The Chinese Remainder Theorem, Associative Algebras, and Multiplicative Complexity

Glenn S. Zelniker
The Athena Group, Inc. and University of Florida

Fred J. Taylor
University of Florida

Abstract

Polynomial multiplication continues to play a fundamental role in many important algorithms (*e.g.*, convolution, correlation). Many methods have been developed which facilitate highly efficient polynomial multiplication. One such method is based on the Chinese Remainder Theorem (CRT), a classic result from ring theory. The CRT is known to reduce the complexity of polynomial multiplication from $O(N^2)$ to $O(N)$. A new interpretation of this complexity reduction is given in the context of associative algebras. This new point of view provides a clearer understanding of the CRT.

1 Introduction

Several fundamental signal processing operations (*e.g.*, cyclic convolution, correlation) can be cast in polynomial form. Fast algorithms for performing these operations are often based on the problem of computing the product of two polynomials f and g modulo some other polynomial p of degree N with minimal multiplicative complexity [Bla85], [MR79]. The Chinese Remainder Theorem (CRT), when applied to polynomial rings, provides a particularly efficient solution to this problem.

For instance, the polynomial residue number system (PRNS) [Ska87] is concerned with the problem of computing convolutions and correlations and long-wordlength real and complex multiplications. The PRNS is based on embedding computations in a polynomial ring over a finite field and exploiting the CRT, which reduces the multiplicative complexity from $O(N^2)$ to $O(N)$. A thorough description of the PRNS is not the objective of this report (a comprehensive treatment is given by [Ska87]). Of significant interest, however, is a deeper understanding of the isomorphism that allows such a dramatic reduction in multiplicative complexity. It will be shown that the complexity has a simple, yet important interpretation in the context of associative algebras.

2 Polynomial Rings and the CRT

Let F be a field. Recall that by $F[x]$ is meant the ring of polynomials with coefficients in F and that F^N denotes the N-fold cartesian product of F with itself. The Fast cyclic convolutions and correlations are premised on the existence of an isomorphism between the quotient rings $F[x]/\langle x^N - 1\rangle$ or $F[x]/\langle x^N + 1\rangle$ and the ring F^N. It is essential that the following condition is met:

Condition 1 The polynomial $x^N \pm 1$ has N distinct linear factors over the base field F. In this case, we have

$$x^N \pm 1 = (x - r_0)(x - r_1)\cdots(x - r_{N-1}).$$

This condition obviously depends on the nature of the field F and the degree N. The PRNS, for example, is based on the field $F = GF(p)$ for some prime p. Admissible choices for p and N are easily obtained using elementary number theory (see, for example, [HW38], [Ska87]).

Returning again to the general case of F an arbitrary field, assume that condition 1 is met. Then the principal ideals $\langle x - r_i\rangle$ generated by the distinct linear factors $(x - r_i)$ are pairwise relatively prime. The existence of the isomorphism between $F[x]/\langle x^N \pm 1\rangle$ and F^N is now guaranteed by the CRT [Lan84].

Theorem 1 (Chinese Remainder Theorem) *Let R be a ring and $I_1, I_2, \ldots, I_n \subset R$ a set of pairwise relatively prime ideals,* i.e.,

$$I_k + \bigcap_{j \neq k} I_j = R.$$

If J is defined by

$$J = \bigcap_{i=1}^{n} I_i,$$

then

$$R/J \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n.$$

To apply the CRT to our problem, let R be $F[x]$. Also, let $I_i = \langle x - r_i\rangle$, $i = 0, 1, \ldots, N-1$ where the r_i are the N distinct roots of the congruence $x^N \pm 1 = 0$. Then $\bigcap_{i=1}^{N} I_i = \langle x^N \pm 1\rangle$ and hence

$$\frac{F[x]}{\langle x^N \pm 1\rangle} \cong \frac{F[x]}{\langle x - r_0\rangle} \oplus \frac{F[x]}{\langle x - r_1\rangle} \oplus \cdots \oplus \frac{F[x]}{\langle x - r_{N-1}\rangle}.$$

But $F[x]/\langle x - r_i\rangle \cong F$, whence

$$F[x]/\langle x^N \pm 1\rangle \cong F^N. \tag{1}$$

Eq. 1 is the fundamental result upon which most fast polynomial multiplication systems are premised. The forward and inverse mappings relating the two isomorphic rings will now be developed. First, let $f(x) = f_0 + f_1 x + \cdots + f_{N-1}x^{N-1}$ be a polynomial in the ring $F[x]/\langle x^N \pm 1\rangle$. The image $\vec{\phi}$ of $f(x)$ in F^N is given by the canonical homomorphism

$$\vec{\phi} = (f(r_0), f(r_1), \ldots, f(r_{N-1}))^T \in F^N.$$

This mapping can be represented in matrix form as

$$\begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_N \end{pmatrix} = \begin{pmatrix} 1 & r_0 & \cdots & r_0^{N-1} \\ 1 & r_1 & \cdots & r_1^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & r_{N-1} & \cdots & r_{N-1}^{N-1} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix} = \mathbf{V}\vec{f}.$$

The N-by-N matrix $\mathbf{V} \in M_{N\times N}(F)$ is a Vandermonde matrix and is intimately related to the problem of Lagrange Interpolation. If $\mathbf{V}$ is invertible over $M_{N\times N}(F)$, then a polynomial $f(x)$ can be recovered from its image $\vec{\phi} \in F^N$ simply by

$$\vec{f} = \mathbf{V}^{-1}\vec{\phi}.$$

The following theorem [GOR87] establishes the invertibility of $\mathbf{V}$.

