IBM Journal of research and development

IBM J. Res. Develop., Vol. 20, No. 3, pp. 197–300, May 1976

H. J. Nussbaumer

Complex Convolutions via Fermat Number Transforms

Abstract: An approach is described for computing complex convolutions modulo a Fermat number. It is shown that this technique is particularly efficient when the complex convolution is computed by means of Fermat Number Transforms and leads to improved implementation of complex digital filters.

Introduction

In most applications that involve the processing of digital signals, the bulk of the processing workload corresponds generally to digital filter functions. Among the various techniques that have been proposed for the efficient implementation of digital filters, those using finite field transforms [1, 2] are particularly promising. In such approaches, the continuous convolution corresponding to the digital filtering process is divided into a series of circular convolutions by the conventional overlap-add, overlap-save methods [3] and the various circular convolutions are computed by means of finite field transforms having the circular convolution property. The advantages of these transforms are the elimination of roundoff errors and the possibility of computation without multiplications. Additional computational savings can be achieved by using Fermat Number Transforms [4, 5] which are finite-field or ring transforms amenable to fast transform algorithms.

In this communication we consider the case of filtering complex signals. This case is important in many applications such as radar, sonar, and modem equalizers [6]. We show that, owing to the special representation of complex numbers in a Fermat number ring, it permits more efficient computation of complex convolutions than does the conventional complex number field. We then extend these results to the case of complex convolutions computed with Fermat transforms and show that the number of multiplications can be reduced by a factor of two when compared to the conventional Fermat transform approach.

Complex convolutions in a Fermat field

Consider a complex integer sequence $\{y_n\}$ to be filtered by a complex sequence having N terms $\{b_n\}$, in which $\{u_n\}$ is the filtered output sequence. $\{u_n\}$ is defined by the convolution

$$u_m = \sum_{n=0}^{N-1} b_n \, y_{(m-n)}. \tag{1}$$

Assuming $\{x_n\}$, $\{a_n\}$, $\{z_n\}$ and $\{\hat{x}_n\}$, $\{\hat{a}_n\}$, $\{\hat{z}_n\}$ are respectively the in-phase and quadrature signal components of $\{y_n\}$, $\{b_n\}$, $\{u_n\}$, we have:

$$y_n = x_n + j\,\hat{x}_n; \tag{2}$$

$$b_n = a_n + j\,\hat{a}_n; \tag{3}$$

$$u_n = z_n + j\,\hat{z}_n, \qquad j = \sqrt{-1}. \tag{4}$$

Under these conditions, the in-phase and quadrature components of the output sequence become:

$$z_m = \sum_{n=0}^{N-1} \left(a_n x_{(m-n)} - \hat{a}_n \hat{x}_{(m-n)} \right), \tag{5}$$

$$\hat{z}_m = \sum_{n=0}^{N-1} \left(\hat{a}_n x_{(m-n)} + a_n \hat{x}_{(m-n)} \right). \tag{6}$$

It can be seen that direct computation of each complex output sample W_m requires $4N$ multiplications and $4N-2$ additions. These figures can be lowered to $3N$ multiplications and $3N+2$ additions by computing z_m with Golub's algorithm [7]

$$z_m = \sum_{n=0}^{N-1} \Big((a_n - \hat{a}_n)(x_{(m-n)} + \hat{x}_{(m-n)}) - a_n \hat{x}_{(m-n)} + \hat{a}_n x_{(m-n)} \Big). \tag{7}$$

Now consider the case of a convolution computed modulo a Fermat number $p = 2^q + 1$ with $q = 2^r$, as $2^q \equiv -1$, and $\frac{q}{2} = 2^{r-1}$, $j = \sqrt{-1}$ can be represented in this ring by $2^{q/2}$. It is therefore possible to compute directly a complex convolution u_m in a Fermat number system by

$$u_m = \left(\left(\sum_{n=0}^{N-1} (a_n + 2^{q/2}\hat{a}_n)(x_{(m-n)} + 2^{q/2}\hat{x}_{(m-n)})\right)\right), \quad (8)$$

where any quantity enclosed by superfluous double parentheses is to be replaced by its value modulo p.

