MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 151
JULY 1980, PAGES 757–765

Existence Theorems for Transforms Over Finite Rings With Applications to 2-D Convolution

By David P. Maher

Abstract. An existence theorem for Fourier-like transforms over arbitrary finite commutative rings is proven in a simple fashion. Corollaries for the case of residue class rings over the integers and extensions of those rings follow directly. The theory is applied to construct very fast algorithms for the computation of two-dimensional convolutions over the integers mod M.

1. Introduction. The number of applications of Fourier-like transforms in finite rings is rapidly increasing, mainly in the areas of fast digital convolution [1] and algebraic decoding algorithms [6], [11]. Pollard [15] described uses of transforms in finite fields as well as in Z_M, the ring of integers mod M. Coefficients of the Mattson-Solomon polynomial used in coding theory are finite field transforms [10]. Nicholson [12] considered theoretical and implementation questions for transforms in integral domains. Agarwal and Burrus [1] and several other authors [13], [16] have discussed signal processing applications of transforms over Z_M where M is a Mersenne or Fermat number. Applications in ring extensions of the form $Z_M[i]$ have been studied in [1], [17] in the case where M is square free and $i^2 + 1 = 0$. These last two restrictions were necessary only because the question of existence of Fourier-like transforms of a given length had not been solved for the case of an arbitrary algebraic extension of Z_M. We shall indicate below how transforms in higher degree extensions of Z_M are quite useful for fast computation of two-dimensional convolutions and we provide a succinct proof of an existence theorem for transforms over an arbitrary finite commutative ring with unit R. This theorem immediately implies a useful corollary for algebraic extensions of Z_M.

2. The General Problem. Let A be a finite abelian group and let R be a finite commutative ring with unit. We are interested in processing functions defined on A with images in R. In particular, we want to efficiently compute the convolution of two such functions:

$$f * g(a) = \sum_{b \in A} f(a - b)g(b). \tag{1}$$

Suppose that N is the exponent of A, that α is an Nth root of unity in R, and that N is invertible in R. Then for $f\colon A \longrightarrow R$ we define

$$Tf(a) = \sum_{b \in A} f(b)\alpha^{ab}, \tag{2}$$

Received August 14, 1978; revised July 5, 1979.
1980 *Mathematics Subject Classification.* Primary 12C99, 10–04.

0025-5718/80/0000-0105/$03.25

$$Sf(a) = N^{-1} \sum_{b \in A} f(b)\alpha^{-ab}. \tag{3}$$

We want to know when T can be thus defined and when S is an inverse for T. For then the convolution $f * g$ may be computed by transforming the pointwise product $Tf \cdot Tg$ by S. Since T has the same algebraic form as the DFT over the complex numbers, fast algorithms may be used to compute T and S. For many applications, the advantages of using a ring R other than $\mathbf{C}$, for processing discrete valued functions, are discussed in the references. They generally include the elimination of computation quantization noise as well as a reduction in the number of multiplications needed to complete a convolution computation.

Past approaches to the problem of proving the existence of transforms in a ring of given type have entailed the use of a rather detailed analysis of the multiplicative group of the ring. This is not difficult in the case of Z_M [1], but is more difficult in the case of extensions of Z_M [19], and even more so in the case of an arbitrary ring. Here we avoid this by considering the maximal ideals of the given ring.

THEOREM 1. *Let A be a finite abelian group with exponent N, let R be a finite commutative ring with unit, and let $\{M_1, M_2, \ldots, M_s\}$ be a list of all the maximal ideals of R. Let m_i be the number of elements in the quotient R/M_i. Then there exists a transform of the form* (2) *such that $T(f * g) = Tf \cdot Tg$, and such that S is an inverse for T, if and only if there exists an α in R which is of order divisible by N, mod M_i for all i. This is true if and only if N divides $m_i - 1$ for all i.*

Proof. First suppose A is the cyclic group Z_N.

