Conditions for the Existence of Fast Number Theoretic Transforms

DUŠAN M. KODEK

Abstract—**A new theorem that gives necessary and sufficient conditions for the existence of computationally fast number theoretic transforms is presented. The theorem combines the general conditions for the existence of number theoretic transforms in the rings of integers modulo m with two conditions for high computational efficiency.**

Index Terms—**Digital filtering, discrete Fourier transforms, fast convolution, fast Fourier transform (FFT), Fermat number transforms, number theoretic transforms.**

I. Introduction

Several authors [1]–[4] have demonstrated the usefulness of the discrete Fourier transforms (DFT's) defined over the rings of integers modulo m. In particular, they can be used to compute finite discrete convolutions without roundoff errors and with substantially fewer operations than with the conventional complex DFT. These qualities have made them an attractive alternative for many applications, and they have been used especially in digital signal processing [4], [6].

The length N DFT's defined over the ring of integers modulo m can be written as a transform pair

$$X(k) \equiv \sum_{l=0}^{N-1} x(l) w_N^{lk} \pmod{m}, \qquad k = 0, 1, \cdots, N-1 \tag{1}$$

$$x(l) \equiv N^{-1} \sum_{k=0}^{N-1} X(k) w_N^{-lk} \pmod{m}, \qquad l = 0, 1, \cdots, N-1 \tag{2}$$

and are now known in the engineering literature as number theoretic transforms (NTT's).

II. Existence of the Number Theoretic Transforms

The necessary and sufficient conditions for the existence of number theoretic transforms defined by (1) and (2) were given by Agarwal and Burrus [4], [14] in a theorem which we include here without a proof.

Theorem 1: Let Z_m be a ring of integers modulo m, $m = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$. A number theoretic transform of length N exists in Z_m if and only if N divides the greatest common divisor of the numbers, $p_1 - 1, p_2 - 1, \cdots, p_l - 1$.

This theorem is in fact a special case of a more general theorem [9], [10], which gives conditions for the existence of a length N discrete Fourier transform in some commutative ring with unity. The conditions require that a ring contains a certain number w_N, called the primitive Nth root of unity, that is defined by

$$w_N^N = 1 \tag{3}$$

and

$$w_N^r \neq 1, \qquad r = 1, 2, \cdots, N-1. \tag{4}$$

It is also necessary that numbers $w_N^r - 1$, $r = 1, 2, \cdots, N-1$, are not divisors of zero and that there exists a multiplicative inverse N^{-1} of N.

The conditions concerning w_N become in the rings of integers modulo m equivalent to the congruences

$$w_N^N \equiv 1 \pmod{p_i^{n_i}}, \qquad i = 1, 2, \cdots, l \tag{5}$$

$$w_N^r \not\equiv 1 \pmod{p_i}, \qquad i = 1, 2, \cdots, l; r = 1, 2, \cdots, N-1 \tag{6}$$

and it is not too difficult to see that Theorem 1 fulfills all of the above conditions. This theorem has been since used as a starting point for many subsequent results [7], [8] that extended the types and applications of number theoretic transforms. Still, it does not give any information about the computational efficiency, and it is easy to see that this efficiency depends heavily upon the values of parameters N, m, and w_N.

III. Conditions for the Existence of Fast NTT's

Let us now limit our attention to those number theoretic transforms that conform to the following two requirements for high computational efficiency.

1) $N = 2^n$. This is an obvious consequence of the FFT algorithm which is most efficient for highly composite numbers N.

2) $w_N \equiv \sqrt[2^s]{2\mu} \pmod{m}$, $\mu \geqq 1$, $0 \leqq s \leqq n-1$. Primitive roots of this form reduce all or a part of multiplications by powers of w_N to simple and fast shifting operations. It is precisely this property of number theoretic transforms that makes them attractive in comparison to other discrete Fourier transforms.