Because $2^q \equiv -1$, Eq. (8) becomes

$$u_m = ((z_m + 2^{q/2}\hat{z}_m)). \quad (9)$$

The in-phase and quadrature components z_m and $\hat{z}_m$ of the output sample can be separated by considering the auxiliary convolution

$$v_m = \left(\left(\sum_{n=0}^{N-1} (a_n - 2^{q/2}\hat{a}_n)(x_{m-n} - 2^{q/2}\hat{x}_{m-n})\right)\right), \quad (10)$$

$$v_m = ((z_m - 2^{q/2}\hat{z}_m)). \quad (11)$$

Combining (9) and (11) yields

$$z_m = ((-2^{q-1}(u_m + v_m))); \quad (12)$$

$$\hat{z}_m = ((-2^{q-2/2}(u_m - v_m))), \quad (13)$$

which shows that computing a complex output sample requires only $2N$ multiplications and $2N + 4$ additions, that is to say half as many multiplications as with the conventional approach.

With this method, it is therefore possible to compute a complex convolution modulo a Fermat number with fewer operations than with the conventional approach or Golub's algorithm. The price to be paid for this reduction in number of operations is that all multiplications and additions must be performed in the finite Fermat field or ring. This will usually lead to the use of word lengths longer than with the conventional approach, or Golub's algorithm, in order to prevent overflow in the final result. This means that the reduction in number of operations achieved with the proposed approach does not necessarily translate into processing workload reduction.

We show, however, in the next section that when the complex convolution is computed by means of Fermat Number Transforms, it is possible to reduce the number of operations without additional penalty in word length increase, thereby achieving an overall processing workload reduction.

Complex convolutions using Fermat Number Transforms

As outlined in [4] and [5], a promising approach to computing convolutions consists in replacing direct or Fast Fourier Transform implementation (FFT) by Fermat Number Transform (FNT) implementation.

In such an approach, the continuous convolution is converted into a series of circular convolutions on blocks of samples $\{x_n\}$ and $\{a_n\}$ to which zeros are appended to prevent folding and aliasing. FNT transforms $\{A_k\}$ and $\{X_k\}$ of $\{a_n\}$ and $\{x_n\}$ are then computed and, because the FNT transform has the cyclic convolution property, taking the inverse FNT transform of $\{A_k \cdot X_k\}$ yields the desired convolution products. As Fermat Number Transforms can be computed by fast algorithms without multiplications, this method yields a drastic reduction in number of multiplications when compared to either direct or FFT implementation.

Fermat Number Transforms are computed modulo a Fermat number. The method described in the preceding section for computing complex convolutions modulo a Fermat number is therefore directly applicable to the case of a FNT implementation. However, in contrast with the approach discussed in the preceding section, taking advantage of the particular representation of complex numbers in a Fermat ring to reduce the number of operations will not yield additional word length increases because word sizes must already be tailored for operation modulo a Fermat number in the FNT implementation [4, 5].

In order to make these points precisely, let us first consider the conventional computation of a complex cyclic convolution via FNT. The Fermat and Inverse Fermat Number Transforms can be defined as

$$\text{FNT } (x_n) \triangleq X_k = \left(\left(\sum_{n=0}^{N-1} x_n 2^{nk}\right)\right); \quad (14)$$

$$\text{I FNT } (X_k) \triangleq x_m = \left(\left(R \sum_{k=0}^{N-1} X_k 2^{-mk}\right)\right); \quad (15)$$

$$N = 2q \qquad R = 2^{-(r+1)} \qquad n, k = 0, 1, \cdots, N-1.$$

Assuming X_k, $\hat{X}_k$, A_k, $\hat{A}_k$ are respectively the Fermat Number Transforms of x_n, $\hat{x}_n$, a_n, $\hat{a}_n$, the in-phase and quadrature components of the complex circular convolution become

$$z_m = \text{I FNT } \{A_k X_k - \hat{A}_k \hat{X}_k\}, \quad (16)$$

$$\hat{z}_m = \text{I FNT } \{\hat{A}_k X_k + A_k \hat{X}_k\}. \quad (17)$$

We can see that for a complex circular convolution of N points, this method requires computing six Fermat or Inverse Fermat Number Transforms and $4N$ multiplications and $2N$ additions in the transform domain.