Sufficiency. By the Chinese Remainder Theorem we have

$$R/\left(\bigcap_i M_i\right) \simeq \prod_i R/M_i. \tag{4}$$

Since each factor R/M_i is a finite field, the multiplicative group of each is cyclic of order $m_i - 1$, and since each of these orders is divisible by N, there is an element α_i of order N in each R/M_i. So by the isomorphism (4), there is at least one α in R such that α mod M_i is α_i for all i and this α is of order N. This is all we need for T to be defined and for $T(f * g)$ to be equal to $Tf \cdot Tg$, as can be verified by direct computation. To show that S is an inverse for T, we first note that if N were not invertible, it would be a zero divisor in R, and so if t is the additive order of N in R, i.e. $tN = 0$, then t is a zero divisor and is in some maximal ideal M_i. The additive order of t divides N which divides $m_i - 1$, but t must also divide m_i which is impossible, so N must be invertible. Now we write

$$ST(f)(n) = N^{-1} \sum_{k=0}^{N-1} \left(\sum_{j=0}^{N-1} f(j)\alpha^{jk} \right) \alpha^{-kn}$$

$$= N^{-1} \sum_{j=0}^{N-1} f(j) \sum_{k=0}^{N-1} \alpha^{k(j-n)},$$

so that S is an inverse for T, if

$$\sum_{k=0}^{N-1} \alpha^{kq} = \begin{cases} 0 & \text{for } 0 < q < N, \\ N & \text{for } q = 0. \end{cases}$$

The second case is clearly true, and we see that

$$\sum_{k=0}^{N-1} \alpha^{kq} = \sum_{k=0}^{N-1} \alpha^{(k+1)q},$$

so $(1 - \alpha^q)\Sigma_{k=0}^{N-1} \alpha^{kq} = 0$, and as long as $1 - \alpha^q$ is not a zero divisor for each $q \neq 0$, we have what we want. Suppose otherwise, then by the isomorphism (4), $\alpha_i^q - 1$ would be 0 in R/M_i, contradicting the assumption that α_i is of order N.

Necessity. If $N \nmid m_i - 1$ for some i, then for any $\alpha \in R$, we must have that α_i $(= \alpha \bmod M_i)$ is either 0 or is of some order rather than N, say L. But then $\Sigma_{k=0}^{N-1} \alpha_i^{qk} = N$ for $q = L$, and this completes the proof of the theorem for $A = Z_N$. For the general case, by the fundamental theorem of abelian groups, A may be viewed as a direct sum of cyclic groups, each of whose orders divides the exponent N. So the theorem is proven for each of the factors of A, hence for A itself.

When A is not cyclic, a transform is usually referred to as multidimensional, and when it is cyclic of order N, the transform is said to be of length N. An admissible value of α for the transform (2) will be called a *principal Nth root of unity* in R.

COROLLARY 1. *An invertible transform T of length N over Z_M of the form* (2) *exists if and only if N divides $p - 1$ for each prime p dividing M.*

Proof. This follows immediately, since a maximal ideal in Z_M is generated by a prime dividing M. A proof of this corollary was first indicated by Pollard [15], and later Agarwal and Burrus [1], [2] gave another proof, which has been subject to some criticism [7], [18] due to informality and to a nonstandard use of the term "order."

Corollary 1 may be used to find sequence lengths for which an invertible transform exists given the ring of values Z_M. If we have convenient values N and α in mind, we may want to know which values of M accommodate them. As explained in [1], we often want N to be highly divisible so that fast algorithms may be used, and we want multiplication by powers of α to be as fast as possible. We also want M to be large enough to allow computation of integral convolution without overflow, but small enough so that the computer word size required is small. So we indicate a method for finding all possible values for M given N and α by the following.

COROLLARY 2. *(M, N, α) are parameters for a Fourier-like transform for functions f: $Z_N \longrightarrow Z_M$ if and only if M divides $\alpha^N - 1$ but is prime to $\alpha^k - 1$ for all k less than N dividing N.*

Possible uses for transforms in extension rings include the simultaneous processing of more than one signal and a method for computation of multidimensional convolution. We explain the latter application. Two-dimensional cyclic convolution in a ring R is a special case of the general situation considered in Section 2, where A is a product

of two cyclic groups. Often, however, a two-dimensional convolution in R may be computed via a one-dimensional convolution in an extension of R by way of a technique developed by Nussbaumer and Quandalle [14] for applying polynomial transforms over the rationals. Here we reinterpret and extend some of their work.