The requirements 1) and 2) define a special subclass of number theoretic transforms. Many NTT's that are of practical interest belong to this subclass. For practical implementations there is, however, the third requirement, namely the simplicity of arithmetic modulo m. Since all operations are performed modulo m, this arithmetic must be simple in order to achieve high computational efficiency. We shall mention this problem again in the last section and proceed here with the requirements 1) and 2).

The general conditions of Theorem 1 may now be replaced with more specific ones that apply to our particular subclass. Let us start with the following corollary of Theorem 1.

Corollary 1: Let Z_m be a ring of integers modulo m, $m = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$. The length $N = 2^n$ NTT exists in Z_m if and only if it is possible to write all the primes p_i, $i = 1, 2, \cdots, l$, in the form $p_i = g_i 2^{h_i} + 1$, where g_i is an arbitrary odd number and $h_i \geqq n$.

Proof: It follows from Theorem 1 that primes p_i, $i = 1, 2, \cdots, l$, must be greater than two for the length $N > 1$ transforms to exist. Every prime number that is greater than two can always be written as

$$p_i = g_i 2^{h_i} + 1, \qquad i = 1, 2, \cdots, l \tag{7}$$

where $h_i \geqq 1$ and g_i an odd number. The greatest common divisor of numbers $p_i - 1$, $i = 1, 2, \cdots, l$ can therefore be written as

$$(p_1 - 1, p_2 - 1, \cdots, p_l - 1) = c2^d \tag{8}$$

where c is the greatest common divisor of numbers g_i, $i = 1, 2, \cdots, l$, and d is the smallest of the exponents h_i, $i = 1, 2, \cdots, l$. It then follows from Theorem 1 that length $N = 2^n$ NTT's exists exactly when 2^n divides 2^d, which is true if all the exponents h_i conform to $h_i \geqq n$. Q.E.D.

This corollary gives the conditions for the existence of length $N = 2^n$ NTT's. We can now proceed with requirement 2), which requires the existence of primitive Nth roots of the form

$$w_N \equiv \sqrt[2^s]{2^\mu} \pmod{m}, \qquad \mu \geqq 1, 0 \leqq s \leqq n-1. \tag{9}$$

Numbers defined by (9) are the solutions of the congruence

$$y^{2^s} \equiv 2^\mu \pmod{m} \tag{10}$$

which is not always solvable. It is therefore necessary to check if these numbers exist under our particular conditions. Congruence (10) has solutions if and only if the following congruences hold [11]:

$$2^{\mu(p_i-1)/d_i} \equiv 1 \pmod{p_i}, \qquad i = 1, 2, \cdots, l \tag{11}$$

where d_i is the greatest common divisor of numbers 2^s and $p_i - 1$.

Manuscript received June 19, 1979; revised May 21, 1980.
The author is with the Department of Electrical Engineering and Computer Science, University of Ljubljana, Ljubljana, Yugoslavia.

0018-9340/81/0500-0359$00.75 © 1981 IEEE

Since we are interested only in transforms that conform to Corollary 1, we have $d_i = 2^s$ and $(p_i - 1)/d_i = a_i 2^{n-s}$, $i = 1, 2, \cdots, l$.

It is now easy to see that (11) holds if we have

$$2^{\mu 2^{n-s}} \equiv 1 (\bmod p_i),\ i = 1, 2, \cdots, l. \tag{12}$$

Equation (12) guarantees the existence of the numbers w_N defined by (9). We shall show the conditions under which it is true in the proof of the following theorem, which is the main result of this paper.

Theorem 2: Let Z_m be a ring of integers modulo m, $m = p_1^{n1} p_2^{n2} \cdots p_l^{nl}$, in which all the primes p_i, $i = 1, 2, \cdots, l$, can be written in the form $p_i = g_i 2^{h_i} + 1$, where g_i is an arbitrary odd number and $h_i \geqq n$. The length $N = 2^n$ NTT with $w_N = \sqrt[2^s]{2^\mu}$, $\mu \geqq 1$, $0 \leqq s \leqq n - 1$, exists in Z_m if and only if m divides the number $2^{\mu 2^{n-s-1}} + 1$.