As all operations are performed modulo a Fermat number, we can reduce the number of multiplications in the transform domain by using the method described in the preceding section. Under these conditions, z_m and $\hat{z}_m$ become

$$z_m = ((-2^{q-1}(\text{IFNT } \{(A_k + 2^{q/2}\hat{A}_k)(X_k + 2^{q/2}\hat{X}_k) + (A_k - 2^{q/2}\hat{A}_k)(X_k - 2^{q/2}\hat{X}_k)\}))); \quad (18)$$

$$\hat{z}_m = ((-2^{q-2/2}(\text{IFNT } \{(A_k + 2^{q/2}\hat{A}_k)(X_k + 2^{q/2}\hat{X}_k) - (A_k - 2^{q/2}\hat{A}_k)(X_k - 2^{q/2}\hat{X}_k)\}))). \quad (19)$$

If we compare the conventional approach (16), (17) to that corresponding to (18), (19), we can see that both methods require computing six Fermat or Inverse Fermat Transforms but that the proposed approach requires only $2N$ multiplications and $6N$ additions in the transform domain.

Moreover, if the filter is time invariant, $-2^{q-1}(A_k + 2^{q/2}\hat{A}_k)$, $-2^{q-1}(A_k - 2^{q/2}\hat{A}_k)$ can be precomputed once and for all so that the number of additions in the transform domain reduces to $4N$.

The proposed approach permits, therefore, the computation of a circular convolution by means of FNT with an average of only two multiplications per complex output sample instead of four multiplications in the conventional case. This processing workload reduction is achieved without word length increase.

Conclusion

It has been shown that complex convolutions can be computed efficiently modulo a Fermat number thanks to the particular representation of complex numbers in the corresponding field or ring.

This result is especially significant when complex convolutions are computed by means of Fermat Number Transforms. In that case, all operations are already performed modulo a Fermat number so that the proposed approach permits halving the required number of multiplications without imposing additional overflow constraints over what is required for the conventional technique using Fermat Number Transforms.

The method described in this paper may be used for filtering complex signals and therefore can find application in a number of cases concerning, e.g., radars, sonars, and modems.

References

1. J. M. Pollard, "The Fast Fourier Transform in a Finite Field," *Math. Comput.* **25,** 365 (1971).
2. D. E. Knuth, *The Art of Computer Programming. Vol. 2., Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1969. Ch. 4.3.3.C, pp. 269-275.
3. B. Gold, C. M. Rader, A. V. Oppenheim, and T. G. Stockham, *Digital Processing of Signals*, McGraw-Hill Book Company, Inc., New York, 1969. Ch. 7, pp. 203-213.
4. C. M. Rader, "Discrete Convolutions via Mersenne Transforms," *IEEE Trans. Comput.* **C-21,** 1269 (1972).
5. R. C. Agarwal and C. S. Burrus, "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proc. IEEE* **63,** 550 (1975).
6. R. D. Gitlin, E. Y. Ho, and J. E. Mazo, "Passband Equalization of Differentially Phase-Modulated Data Signals," *Bell System Tech. J.* **52,** 219 (1973).
7. R. C. Singleton, "An Algorithm for Computing the Mixed Radix Fast Fourier Transform," *IEEE Trans. Audio and Electroacoustics* **AU-17,** 93 (1969).

Received November 10, 1975

The author is located at Compagnie IBM France, Centre d'Etudes et Recherches 06610 La Gaude, France.

Recent IBM Patents

The following patents were recently issued by the countries in which the inventions were made.

Germany

1,814,676	H. H. Berger and S. Wiedmann	Improvements in or Relating to Circuits for use in Data Storage Apparatus
2,247,735	A. Blum, L. Reichl, C. Mohr, R. Assmuth, G. Sonntag and W. Schmidt	Data Processing System
2,309,186	E. Feicht, H. Schettler, W. Houg and R. Remshardt	Means for Equalizing Line Potential When the Connecting Switch is Open
2,340,770	U. Baitinger, M. Illi, R. Clemen, W. Houg and K. Gansslosor	Fast Source
MR04,415	W. Fischer and H. Walgher	Administrative Terminal Printer