Let f and g be functions defined on a group $Z_{qr} \times Z_q$ with images in a ring R. Then we may construct two functions

$$\bar{f}, \bar{g}\colon\ Z_{qr} \longrightarrow R[X]/(X^q - 1) \quad \text{by } \bar{f}(a) = \sum_{i \in Z_q} f(a, i)X^i.$$

One sees that the two-dimensional convolution of f and g may be obtained by one-dimensional convolution of $\bar{f}$ and $\bar{g}$ in $R[X]/(X^q - 1)$. But this latter convolution may in many cases be calculated by decomposing the polynomial ring into a product of algebraic extensions of R, then using transforms to compute the convolution in each factor, and finally using the Chinese Remainder Theorem to assemble the final result. The many advantages of this method are discussed in [14] in the case where R is the field of rational numbers. However, the method and its advantages apply to any commutative ring, as long as we have knowledge of the transforms which may be defined in extensions of those rings. Such knowledge may be obtained with the aid of Theorem 1 above and Corollary 3 below, as well as the discussions in [9]. In Section 3 we explain another approach to 2-D convolution, which in some cases is much more efficient than any other yet known.

The existence of invertible transforms in algebraic extensions of Z_M is determined by the following.

COROLLARY 3. *Suppose $Z_M[\zeta]$ is an algebraic extension of Z_M and that $Q(X)$ is the minimal polynomial of ζ over Z_M and that $\Pi_j Q_{ij}(X)^{l_j} = Q(X)$ mod p_i is a factorization of $Q(X)$ into irreducible polynomials* mod p_i *for each prime p_i dividing M. If n_{ij} is the degree of $Q_{ij}(X)$, then an invertible transform of length N of the form* (2) *exists in $Z_M[\zeta]$ if and only if there exists an α which is of order divisible by N in each local factor of $Z_M[\zeta]$* mod p_i *for all i. The latter is true if and only if N divides $p_i^{n_{ij}} - 1$ for all i, j.*

Proof. $Z_M[\zeta] \cong Z_M[X]/(Q(X))$ and Z_M is a direct sum of rings of the form $Z_p r$, where p^r is the highest power of p dividing M. Hence $Z_M[\zeta]$ is a direct sum of rings of the form $Z_p r[X]/(Q(X))$, where here $Q(X)$ is read mod p^r. A maximal ideal in $Z_p r(X)$ is generated by p together with a monic irreducible polynomial. We note that if a monic polynomial is irreducible mod p, it is irreducible mod p^r. Hence if $Q(X)$ splits into $\Pi_j Q_j(X)$ mod p, $Z_p r[X]/(Q(X))$ splits into a direct sum of local rings

$$\bigoplus_j Z_p r[X]/(Q_j(X)),$$

where each factor has a quotient field of p^{n_j} elements. Extending this argument to each p_i, the corollary now follows from Theorem 1.

3. Applications to 2-D Convolution. Here we explain applications of the forgoing to the fast computation of 2-D digital convolutions. Such convolutions are used in the filtering of 2-D signals in such areas as image processing, seismic data analysis, and control theory.

We want to filter a 2-D discrete quantized signal $x(i, j)$ by convolving it with the pulse response of the filter $h(i, j)$, producing an output signal $y(i, j)$. Suppose that the values of $x(i, j)$, $h(i, j)$, and $y(i, j)$ are limited to any of M quantization levels, and that the x and h arrays have dimension $k \times l$. Then the convolution,

$$y(i, j) = \sum_{m=0}^{l-1} \sum_{n=0}^{k-1} x(m, n)h(i - m, j - n), \tag{5}$$

may be computed entirely in the ring Z_M. Usually (5) is computed using complex discrete Fourier transform (DFT) methods. These methods are much faster than straightforward calculation, but they introduce truncation error which can be very troublesome. Our goal here is to produce algorithms which are often considerably faster than complex DFT methods, and which reduce or completely eliminate truncation error.

