Finite Field Multiplication via Number-Theoretic Transforms

Edusmildo Orozco, Dorothy Bollman, Edgar Ferrer

eorozco@uprrp.edu
bollman@cs.uprm.edu
eferrer@cs.uprm.edu

University of Puerto Rico

Acknowledgement: This work was partially supported by a UPR-RP FIPI Grant

The 9*th* International Conference on Finite Fields and Their Applications

July 13–17, 2009, Dublin, Ir.

Introduction

- *Complex field:* If a and b are $m-$ degree polynomials, $a * b = a \otimes b$, $O(m^2)$. Convolution theorem: $a \otimes b = F^{-1}(F(\bar{a}) \odot F(\bar{b}))$, $O(m \log m)$.
- *Finite fields:* Can we use the same technique to multiply elements in $GF(p^m)$ represented in the polynomial basis?
- *Problems:*
  1. The DFT$\rightarrow$ NTT of length d exists over $GF(p)$ iff $d|p-1$.
  2. Reduction mod the irreducible polynomial defining $GF(p^m)$.
- *This talk:* Multiplication in $GF(p^m)$ defined by an irreducible trinomial $x^m - x^n - 1$ can be performed in $O(m \log m)$ time.

Useful concepts

- A matrix whose descending diagonals are constant is called *Toeplitz.*
- A Toeplitz matrix such that every row after the first is obtained by a right circular shift from the previous row is called *circulant.*
- Any $m \times m$ Toeplitz matrix can be embedded in an $L \times L$ *circulant* matrix, where $L \geq 2m - 1$.
- Let C be a circulant $n \times n$ matrix and let x be a vector of length n. Then $Cx = c \otimes x$, where c is the first column of C.

The Mastrovito matrix: $GF(2^m)$ defined by an irreducible trinomial $x^m + x^n + 1$

- Avoid polynomial mod reduction: convert $c = a * b \mod x^m + x^n + 1$ to $c = Zb$, where Z involves the coefficients of a.
- Extend Mastrovito's idea to $GF(p^m)$, p odd and $x^m - x^n - 1$ irreducible over $GF(p)$.

Polynomial multiplication as a matrix-vector product:

$$a * b = Mb, \text{ where}$$

$$M = \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & & & \vdots & & \vdots \\ a_{m-2} & a_{m-3} & a_{m-4} & \cdots & a_0 & 0 \\ a_{m-1} & a_{m-2} & a_{m-3} & \cdots & a_1 & 0 \\ 0 & a_{m-1} & a_{m-2} & \cdots & a_2 & a_1 \\ 0 & 0 & a_{m-1} & \cdots & a_3 & a_2 \\ \vdots & & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_{m-1} & a_{m-2} \\ 0 & 0 & 0 & \cdots & 0 & a_{m-1} \end{pmatrix}$$

Polynomial multiplication as a matrix-vector product: $a * b = Zb$

$$Z = \begin{pmatrix} M_0 + c_{m,0}M_m + c_{m+1,0}M_{m+1} + \cdots + c_{2m-2,0}M_{2m-2} \\ M_1 + c_{m,1}M_m + c_{m+1,1}M_{m+1} + \cdots + c_{2m-2,1}M_{2m-2} \\ \vdots \\ M_{m-1} + c_{m,m-1}M_m + c_{m+1,m-1}M_{m+1} + \cdots + c_{2m-2,m-1}M_{2m-2} \end{pmatrix},$$

where M_k is $k-th$ row of M and each $c_{i,j}$ satisfies

$$\alpha^i = c_{i,0} + c_{i,1}\alpha + \cdots + c_{i,m-1}\alpha^{m-1}.$$

A Toeplitz variant of the Mastrovito matrix

Lemma

If $GF(p^m)$ *is defined by an irreducible trinomial of the form* $x^m - x^n - 1$, *then* $Z' = \begin{pmatrix} \text{last } m \text{ rows of } Z \\ \text{first } n \text{ rows of } Z \end{pmatrix}$ *is Toeplitz.*

Remarks

i. Z' *is completely defined by its first row:*

$$M_n + c_{m,n}M_m + c_{m+1,n}M_{m+1} + \cdots + c_{2m-2,n}M_{2m-2}.$$

ii. *For odd* p, *coefficients* $c_{m+i,n}$ *are either* $0, 1,$ *or* 2.

