A New Transform To Replace Fermat Transform for Digital Signal Processing

Huizhu Lu
Department of Computing and Information Sciences
Oklahoma State University
Stillwater, Ok 74078
Tel. (405)744-5673

J. B. Conrey
Department of Mathematics
Oklahoma State University
Stillwater, Ok 74078
Tel. (405)744-5847

ABSTRACT

A new formula $M_k = 2^k - 3$ is proposed to generate primes with the least primitive root $= 2$ for use as the modulus in number theoretic transforms. The maximum sequence-length, $M_k - 1$, is achieved with $\alpha = 2$. The well known hardware word-length / sequence-length constraint problem in the Fermat Transform is solved herein. Due to the special structure of the new formula, the multiplication of a power of 2 can be implemented by simple shifts and additions with binary logic circuits. Therefore, the speed of the number theoretic transform with those moduli and $\alpha = 2$ is faster than that of the fast Fourier transform. The results of computations are perfectly accurate without round-off error.

In summary, the number theoretic transform with the new moduli may replace the Fermat Transform. It also has the potential to replace the fast Fourier transform in a larger area.

I. Introduction

In the past two decades, Fermat numbers

$$F_t = 2^{2^t} + 1 \tag{1}$$

and Mersenne numbers

$$M_p = 2^p - 1 \tag{2}$$

where p is a prime, have been used as moduli in number theoretic transforms for fast circular (i.e., periodical) convolution and precise deconvolution in the area of digital signal processing [1-14]. This transform is defined as follows. Let M be the modulus. We shall assume that M is a prime though this assumption is not absolutely necessary. We shall work in $R_M = Z/MZ$, the ring of integers modulo M. Let n be a divisor of $M-1$ and let α be an element of order n in the multiplicative group of R_M. (If $n = M-1$, then α is a primitive root of M.) Let T be the n x n matrix with entries $t_{ij} = \alpha^{ij}$ where $i, j = 0, 1, ..., n-1$, and let $U = (u_0, u_1, ..., u_{n-1})$ be an n-vector. The transform of U is the n-vector $T_n U$. It is easy to see that the inverse transform T_n^{-1} has ij entry $n^{-1}\alpha^{-ij}$, where $i, j = 0, 1, ..., n-1$. It is called Fermat Transform (or Mersenne Transform) if a Fermat number (or a Mersenne number) is used as the modulus in the above number theoretic transform. The Fermat Transform with $\alpha = 2$ is also called Rader Transform.

The transform behaves well under convolution. Thus, if U and V are two n-vectors, then, their convolution is $W = U \otimes V$, where kth component of W is

$$W_k = \sum_{m=0}^{n} u_m v_{k-m} \tag{3}$$

where $k = 0, 1, ...n-1$.

Then, in the ring R_M, we have

$$U \otimes V = T_n^{-1}(T_n U * T_n V) \tag{4}$$

where $*$ denotes pointwise multiplication.

When F_t or M_p have been used as moduli in the number theoretic transform, α is often chosen as 2 or $\sqrt{2}$, and the radix is chosen as 2 for implementation of arithmetic operations. The advantages of the number theoretic transform over the Fast Fourier Transform (FFT) are described as follows:

(1) the results are exact since only integers are used;

(2) the computation speed is faster than that of FFT since the multiplication of a power of 2 when using the above moduli is implemented by shifts and additions with binary logic circuits.

However, there are some drawbacks to the use of F_t and M_p as moduli. First of all, it is most convenient for the modulus M to be a prime. While there is an ample supply of primes of the form M_p where p is a prime, the only prime values known for F_t are when $t = 0, 1, 2, 3,$ or 4. A more serious problem though is known as the sequence-length constraint problem. When using the above moduli it is natural to represent integers using the radix-2 since as mentioned above the multiplications necessary to compute transforms become simple. However, the order of 2 in the ring R_M is relatively small, only about the size of $\log M$. Therefore, the maximum length of a sequence which can be transformed is only a linear function of the hardware word-length (=number of bits needed to represent the modulus). A two dimensional implementation method was proposed by Rader, Ararwal, and Burrus[2][4]. Using a two dimensional implementation of a one dimensional convolution, the maximum length of sequences is twice the square of the hardware word-length. Recently, Lu and Lee[14] proposed a new formula, $M = p^{q^t} \pm (p-1)$, to generate more primes M (including Fermat and Mersenne numbers) for number theoretic transforms. They obtained the maximum sequence-length equal to $M - 1$, which is exponentially proportional to hardware word-length. However, the implementation of the transform involves the use of radix-3 arithmetic.