As is explained in [5], in order to perform the 2-D convolution (5) using DFT's it is necessary to extend the $k \times l$ arrays x and h to $K \times L$ arrays for $K = 2K - 1$, $L = 2l - 1$ by appending zeros. This is because transform methods compute cyclic convolutions. For example, the 1-D convolution of arrays $(a(0), \ldots, a(L - 1))$ and $(b(0), \ldots, b(L - 1))$ can be accomplished by computing the coefficients of the polynomial

$$c(W) = \left(\sum_{i=0}^{L-1} a(i)W^i \right) * \left(\sum_{i=0}^{L-1} b(i)W^i \right).$$

Cyclic convolution of length L computes the coefficients of the remainder of $c(W)/(W^L - 1)$. If we calculate the remainder of $c(W)/p(W)$ for some polynomial p of degree L other than $W^L - 1$, we shall call the result *quasicyclic convolution* of length L. We note that if $a_j = b_j = 0$ for all $j \geqslant (L + 1)/2$, then $c(W)$ equals the remainder of $c(W)/p(W)$ for any p of degree L, hence the results of the three types of convolution are the same. We use this observation in the 2-D case as follows: We suppose that $x(i, j)$ and $h(i, j)$ are two $K \times L$ arrays which have been extended from $k \times l$ arrays by appending zeros as suggested above. Map $x(i, j)$ and $h(i, j)$ into length K 1-D arrays of polynomials by

$$x(i, j) \longrightarrow X_i(W) = \sum_{j=0}^{L-1} x(i, j)W^j. \tag{6}$$

Each polynomial $X_i(W)$ and $H_i(W)$ is considered to be an element of degree less than L in the ring $R = Z_M[W]/p(W)$, where $p(W)$ is some polynomial of degree L. Now 2-D acyclic convolution of $x(i, j)$ and $h(i, j)$ can be accomplished by length K cyclic convolution of $X_i(W)$ and $H_i(W)$ in the ring R (the 2-D convolution which results may be quasicyclic in the horizontal direction). To accomplish this we must find Fourier-like transforms of length K in R. Our emphasis will be on transforms having fast algorithms, and which can be performed without multiplications.

Our 2-D convolution scheme is sketched in Figure 1. We let T denote a length K transform over R, as defined by (2), where A is the group Z_K. In this implementation, the transform of the 2-D pulse response of the filter is premultiplied by K^{-1} and stored in a ROM.

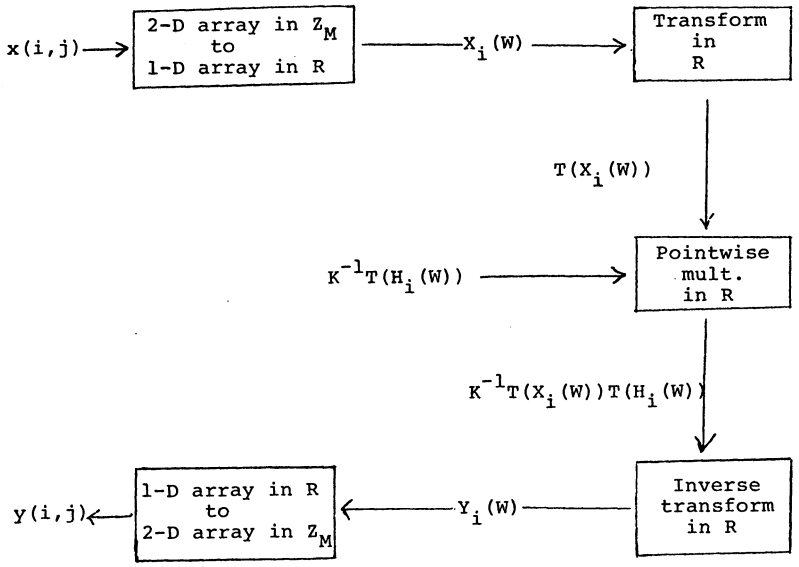

FIGURE 1

The $K \times L$ quasicyclic convolution algorithm

We need to develop fast methods for multiplication in R as well as for the calculation of T and T^{-1}. We must also show such transforms exist in nice cases. We make some assumptions here which we shall justify later. Suppose that we can take α equal to W in (2) so that W is a principal Kth root of unity in R. If we further suppose that K is a power of 2 and $p(W) = W^K + 1$, then a calculation of T requires no multiplications and $K \log_2 K$ additions in R if we use the FFT algorithm. Suppose now that a is a principal rth root of unity in Z_M, and that $K = rn$ and $L = rn/2$ for some power of 2, n. Then we have

