin, 1948.

5. Reed, I. S. and Truong, T. K., "Convolutions over Residue Classes of Quadratic Integers," *IEEE Trans. on Information Theory*, Vol. IT-22, No. 4, pp. 468-475, July 1976.

6. Leibowitz, L. M., "A Simplified Binary Arithmetic for the Fermat Number Transform," *IEEE Trans. on Acoustics, Speech, and Signal Processing*, Vol. ASSP-24, No. 5, pp. 356-359, October 1976.

7. Chang, J. J., Truong, T. K., Reed, I. S., Hsu, I. S., and Shao, M. H., "VLSI Design of a Single Chip for the Multiplication of Integers Modulo a Fermat Number," *Proceedings ICASS 85*, IEEE International Conference on Acoustics, Speech, and Signal Processing. Vol. 3, March 26-29, 1985, pp. 1388-1391.

8. Reed, I. S. and Truong, T. K. "Complex Integer Convolution over a Direct Sum of Galois Fields," *IEEE Trans. on Information Theory*, Vol. IT-21, No. 1, pp. 657-661, November 1975.

9. Niven, I. and Zuchkerman, H. S., *An Introduction to the Theory of Numbers*, John Wiley and Sons, Inc., New York, 1966.

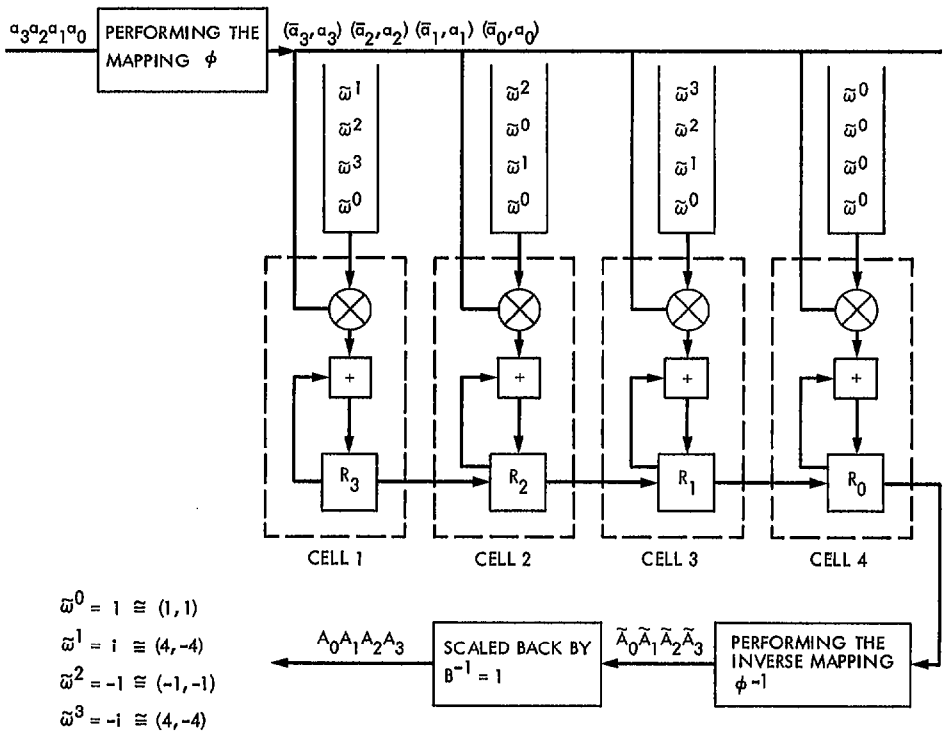

Fig. 1. The systolic array to compute a 4-point DFT over the direct sum of two copies of Z_{17}