Proof: Let us first show that (12) holds. Since m divides $2^{\mu 2^{n-s-1}} + 1$ and since we can write

$$2^{\mu 2^{n-s}} - 1 = (2^{\mu 2^{n-s-1}} + 1)(2^{\mu 2^{n-s-1}} - 1) \tag{13}$$

we see that m divides $2^{\mu 2^{n-s}} - 1$ too, and that (12) holds. This guarantees the existence of numbers $\sqrt[2^s]{2^\mu}$.

Ring Z_m satisfies Corollary 1. Knowing that numbers $\sqrt[2^s]{2^\mu}$ exist, it is now enough to prove that (5) and (6) hold for $w_N = \sqrt[2^s]{2^\mu}$ if and only if m divides $2^{\mu 2^{n-s-1}} + 1$.

Suppose first that (5) and (6) hold. Congruences (6) must hold for all $1 \leqq r \leqq 2^n - 1$, and therefore also for $r = 2^{n-1}$

$$2^{\mu 2^{n-s-1}} \not\equiv 1\ (\bmod p_i), \qquad i = 1, 2, \cdots, l. \tag{14}$$

These congruences require that none of the primes p_i, $i = 1, 2, \cdots, l$, divides the number

$$2^{\mu 2^{n-s-1}} - 1 = (2^\mu - 1) \prod_{t=0}^{n-s-2} (2^{\mu 2^t} + 1). \tag{15}$$

At the same time it follows from (5) that

$$2^{\mu 2^{n-s}} \equiv 1\ (\bmod p_i^{ni}), \qquad i = 1, 2, \cdots, l \tag{16}$$

which means that all of the powers p_i^{ni}, $i = 1, 2, \cdots, l$, divide the number

$$2^{\mu 2^{n-s}} - 1 = (2^\mu - 1) \prod_{t=0}^{n-s-1} (2^{\mu 2^t} + 1). \tag{17}$$

Both requirements can be fulfilled simultaneously if all of the powers p_i^{ni} divide $2^{\mu 2^{n-s-1}} + 1$. This is possible only if m divides $2^{\mu 2^{n-s-1}} + 1$ and we have thus proved necessity.

To prove sufficiency let us suppose that m divides $2^{\mu 2^{n-s-1}} + 1$ and show that congruences (5) and (6) hold. It is easy to see from (16) and (17) that for $w_N = \sqrt[2^s]{2^\mu}$ divisibility of $2^{\mu 2^{n-s-1}} + 1$ by m guarantees the validity of (5). Let us proceed with the congruences (6), which can now be written as

$$(\sqrt[2^s]{2^\mu})^r \not\equiv 1 (\bmod p_i) \qquad \begin{matrix} r = 1, 2, \cdots, 2^n - 1 \\ i = 1, 2, \cdots, l. \end{matrix} \tag{18}$$

Suppose that (18) does not hold and that $r = e$, $e \leqq 2^n - 1$, is the smallest exponent for which

$$(\sqrt[2^s]{2^\mu})^e \equiv 1 (\bmod p_i). \tag{19}$$

Since we just proved that (16) is true, e must divide 2^n and is therefore of the form $e = 2^v$. For $0 \leqq v \leqq s$ we have

$$2\mu \equiv 1 (\bmod p_i) \tag{20}$$

which means that at least one p_i divides $2\mu - 1$. For $s + 1 \leqq v \leqq n - 1$ we have

$$2^{\mu 2^{v-s}} \equiv 1 (\bmod p_i) \tag{21}$$

which means that at least one p_i divides $2^{\mu 2^{v-s}} - 1$. Since it is easy to show [12] that numbers $2\mu - 1$, $2\mu + 1$, $2^{\mu 2} + 1, \cdots, 2^{\mu 2^{n-s-1}} + 1$, are pairwise relatively prime and since modulus m divides $2^{\mu 2^{n-s-1}} + 1$, its primes p_i cannot satisfy (20) and (21). The smallest exponent e for which (19) is true equals 2^n, which completes the proof of the theorem. Q.E.D.