$$R = Z_M[W]/(W^{nr/2} + 1) \overset{\Phi}{\simeq} \prod_{i=0}^{r/2-1} Z_M[W]/(W^n - a^{2i+1}), \tag{7}$$

where Φ is the chinese remainder isomorphism. That Φ exists follows from the fact that a is a principal rth root of 1 and from the proof of Theorem 1. Note that Φ has the form of an "incomplete" Fourier-like transform over R. It is incomplete in the sense that it is factoring $Z_M[W]$ mod $W^{nr/2} + 1$ instead of mod $W^{nr} - 1$, and because the $W^n - a^{2i+1}$ are not factored any further. Nevertheless we can use a partial FFT algorithm to compute Φ and Φ^{-1}—we just leave out the appropriate steps. If P and Q are two elements of R, then their product may be computed by

$$P * Q = \Phi^{-1}(\Phi(P) \cdot \Phi(Q)). \tag{8}$$

The multiplication on the right-hand side of (8) entails $r/2$ length n convolutions

mod $W^n - a^{2i+1}$. Let M_1 be the number of Z_M multiplications involved in one computation of Φ (or Φ^{-1}), and let M_2 be the number of Z_M multiplications involved in one length n convolution mod $W^n - a^{2i+1}$, then the total number of multiplications required per point for the entire algorithm of Figure 1 is

$$M = 4M_1/nr + M_2/n, \tag{9}$$

assuming that $\Phi(K^{-1}T(H_i(W))$ is precalculated.

The total number of Z_M additions for a complete calculation of T or T^{-1} is the same as that for $nr/2$ length nr FFTs, which is $(n^2r^2/2) \cdot \log_2 nr$, as 1 addition in R amounts to $nr/2$ additions in Z_M. Each application of Φ or Φ^{-1} uses a partial FFT of length $nr/2$ requiring $(nr/2)\log_2(nr/4)$ Z_M-additions. So if each length n convolution mod $W^n - a^{2i+1}$ requires A_2 additions, then the total number of Z_M additions per point is

$$A = 4 \log_2 nr + A_2/n - 4. \tag{10}$$

We now show examples where A_2, M_1, and M_2 are small and which justify the assumptions we made above. Here we let M be the tth Fermat number $2^{2^t} + 1 = F_t$. It has been observed several times [1], [2], [13] that Z_{F_t} supports transforms which are extremely nice from a computational point of view. We shall exploit that fact below. We also observe that arithmetic modulo a Fermat number can be done very quickly on many binary computers. See [2].

LEMMA. *Let r be the largest power of 2 dividing* GCD$\{p_i - 1$ st $p_i | F_t$, p_i *prime*$\}$. *Let a be a principal root of order r in Z_{F_t}, and set a* mod p_i *equal to $a_i^{e_i}$, where $e_i r$ is the largest power of 2 dividing $p_i - 1$, then W is of order ne_ir in $Z_{p_i}[W]/(W^n - a_n)$ for all i whenever n is a power of 2.*

Proof. By hypothesis, a_i has no square root mod p_i, and since -1 is a square mod p_i (p_i must have the form $k2^{t+2} + 1$, if p_i divides F_t and is prime), a_i cannot be -4 times a fourth power mod p_i. Therefore by [8, p. 221], $W^n - a^i$ is irreducible if n is a power of 2. Thus W is of order ne_ir mod $W^n - a^i$ for all i.