United Kingdon

1,396,834	J. R. Taylor	Data Storage Apparatus

United States

3,572,555	A. H. Knight and M. J. Miller	Xerographic Toner Dispenser
3,903,324	T. F. Gukelberger, Jr., and W. J. Kleinfelder	Method of Changing the Physical Properties of a Metallic Film by Ion Beam Formation
3,903,328	E. R. Burdette, Jr., D. D. Dean and W. L. Mitchell	Conductive Coating
3,903,364	E. G.-H. Lean	High Resolution Line Scanner
3,903,516	N. R. Mauro, Jr.	Control Logic for Gas Discharge Display Panel
3,905,841	A. Simonetti	Method of Improving Dispersability of Small Metallic Magnetic Particles in Organic Resin Binders
3,906,141	C. W. Anderson, D. O. Castrodale and J. T. Martin	Printing System
3,906,153	A. Polischuk-Sawtschenko	Remote Synchronous Loop Operations Over Half-Duplex Communications Link
3,906,218	H. J. Nussbaumer	Digital Filters
3,906,254	R. D. Lane and R. A. Manning	Complementary FET Pulse Level Converter
3,906,432	E. A. Ash	Grating Guides for Acoustic Surface Waves
3,906,468	O. Voegeli	Semicircular Magnetic Domain Propagation Apparatus
3,906,480	A. A. Schwartz and J. R. Stewart	Digital Television Display System Employing Coded Vector Graphics
3,906,485	S. J. Hong and D. L. Ostapko	Data Coding Circuits for Encoded Waveform with Constrained Charge Accumulation
3,906,538	J. Matisoo and H. H. Zappe	Techniques for Minimizing Resonance Amplitudes of Josephson Junction
3,906,649	D. W. Schaefer and J. W. Woods	Dimensionally Stable Film Mounting
3,907,091	J. H. Meier and J. W. Raider	Type Disc-Interposer Assembly for a Printer
3,907,429	L. Kuhn, R. A. Myers, K. S. Pennington and B. R. Shah	Method and Device for Detecting the Velocity of Droplets Formed From a Liquid Stream
3,908,155	D. W. Skinner	Wafer Circuit Package
3,908,194	L. T. Romankiw	Integrated Magnetoresistive Read, Inductive Write, Batch Fabricated Magnetic Head
3,908,809	H. S. Beattie	High Speed Printer
3,908,896	J. L. Monrolin	Digital Resolver Filter and Receiver Using Same
3,908,925	H. O. Rinkleib and W. J. Rueger	Tape Cassette Opener
3,908,986	C. D. Bleau	Sheet Aligning Mechanism
3,909,094	T. R. Gardner	Gas Panel Construction
3,909,629	P. T. Marino	H-Configured Integration Circuits With Particular Squelch Circuit
3,909,630	B. C. Fiorino and P. T. Marino	High-Rate Integration, Squelch and Phase Measurements
3,909,634	G. A. Maley and J. L. Walsh	Three State Latch
3,909,637	J. A. Dorler	Cross-Coupled Capacitor For AC Performance Tuning
3,909,678	A. A. Rifkin and R. W. Staats	Packaging Structure For A Plurality of Wafer Type Integrated Circuit Elements