In this paper, a different solution with fast speed execution to the sequence length problem is offered. Namely, we propose a new formula to generate primes, M. Using these primes as moduli for number theoretic transform, we can have both maximum sequence-length $M-1$ and fast implementation of transforms with convenient radix-2 arithmetic. This paper contains four sections. In section II, a special new formula for the number theoretic transform is introduced. In Section III, a simple scheme for the implementation of arithmetic operations required in the number theoretic transform and circular convolution computation is presented. Section IV gives conclusions.

II. New Moduli for Number Theoretic Transforms

In general, modulo M does not have to be a prime in number theoretic transforms. However, we have to satisfy that both α and n are relatively prime to M for the existence of n^{-1}, and for $\alpha^n \equiv 1$ to hold. Moreover, we have to satisfy the condition that $\alpha^c - 1$ is relatively prime to M for each integer $c, 1 \leq c \leq n-1$ which is a necessary and sufficient condition for obtaining $T_n T_n^{-1} = I$ in modular arithmetic. If the modulus is a prime, all conditions indicated above are easily satisfied. Therefore, let M be a prime.

We propose to use moduli, M_k, of the form

$$M_k = 2^k - 3 \tag{5}$$

with 2 as the least primitive root for the primes M_k. Some desired primes generated by the above formula are listed in Table 1.

Table 1

Some desired primes with least primitive root = 2

k	$M_k = 2^k - 3$	Maximum sequence-length with $\alpha = 2$
3	5	4
4	13	12
5	29	28
6	61	60
9	509	508
10	1,021	1,020
12	4,093	4,092
14	16,381	16,380
20	1,048,573	1,048,572

The hardware word-length required to represent each prime, M_k, listed in Table 1 equals k which is less than 32 bits using binary logic circuits. The maximum sequence-lenth which can be transformed is exponentially proportional to the hardware word-length. This is a tremendous improvement of traditional Fermat and Mersenne transforms with binary logic circuits. The sequence-length constraint problem in one dimentional circular convolution using number theoretic transform is solved herein. The execution speed of the number theoretic transform with the new modulus is faster than that of FFT since the multiplication by a power of 2 can be implemented by shifts and additions(+3) as shown in the next section.

The primes listed in Table 1 have the range 5 to 1,048,573. Among those moduli, we can choose a suitable modulus for practical use. In general, the above primes should provide enough choice.

As is well known, n^{-1} exists in a ring of integers modulo M if and only if n is relatively prime to M. Thus, an advantage of M being prime is that n^{-1} necessarily exists.

In the next section, we provide the implementation of the basic arithmetic operations which are required in the number theoretic transforms and the circular convolution.

III. Implemention of Arithmetic Operations

In this section, a scheme of the implementation of arithmetic operations for the transforms, inverse transforms, and circular convolution of the two sequences, are presented. It includes number representation, addition, subtraction, multiplication by a power of m, and general multiplication in the ring of integers. Assume that the range [0,$M/2$] is used to represent zero and positive numbers, and the range $(M/2, M)$ is used to represent negative numbers. The integers whose absolute values do not exceed $M/2$ can be exactly represented in the ring of integers modulo M. In order to obtain the fast computation speed, the value of the radix, m, should be chosen as the value of α in the number theoretic transform, i.e., $m = \alpha$. If a prime listed in Table 1 is used as a modulus for the number theoretic transform, $m = \alpha = 2$ is the best choice for obtaining the fastest execution speed of arithmetic operations.

The method presented below is a simplified version of the general method proposed by Lu and Lee[14].