24ACSSC-12/90/0311 $1.00

Theorem 2 *The Vandermonde matrix* $\mathbf{V}$ *is invertible over the field* F.

Proof: For $k = 0, 1, \ldots, N-1$, define the polynomials $L_k(x)$ by

$$L_{k,0} + L_{k,1}x + \cdots + L_{k,N-1}x^{N-1} = \left(\prod_{j \neq k}(x - r_j)\right)\left(\prod_{j \neq k}(r_k - r_j)\right)^{-1},$$

which are the Lagrange interpolation polynomials over the field F. It immediately follows that $L_k(r_j) = \delta_{kj}$ (where $\delta_{kj} = 0$ if $k \neq j$ and $\delta_{kj} = 1$ if $k = j$), so the inverse of $\mathbf{V}$ is given by

$$\mathbf{V}^{-1} = \begin{pmatrix} L_{0,0} & L_{1,0} & \cdots & L_{N-1,0} \\ L_{0,1} & L_{1,1} & \cdots & L_{N-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ L_{0,N-1} & L_{1,N-1} & \cdots & L_{N-1,N-1} \end{pmatrix}. \quad \square$$

The isomorphism represented by $\mathbf{V}$ allows the product of two polynomials in the ring $F[x]/\langle x^N \pm 1\rangle$ (a computation which requires $O(N^2)$ F-multiplies) to be computed in the ring F^N (with just $O(N)$ F-multiplies). An important interpretation of this reduction in multiplicative complexity is provided by viewing the computations as occurring over an associative algebra.

3 Associative Algebras and Complexity

For a deeper understanding of why the Chinese remainder theorem reduces multiplicative complexity from $O(N^2)$ to $O(N)$, it will be necessary to move the discussion away from ring theory. The reason is simple; there is no notion of *basis* in a ring. The theory of vector spaces is also unsatisfactory since there is no multiplicative structure in a vector space. *Associative algebras* [Jac85], however, suffer from neither of these shortcomings and are the ideal algebraic structure in which to discuss our particular complexity issue.

Definition 1 *An* **associative algebra** *over a field* F *is a pair consisting of a ring* $(R, +, \cdot, 0, 1)$ *and a vector space* R *over* F *such that the underlying set* R *and the addition and* 0 *are the same in the ring and vector space, and*

$$a(xy) = (ax)y = x(ay)$$

holds for $a \in F$ *and* $x, y \in R$. *If* R *is finite dimensional over* F, *then the algebra is said to be* **finite dimensional**.

It is simple to impose the structure of an associative algebra on the rings $F[x]/\langle x^N \pm 1\rangle$ and F^N. Simply maintain the multiplicative and additive structures of both rings and let the field F act on both of the rings with the scalar-vector product defined in the obvious way. It is trivial to verify that all of the axioms are satisfied and that what results is a pair of associative algebras over F.

Ignoring for now the multiplicative structure, the vector space (over F) $F[x]/\langle x^N \pm 1\rangle$ is of dimension N with basis

$$\mathcal{B}_1 = \{\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{N-1}\} := \{1, x, x^2, \ldots, x^{N-1}\}$$

and hence is isomorphic to the F-vector space F^N with canonical basis

$$\mathcal{B}_2 = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_N\}$$

where

$$\vec{e}_i = (0, 0, \ldots, \overset{i}{1}, 0, \ldots, 0).$$

It is thus clear that the mapping represented by $\mathbf{V}$ is a vector space isomorphism. The notion of isomorphic algebras, however, still needs to be clarified.

Definition 2 *A map of an algebra* R *into an algebra* S *over the same field* F *is an* **algebra isomorphism** *if it is both a ring isomorphism and a linear map.*

Theorem 3 *The mapping represented by the matrix* $\mathbf{V}$ *is an algebra isomorphism of the* F*-algebras* $F[x]/\langle x^N \pm 1\rangle$ *and* F^N.