PROPOSITION. *Let a and r be as in the Lemma with n a power of 2, then there exists an invertible Fourier-like transform of the form* (2), *where $A = Z_{nr}$, $R = Z_{F_t}[W]/W^{nr/2} + 1$ and $\alpha = W$, which requires no multiplications in Z_{F_t}.*

Proof. By the Chinese Remainder Theorem,

$$R \simeq \prod_{j \text{ odd}} Z_{F_t}[W]/(W^n - a^j). \tag{11}$$

Since in each factor of (11), j is odd, and we assume that the order of a is a power of 2, each a^j satisfies the hypothesis concerning a in the lemma. So W is of order ne_ir mod$(p_i, W^n - a_i^j)$ for each i, j. Hence W is of order divisible by nr mod each irreducible factor of $W^n - a_i^{je_i}$, hence the proposition follows from Corollary 3. The order of W is nr, since under the hypotheses one of the e_i must be 1.

Note. The length of the transform can be changed from rn to $rn/2^b$ by replacing a with a^{2^b} or by taking $\alpha = W^{2^b}$.

Consider the Fermat numbers F_t for $t = 5$ or 6, which are of reasonable size for filtering purposes. In both cases we know that $r = 2^{t+2}$. So for example, with $t = 6$ we can use Proposition 1 to construct a 512×256 pseudocyclic convolution algorithm using $n = 2$, $r = 256$ and $a = \sqrt{2}$. Using (9), we get that the total number of multiplications per point required is 3.5 for: M_1 is $nr/2$, as each application of Φ is a partial FFT, where all multiplications are by even powers of $a = \sqrt{2}$ except in the last step, where multiplications by a^{2i+1} must be performed. Multiplications by 2 are bit shifts mod F_t and performed so quickly on a binary computer that they need not be counted as general multiplications. Also note that for all $t > 1$, $\sqrt{2} = 2^{2^{t-2}}(2^{2^{t-1}} - 1)$, hence multiplication by $\sqrt{2}$ requires only 2 shifts and one addition. We need one multiplication for each of $nr/2$ points for each application of Φ and Φ^{-1} (that being by $\sqrt{2}$), so that $4M_1/nr = 2$. For M_2 we note that in [4, p. 395] there is an algorithm for acyclic length 2 convolution, which requires a total of 5 additions and 3 multiplications so that $M = 3.5$ and $A = 34.5$. If we take $t = 6$, $a = 2$, $n = 2$, and $r = 128$, we get a 256×128 convolution requiring only 1.5 multiplications and 30.5 additions per point since $M_1 = 0$. In this case all multiplications in the computation of T, T^{-1}, Φ and Φ^{-1} are shifts in an array or in a word. In general, minimum values of A_2 and M_2 will increase as n increases. For smaller values of n, M_2 and A_2 may be relatively small. This hope is based on an examination of the work in [4], [14], [20], where short convolution algorithms are given for $n \leqslant 9$.

Remarks. (1) A $K \times L$ convolution performed directly requires KL multiplications and KL additions per point. An algorithm which uses a 2-D complex DFT requires $\log K + \log L + 1$ complex multiplications and $2(\log K + \log L)$ complex additions per point. In the 512×256 case this amounts to $M = 18$ and $A = 34$ in C as opposed to $M = 3.5$ and $A = 34.5$ in Z_M with our method (assuming precomputation on one fixed array). Since two of the multiplications for each point are by $\sqrt{2}$, which involves two shifts and one addition, it is more accurate to say $M = 1.5$ and $A = 36.5$ in our case. Another approach is to use 2-D Fermat number transforms instead of the complex DFT, but there are size limitations. The largest size allowable for the sixth Fermat number is 256×256. The number of algebraic operations required for this method is comparable to the requirements for the algorithms we have presented; however, the 2-D FNT method involves considerably more computational overhead in the form of load and store operations. This is because with our method the kernel for the "outer" 1-D transform is a power of W, so that multiplications by powers of the kernel involve shifts of positions of words in an array, which can be accomplished using a moving pointer. However, the kernel of both 1-D transforms in the 2-D FNT is a power of $\sqrt{2}$, so that multiplication by powers of the kernel involves a shifting operation modulo the Fermat number. This involves loading the multiplicand into a shift register and storing the result.

(2) The algorithms we present here are quite amenable to parallel processing due to the extensive use of the FFT algorithm.

(3) Convolution of square arrays can be done by substituting W^2 for W in the transform T.

(4) There are only a few choices for the modulus M which seem to be very suitable for calculation on a general purpose computer. Other choices may require specially designed arithmetic units. This is discussed in [1], [2].