(1) Number Representation

Use 2's complement modulo M represent the numbers. Then, the positive number $D = d_t d_{t-1} ... d_0$ in radix-2 arithmetic is

$$D = \sum_{i=0}^{t} d_i 2^i \qquad (6)$$

where $d_i = 0, 1$. The absolute value of D should not exceed $M/2$ as we proposed. The negative number in the ring of integers modulo M in radix-2 arithmetic is

$$-D = -\sum_{i=0}^{t} d_i 2^i = M - \sum_{i=0}^{t} d_i 2^i (mod\ M). \qquad (7)$$

We can implement $-D$ by setting

$$-D = M + 2's\ complement\ of\ D(mod\ M) \qquad (8)$$

and discarding the carry bit from the most significant bit.

(2) Addition/Subtraction

An addition operation in Modulo M arithmetic can be implemented by a conventional addition, and a subtraction can be performed as an addition except negating the subtrahend. If the sum exceeds the modulo M, an additional addition of adding the $2's$ complement of the modulo M to the non-modular sum is necessary for residue reduction, where the carry from most significant bit is discarded.

Example 1: Subtract 6 from 12 in a ring of integers modulo $M =$ 29.

Let modulo $M = 29$. Assume the subtraction is implemented by radix-2 arithmetic since 2 is the least primitive root for the prime 29.

$12\text{-}6 = 12 + 23 = 35 = 6\ (mod\ 29)$.

$29 = (11101)_{radix=2}$

2's complement of 29 is 00011.

$$\begin{array}{r} 01100 \\ +10111 \\ \hline 100011 \\ +00011 \\ \hline 00110 \end{array}$$

We discard the most significant bit of 100011 since it is greater than 11101, and add 00011 to it as residue reduction, we have the result of the computation, 00110 in radix-2 representation.

(3) Multiplication by a Power of α

Multiplication by a power of α is required frequently as a transform proceeds. As $\alpha = 2$, the multiplication by a power of α can be implemented by shifts and additions. When radix-2 arithmetic is used, k-bit hardware word-length is required to represent the numbers from 0 to $M-1$ in a ring of integers modulo M. Multiplication by 2 requires a shift of one position left and an addition of r to it, where

$$r = 3c, \tag{9}$$

c is the carry at $(k+1)$th position. An example is given below to show this method.

Example 2: Multiply 10 by 2^2 in a ring of integers modulo 29.

$M = 2^5 - 3 = 29 = (11101)_{radix=2}, k = 5, a = 3$

Let $radix = \alpha = 2$.

$10 * 2^2 = 40 = 11(mod\ 29)$

$$\begin{array}{r} 10 = 01010 \\ shift\ left\ \ 010100 \\ shift\ left\ \ 101000 \\ \underline{+(r =)00011} \\ 01011 \end{array}$$

Product $= (01011)_{radix=2} = 11(mod\ 29)$

(4) General Multiplication

We store the product of non-modular multiplication of two integers modulo M in a radix binary logic register with length equal to $2n$ bits. We denote the high and low half register by P_h and P_l as shown below.

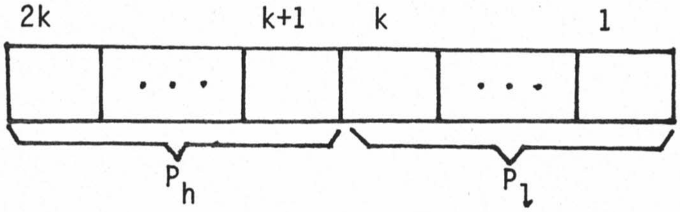

Fig.1 An illustration of P_h and P_l.

Thus, the residue reduction of the product with modulo M may be written as

$$P = P_l + P_h * 2^n \tag{10}$$

i.e.,

$$P = P_l + 3P_h \tag{11}$$

Example 3 is given to illustrate this method.

Example 3: Multiply 12 by 12 in a ring of integers modulo $M = 29$.

$M = 2^5 - 3 = 29$

$2k = 2 * 5 = 10$ bits.

$12 * 12 = 144$

$144 = (0010010000)_{radix=2}$

$P_l = 10000, P_h = 00100$

Product $= (11100)_{radix=2} = 28 = -1(mod\ 29)$

The above scheme of arithmetic operations for the number theoretic transform can be implemented by assembler language easily.