IV. Discussion and Conclusions

The main statement of the above theorem is that the requirements 1) and 2) imply that modulus m must divide the number $2^{\mu 2^{n-s-1}} + 1$. In comparison with the well-known conditions of Theorem 1, which do not give a systematic way of determining the "best" choices of parameters N, w_N, and m, this result greatly simplifies the analysis.

For practical implementations we have to include the requirement for simplicity of arithmetic modulo m. Moduli with a 2-bit binary representation, $m = 2^b + 1$ and $m = 2^b - 1$, are the most obvious choices. It is easy to see that numbers $m = 2^b + 1$ conform to the Theorem 2 very well. This case, however, was analyzed extensively using the conditions of Theorem 1 and it does not seem very likely that Theorem 2 can contribute significantly to practical usefulness of these NTT's.

Without discussing the implications of Theorem 2 for the case of moduli with 3 or more bit binary representation, which may be of some practical value [5], we shall conclude with the following two observations.

1) The appearance of number two (or some power of two) as the primitive Nth ($N = 2^n$) root of unity w_N in rings Z_m, $m = 2^b + 1$, is not explained by Theorem 1. It follows from Theorem 2 that this is an inherent property of rings with moduli of the form $m = 2^b + 1$.

2) The existing analysis of NTT's which conform to requirements 1) and 2) was largely based on the conditions of Theorem 1. These conditions do not give a way to systematic analysis and one must use intuition, insight, and a bit of searching [14]. There is a theoretical possibility that some efficient NTT's were overlooked. Theorem 2 virtually eliminates this possibility.

References

[1] A. Schonhage and V. Strassen, "Schnelle multiplikation grosser zahlen," *Comput.*, vol. 7, pp. 281–292, 1971.

[2] J. M. Pollard, "The fast Fourier transform in a finite field," *Math. Comput.*, vol. 25, pp. 365–374, Apr. 1971.

[3] C. M. Rader, "Discrete convolution via Mersenne transforms," *IEEE Trans. Comput.*, vol. C-21, pp. 1269–1273, Dec. 1972.

[4] R. C. Agarwal and C. S. Burrus, "Fast convolution using Fermat number transforms with applications to digital filtering," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-22, pp. 87–97, Apr. 1974.

[5] J. M. Pollard, "Implementation of number-theoretic transforms," *Electron. Lett.*, pp. 378–379, July 22, 1976.

[6] J. H. McClellan, "Hardware realizations of a Fermat number transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 216–225, June 1976.

[7] E. Vegh and L. M. Leibowitz, "Fast complex convolution in finite rings," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 343–349, Aug. 1976.

[8] H. J. Nussbaumer, "Digital filtering using pseudo Fermat number transforms," *IEEE Trans. Acoust. Speech, Signal Processing*, vol. ASSP-25, pp. 79–83, Feb. 1977.

[9] D. Kodek, "Mathematical conditions for the existence of very fast discrete Fourier transform," in *Proc. 1976 Inform. Int. Symp.*, Bled, Yugoslavia, Oct. 1976, p. 3120.

[10] P. J. Nicholson, "Algebraic theory of the finite Fourier transform," Ph.D. dissertation, Dep. Oper. Res., Stanford Univ., Stanford, CA, 1969.

[11] I. Niven and S. Zuckerman, *An Introduction to the Theory of Numbers.* New York: Wiley, 1960, pp. 43–50.

[12] G. M. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* Oxford, England: Oxford Univ. Press, 1962, p. 14.

[13] E. Dubois and A. N. Venetsanupoulos, "The discrete Fourier transform over finite rings with application to fast convolution," *IEEE Trans. Comput.*, vol. C-27, pp. 586–593, July 1978.

[14] R. C. Agarwal and C. S. Burrus, "Number theoretic transform to implement fast digital convolution," *Proc. IEEE*, vol. 63, pp. 550–560, Apr. 1975.

[15] 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*, vol. 65, pp. 265–267, Feb. 1977.