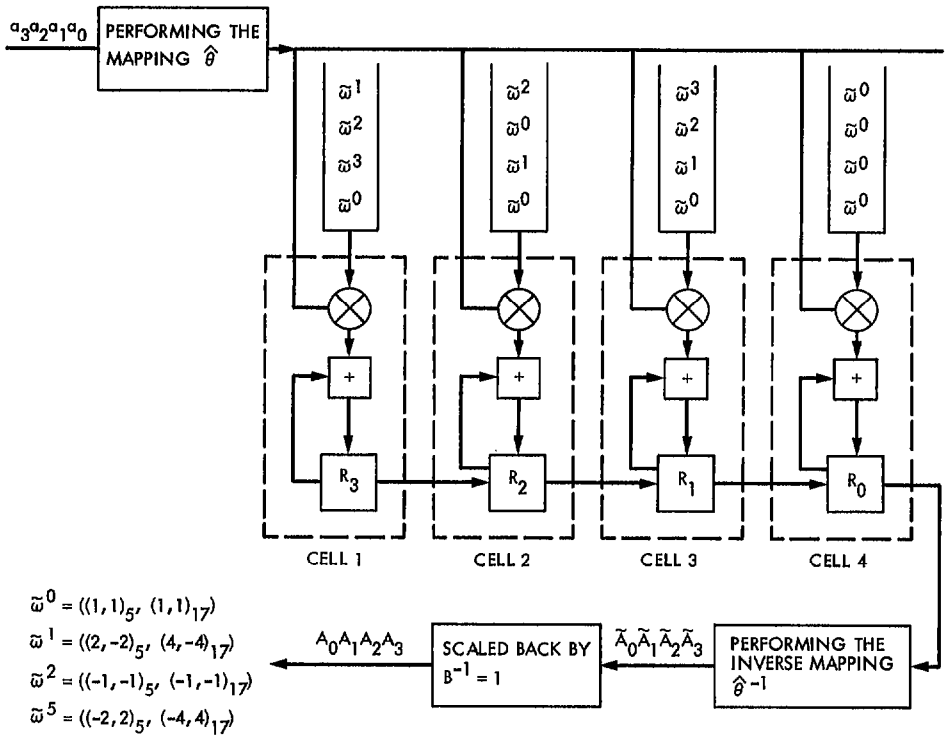

Fig. 2. The systolic array to compute a 4-point DFT over the direct sum of $Z_5[i]$ and $Z_{17}[i]$, where $Z_5[i]$ and $Z_{17}[i]$ are represented by two copies of Z_5 and Z_{17}, respectively

Appendix A

To show that M_n^{-1} in Eq. (7c) satisfies the congruence $M_n \cdot M_n^{-1} \equiv 1 \bmod F_n$ for $k \leqslant n \leqslant r$, consider first the case for $n = k$. Substituting M_k^{-1} in Eq. (7c) into $M_k \cdot M_k^{-1}$ yields

$$\begin{aligned} M_k \cdot M_k^{-1} &\equiv (2^{k+1}+1)(2^{2^{k+2}}+1)\ldots(2^{2^r}+1)\cdot 2^{-(r-k)} \\ &\equiv \underbrace{(2\cdot 2\ldots 2)}_{2^{r-k}}\cdot 2^{-(r-k)} \\ &\equiv 2^{r-k}\cdot 2^{-(r-k)} \equiv 1 \bmod 2^{2^k}+1 \end{aligned}$$

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

$$\begin{aligned} M_n \cdot M_n^{-1} &\equiv (2^{2^k}+1)(2^{2^{k+1}}+k)\ldots(2^{2^{k+i}}+1)\cdot(2^{2^{k+i+2}}+1)\ldots(2^{2^r}+1)\cdot(-2)^{-1} \\ &\quad \times 2^{-(r-k+i+1))}\cdot(2^{2^k}-1) \\ &\equiv [(2^{2^k}-1)\cdot(2^{2^k}+1)\ldots(2^{2^{k+i}}+1)]\,(2^{2^{k+i+2}}+1)\ldots(2^{2^2}+1)\cdot(-2)^{-1} \\ &\quad \times 2^{-(r-(k+i+1))} \\ &\equiv (2^{k+i+1}-1)\cdot(2^{2^{k+i+2}}+1)\ldots(2^{2^r}+1)(-2)^{-1}\cdot 2^{-(r-(k+i+1))} \\ &\equiv (-2)\underbrace{(2\cdot 2\ldots 2)}_{2^{(r-(k+i+1))}}(-2)^{-1}\cdot 2^{-(r-(k+i+1))} \\ &\equiv (-2)\,2^{(r-k+i+1))}\,(-2)^{-1}\cdot 2^{-(r-(k+i+1))} \\ &\equiv 1 \bmod 2^{2^{k+i+1}} \quad \text{for } k+1 \leqslant n \leqslant r \end{aligned}$$

where $n = k + i + 1$.