IV. Conclusions

Nine primes of a range from 5 to 1,048,573 are generated by a new formula. 2 is the least primitive root for these primes. We propose to use these primes as moduli, and 2 as the α in the number theoretic transform and circular convolution calculations. Then, the maximum sequence-length, $M-1$, is obtained. The sequence-length which can be transformed is exponentially proportional to the hardware word-length. Therefore, the hardware word-length of a micro-computer or a mini-computer is enough for general application purposes. The hardware word-length / sequence-length constraint problem in the Fermat Transform has been solved herein. Moreover, due to the special structure of the formula, the multiplication of a power of α (=2) in number theoretic transforms can be implemented by shifts and additions using binary logic circuits. This results in that the execution speed of this number theoretic transform is faster than that of a fast Fourier transform.

A simple scheme of implementation of basic arithmetic operations which are required in the number theoretic transforms and circular convolution has been proposed. The result of calculation is exact without round-off error.

In summary, the number theoretic transform with new moduli may replace the Fermat Transform. It also is a good replacement of DFT and FFT in a large area.

References

[1] Rader, C.M., "Discrete Convolution via Mersenne Transforms," *IEEE Trans. Comput.*, Vol. c-21, No. 12, 1972, pp.1269-1273.

[2] Rader, C.M., "On the Application of the Number Theoretics Transforms of High Speed Convolution to Two-Dimensional Filtering," *IEEE Trans. Circuits and Systems*, Vol. CAS-22, June 1975, p.575.

[3] Agarwal, R.C. & Burrus, C.S., "Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering," *IEEE Trans. Acoust., Speech, and Signal Processing*, Vol. ASSP-22, No. 2, 1974, pp.87-97.

[4] Agarwal, R.C. & Burrus, C.S., "Fast One-Dimensional Digital Convolution by Multidimensional Techniques," *IEEE Trans. Acoust., Speech, and Signal Processing*, Vol. ASSP-22, No. 1, 1974, pp. 1-10.

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

[6] Chevillat, P.R., "Transform-Domain Digital Filtering with Number Theoretic Transforms and Limited Word Lengths," *IEEE Trans. Acoust., Speech, and Signal Processing*, Vol. ASSP-26, 1978, pp. 284-290.

[7] Nussbaumer, H.J., "Digital Filtering Using Pseudo Fermat Number Transform," *IEEE Trans. Acoust., Speech, and Signal Processing*, Vol. ASSP-25, 1977, pp. 79-83.

[8] Brule, J.D., "Fast Convolution with Finite Field Fast Transforms," *IEEE Trans. Acoust., Speech, and Signal Processing*, Vol. ASSP-23, 1975, p. 240.

[9] Reed, E.S., & Truong, T.K., "The Use of Finite Fields to Compute Convolutions," *IEEE Trans. Inform. Theory*, Vol. IT-21, 1975, pp. 208-213.

[10] Nussbaumer, H.J., "Digital Filtering Using Complex Mersenne Transforms," *IBM J. Res. Dev.*, Vol. 20, 1976, pp. 498-504.

[11] Nussbaumer, H.J., *Fast Fourier Transform and Convolution Algorithms,* Springer-Verlag. Berlin(1981)

[12] Morhac, M., ”Precise Deconvolution Using the Fermat Number Transform,” *Comput & Maths. with Appls.,* Vol. 12A, No. 3, 1986, pp. 319-329.

[13] McClellan, J.H., ”Hardware Realization of a Fermat Number Transform,” *IEEE Trans. Acoust., Speech, and Signal Processing,* Vol. ASSP-24, No. 3, 1976, pp. 216-225.

[14] Lu, H. & Lee, S.C., ”A New Approach to Solve the Sequence-Length Constraint Problem in Circular Convolution Using Number Theoretic Transforms,” *Proc. of the 26th Annual Allerton Conference on Communication, Control, and Computing,* University of Illinois, Urbana-Champaign, Illinois, 1988, pp. 1005-1014.

[15] Lu, H. & Lee, S.C., ”Fast Convolution Using Generalized Fermat/Mersenne Number Transforms,” *IEEE Proc. of International Conference on Acoust., Speech, and Signal Processing,* 1988, pp. 1910-1913.