(5) Long 1-D convolutions can be carried out using special mappings of 1-D arrays into 2-D arrays and performing 2-D convolution. This can be done with the 2-D algorithms given above, using mapping techniques which appear in [3]; however, more efficient methods should probably be found.

(6) A complete list of admissible parameters for algorithms of the type discussed here has yet to be developed. Hopefully this will be forthcoming.

Department of Mathematics
Worcester Polytechnic Institute
Worcester, Massachusetts 01609

1. R. C. AGARWAL & C. S. BURRUS, "Number theoretic transforms to implement fast digital convolutions," *Proc. IEEE*, v. 63, 1975, pp. 550–560.

2. R. C. AGARWAL & C. S. BURRUS, "Fast convolution using Fermat number transforms with applications to digital filtering," *IEEE Trans. Acoust. Speech Signal Processing*, v. 22, 1974, pp. 87–99.

3. R. C. AGARWAL & C. S. BURRUS, "Fast one-dimensional convolution by multidimensional techniques," *IEEE Trans. Acoust. Speech Signal Processing*, v. 22, 1974, pp. 1–10.

4. R. C. AGARWAL & J. W. COOLEY, "New algorithms for digital convolution," *IEEE Trans. Acoust. Speech Signal Processing*, v. 25, 1977, pp. 392–409.

5. R. C. GONZALEZ & P. WINTZ, *Digital Image Processing*, Addison-Wesley, Reading, Mass., 1977.

6. J. JUSTESEN, "On the complexity of decoding Reed-Solomon codes," *IEEE Trans. Inform. Theory*, v. 22, 1976, pp. 237–238.

7. D. KIBLER, "Necessary and sufficient conditions for the existence of the modular Fourier transform: Comments on 'Number theoretic transforms to implement fast digital convolution'," *Proc. IEEE*, v. 65, 1977, pp. 265–267.

8. S. LANG, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

9. D. P. MAHER, *Two-Dimensional Convolution Using Ring Extensions*, Proc. Second Annual Workshop on Information Linkage Between Mathematics and Industry, Academic Press, New York, 1980.

10. F. J. MacWILLIAMS & N. J. A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

11. H. MURAKAMI, I. S. REED & L. R. WELCH, "A transform decoder for Reed-Solomon codes in multiple-user communication systems," *IEEE Trans. Inform. Theory*, v. 23, 1977, pp. 675–683.

12. P. J. NICHOLSON, "Algebraic theory of finite Fourier transforms," *J. Comput. System Sci.*, v. 5, 1971, pp. 524–527.

13. H. J. NUSSBAUMER, "Digital filtering using pseudo Fermat number transforms," *IEEE Trans. Acoust. Speech Signal Processing*, v. 25, 1977, pp. 79–83.

14. H. J. NUSSBAUMER & P. QUANDALLE, "Computation of convolutions and discrete Fourier transforms by polynomial transforms," *IBM J. Res. Develop.*, v. 22, 1978, pp. 134–144.

15. J. M. POLLARD, "The fast Fourier transform in a finite field," *Math. Comp.*, v. 25, 1971, pp. 365–374.

16. C. M. RADER, "Discrete convolutions via Mersenne transforms," *IEEE Trans. Comput.*, v. 21, 1972, pp. 1269–1273.

17. I. S. REED & T. K. TRUONG, "Complex integer convolutions over a direct sum of Galois fields," *IEEE Trans. Inform. Theory*, v. 21, 1975, pp. 657–661.

18. M. C. VANWORMHOUDT, "On number theoretic transforms in residue class rings," *IEEE Trans. Acoust. Speech Signal Processing*, v. 25, 1977, pp. 585–586.

19. E. VEGH & L. M. LIEBOWITZ, *Fast Complex Convolution Using Number Theoretic Transforms*, NRL Report 7935, Naval Research Lab., Washington, D.C., 1975, pp. 1–13.

20. S. WINOGRAD, *Some Bilinear Forms Whose Multiplicative Complexity Depends on the Field of Constants*, IBM Research Report RC 5669, Thomas J. Watson Research Center, Yorktown Heights, N. Y., 1975.