3,909,702	B. E. Hart	Switching Voltage Regulator With Optical Coupling
3,909,787	G. J. Laurer and E. A. Moore	Candidate Selection Processor
3,909,791	J. W. van den Berg	Selectively Settable Frequency Divider
3,909,803	W. F. Bankowski, Jr, V. R. Kumar, W. McGovern and J. D. Tartemella	Multi-Phase CCD Shift Register Optical Sensor with High Resolution
3,909,808	W. H. Cochran, D. A. Heuer, and M. J. Sheehan	Minimum Pitch MOSFET Decoder Circuit Configuration
3,910,395	D. F. Colglazier and G. W. Westphal	Apparatus for Print Head Retraction to Facilitate Paper Insertion
3,910,527	O. R. Buhler, J. T. Cutter, J. P. Mantey and D. R. Wood	Web Distribution Controlled Servomechanism in a Reel-to-Reel Web Transport
3,910,570	C. D. Bleau	Document Feed Apparatus
3,911,261	J. M. Taylor	Parity Prediction and Checking Network
3,911,290	R. A. Kenyon and N. G. Vogl, Jr.	N-Phase Bucket Brigade Optical Scanner
3,911,303	P. Y. Hu, K. N. Karol, G. A. Puzo and B. C. Schwartz	Copper Commutator-Aluminum Winding Armature
3,911,321	G. A. Wardly	Error Compensating Deflection Coils in a Conducting Magnetic Tube
3,911,361	R. Bove, A. Kostenko, Jr. and W. J. Tkazyik, Jr.	Coaxial Array Space Transformer
3,911,363	M. A. Patten	Delta Modulation Circuitry with Automatic Squelch and Gain Control
3,911,401	H. Lee	Hierarchical Memory/Storage System for an Electronic Computer
3,911,407	J. C. Greek, Jr., M. E. McBride and H. C. Tanner	Text Processing System
3,911,411	B. E. Argyle and J. C. DeLuca	Magnetic Domain Systems Using Different Types of Domains
3,911,421	P. M. Alt, P. Pleshko and E. S. Schlig	Selection System for Matrix Displays Requiring AC Drive Waveforms
3,911,422	A. W. McDowell and F. M. Lay	Gas Panel with Shifting Arrangement with a Display Having Increased Light Intensity
3,911,424	R. J. Giannuzzi, G. G. Langdon, Jr. and E. Pasternak	Alphanumeric Character Display Scheme for Programmable Electronic Calculators
3,911,428	W. B. Chin	Decode Circuit
3,911,464	W. H. Chang and H.-S. Lee	Nonvolatile Semiconductor Memory
3,911,558	K. Ashar and S. Magdo	Microampere Space Charge Limited Transistor
3,912,144	P. J. Arseneault and E. P. Kollar	Tape Transport for Magnetic Recording with a Rotating Head
3,912,366	G. J. Sprokel	Liquid Crystal Display Assembly Having Polyimide Layers
3,912,391	H. Fleisher, T. J. Harris and E. Shapiro	Optical Information Storage and Retrieval System with Optical Storage Medium
3,912,872	P. R. Callens	Data Transmission Process
3,912,917	H. Nussbaumer	Digital Filter
3,912,943	M. G. Wilson	Video Thresholder
3,913,021	W. F. McCarthy and P. R. Myers	High Resolution Digitally Programmable Electronic Delay for Multi-Channel Operation
3,913,027	H. H. Zappe	High Gain, Large Bandwidth Amplifier Based on the Josephson Effect
3,913,068	A. M. Patel	Error Correction of Serial Data Using a Subfield Code
3,913,071	F. J. Garofalo, Jr.	Data Terminal Having Interaction with Central System
3,913,079	L. L. Rosier	Magnetic Bubble Domain Pump Shift Register
3,913,120	S. K. Lahiri	Thin Film Resistors and Contacts for Circuitry
3,914,588	H. J. Nussbaumer	Digital Filters
3,914,631	A. M. Guzman and H. D. Lawes	Capstan Motor Having a Ceramic Output Shaft and an Adhesively Attached Capstan
3,914,655	R. W. Dreyfus and R. T. Hodgson	High Brightness Ion Source
3,914,745	D. W. Cooper and J. B. Unruh	System and Method for Aligning Textual Character Fields
3,914,749	S. D. Malaviya	D.C. Stable Single Device Memory Cell
3,914,751	G. E. Keefe, Y. S. Lin and L. L. Rosier	Gapless Multithickness Propagation Structure for Magnetic Domain Devices
3,914,760	J. C. Logue	Accurate and Stable Encoding with Low Cost Circuit Elements
3,914,789	C. W. Coker, Jr., T. A. Hickox, J. J. Lynott and T. F. O'Rourke	Manually Operated Magnetic Card Encoder
3,915,047	S. A. Davis and T. A. Hendrickson	Apparatus for Attaching A Musical Instrument to a Computer
3,915,279	G. H. Schacht	Printer Type Element Deflection Limiter
3,915,537	J. B. Harris, K. M. Hoffman, D. W. Hogan, J. R. Mankus and V. P. Subik	Universal Electrical Connector
3,915,698	K. Lee, G. B. Street and J. C. Suits	Stabilization of Manganese Bismuth in the High Temperature Phase
3,915,770	G. R. Santillo, Jr.	Method and Apparatus for Thermo-Chemically Slicing Crystal Boules
3,915,784	M. P. Makhijani, F. Scacciaferro and C. Yakubowski	Method of Semiconductor Chip Separation
3,916,036	E. Gipstein, W. M. Moreau and O. U. Need, III	Sensitized Decomposition of Polysulfone Resists