Proof: The CRT already shows that $\mathbf{V}$ is a ring isomorphism. It is simple to show that $\mathbf{V}$ is F- linear; clearly, $\mathbf{V}(\vec{f} + \vec{g}) = \mathbf{V}\vec{f} + \mathbf{V}\vec{g}$ and for any $a \in F$, $\mathbf{V}(a\vec{f}) = (a\mathbf{V})\vec{f}$. Hence, $F[x]/\langle x^N \pm 1\rangle$ and F^N are isomorphic as F-algebras. $\square$

An element $f(x)$ of $F[x]/\langle x^N \pm 1\rangle$ can be expressed relative to the basis $\mathcal{B}_1$ as

$$f(x) = \sum_{i=0}^{N-1} f_i \vec{v}_i$$

or its image $\vec{\phi} \in F^N$ under $\mathbf{V}$ can be represented relative to the basis $\mathcal{B}_2$ as

$$\vec{\phi} = \sum_{i=1}^{N} \phi_i \vec{e}_i.$$

Notice, however, that $\vec{e}_i \cdot \vec{e}_j = \delta_{ij}\vec{e}_i$ for all $\vec{e}_i, \vec{e}_j \in \mathcal{B}_2$. This is certainly not the case for $\mathcal{B}_1$.

To compute the product of $f, g \in F[x]/\langle x^N \pm 1\rangle$, (*i.e.*, relative to the basis $\mathcal{B}_1$), $f(x)g(x)$ is represented by

$$\left(\sum_{i=0}^{N-1} f_i \vec{v}_i\right)\left(\sum_{j=0}^{N-1} g_j \vec{v}_j\right) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f_i g_j (x^{i+j} \bmod \langle x^N \pm 1\rangle), \quad (2)$$

which has a multiplicative complexity of $O(N^2)$. Instead, the product can be computed by mapping f, g under $\mathbf{V}$ to $\vec{\phi}, \vec{\gamma} \in F^N$ and forming the quantity

$$\left(\sum_{i=1}^{N} \phi_i \vec{e}_i\right)\left(\sum_{j=1}^{N} \gamma_j \vec{e}_j\right) = \sum_{i=1}^{N}\sum_{j=1}^{N} \phi_i \gamma_j \vec{e}_i \vec{e}_j. \quad (3)$$

The nature of the basis $\mathcal{B}_2$, however, allows Eq. 3 to be simplified to

$$\sum_{i=1}^{N}\sum_{j=1}^{N} \phi_i \gamma_j \delta_{ij} \vec{e}_i = \sum_{i=1}^{N} \phi_i \gamma_i \vec{e}_i. \quad (4)$$

Although the complexity of Eq. 3 is still $O(N^2)$, $N(N-1)$ of the multiplies are by zero, yielding an effective complexity of $O(N)$ (the non-zero multiplies are the $\phi_i\gamma_i$ in Eq. 4). This "decoupling" of the basis vectors in $\mathcal{B}_2$ (which is not shared by the basis $\mathcal{B}_1$) is what allows the reduced complexity. More significantly, this basis results in the *minimum* multiplicative complexity. To show this, the following theorem [Bla85], [Win75] is needed.

Theorem 4 *Let* $p(x)$, *a polynomial of degree* N, *be a product of* k *distinct prime polynomials. Every algorithm to compute the polynomial product* $s(x) = f(x)g(x) \bmod (p(x))$ *uses at least* $2N-k$ *multiplications.*

In our case, the polynomial $p(x) = x^N \pm 1$ is assumed to split into N distinct linear factors. Thus, no algorithm can compute the product of $f(x)$ and $g(x)$ in less than $2N - k = 2N - N = N$ multiplications. If $k < N$, there is no isomorphism between $F[x]/\langle x^N \pm 1\rangle$ and F^N and the multiplicative complexity will always be greater than N. It is precisely the factorization of $x^N \pm 1$ into distinct linear factors that allows the change of basis from $\mathcal{B}_1$ to $\mathcal{B}_2$. In turn, this new basis renders the multiplicative complexity as small as is possible.

Acknowledgements

This work was supported in part under NADC, ARO, and FHTIC funding.

References

[Bla85] Richard E. Blahut. *Fast Algorithms for Digital Signal Processing.* Addison-Wesley, Reading, Massachusetts, 1985.

[GOR87] Richard A. Games, S.D. O'Neil, and J.J. Rushanan. *Algebraic Integer Quantization and Conversion.* Technical Report, The MITRE Corporation, Bedford, Massachusetts, 1987.

[HW38] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, Oxford, U.K., 1938.

[Jac85] Nathan A. Jacobson. *Basic Algebra I.* W.H. Freeman and Company, New York, 1985.

[Lan84] Serge Lang. *Algebra.* Addison-Wesley, Reading, Massachusetts, second edition, 1984.

[MR79] J. H. McClellan and C. M. Rader. *Number Theory in Digital Signal Processing.* Prentice-Hall, Englewood Cliffs, New Jersey, 1979.

[Ska87] Alexander Skavantzos. *The Polynomial Residue Number System and its Applications.* PhD thesis, University of Florida, 1987.

[Win75] S. Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *IBM Research Report RC5669*, October 1975.