A Fast Multiplication Algorithm

Theorem

Let $p = t2^k + 1$, t odd, be a prime and let m be such that $2^k \leq 2m - 1$. If $x^m - x^n - 1$ is irreducible over $GF(p)$ for some n, then the multiplication in $GF(p^m)$ can be performed with $O(m \log m)$ mod p operations.

Algorithm

0. Compute the size of the NTT: $L = 2^r$, where $r = 1 + \lceil \log_2 m \rceil$.
1. Compute the first column of Z':

$$a' = [a_n, a_{n+1}, \ldots, a_{m-1}, a_0, \ldots, a_{n-1}, \overbrace{0, \ldots, 0}^{L-(2m-n)}, s_1, \ldots, s_{m-1}].$$

2. $b' = b$ padded with $L - m$ zeros.
3. Compute $F^{-1}(F(a') \odot F(b'))$, where F denotes an NTT of size L.

Computation of s_i :

Case 1. $\frac{m}{2} \leq n < m \Rightarrow a'$ can be computed in $O(m \log m)$

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} + \begin{pmatrix} c_{m,n} & c_{m+1,n} & \cdots & c_{2m-2,n} \\ 0 & c_{m,n} & \cdots & c_{2m-3,n} \\ \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & c_{m,n} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{m-1} \end{pmatrix}$$

Computation of s_i :

Case 2. $1 \leq n < \frac{m}{2} \Rightarrow a'$ can be computed in $O(m)$

(a) For $n = 1$,

$$s_i = \begin{cases} a_i + a_{i+1}, & \text{if } 1 \leq i \leq m-2 \\ a_{m-1}, & \text{if } i = m-1 \end{cases}$$

(b) For $n > 1$,

$$s_i = \begin{cases} a_i + a_{n+i-1} + a_{m-n+i-1}, & \text{if } 1 \leq i \leq n \\ a_i + a_{n+i-1}, & \text{if } n < i \leq m-n \\ a_i + a_{i-(m-n)}, & \text{if } m-n \leq i \leq m-1 \end{cases}$$

Example

$GF(257^6)$ **defined by** $x^6 - x - 1$

- $p = 257 = 2^8 + 1$, $m = 6$, $n = 1 < \frac{m}{2}$.
- $a = [a_0, a_1, a_2, a_3, a_4, a_5]$, $b = [b_0, b_1, b_2, b_3, b_4, b_5]$ in $GF(257^6)$.
- Apply Algorithm 1 to compute $a * b$:
  0. Compute length of the NTT: $L = 2^{1+\lceil \log_2 6 \rceil} = 16$.
  1. Compute the first column of Z' :
     $a' = [a_1, a_2, a_3, a_4, a_5, a_0, 0, 0, 0, 0, 0, a_1 + a_2, a_2 + a_3, a_3 + a_4, a_4 + a_5, a_0 + a_5]$.
  2. Pad b with zeros:
     $b' = [b_0, b_1, b_2, b_3, b_4, b_5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$.
  3. Compute $c = a * b = F^{-1}(F(a') \odot F(b'))$.

Running time ratios for multiplication in $GF(65537)$ $x^m - x^n - 1$, $n < \frac{m}{2}$

m	NTT size	t_M / t_N	t_S / t_N
67	256	0.38	0.67
97	256	0.78	1.38
127	256	1.33	2.35
132	512	0.65	1.37
193	512	1.37	2.41
251	512	2.31	4.07
260	1024	1.13	1.99
390	1024	2.52	4.44
512	1024	2.37	7.63
516	2048	2.01	3.55
758	2048	4.33	7.65
1024	2048	7.88	13.9
1030	4096	3.68	6.50
2047	4096	14.50	25.50
2050	8192	6.72	11.90
4096	8192	27.00	47.30

Conclusions

1. Is there a criteria for determining, given an odd prime $p = t2^k + 1$ and $m \leq \frac{2^k+1}{2}$, whether or not there exists an $n < m$ such that $x^m - x^n - 1$ is irreducible over $GF(p)$?
2. Given any positive integer m_0, does there exists an integer $m > m_0$ and a prime $p = t2^k + 1$ such that $2^k \geq 2m - 1$ and $x^m - x^n - 1$ is irreducible over $GF(p)$ for some $n < m$?
3. For primes $3, 5, 17, 65537$, and 12287 we have performed extensive searches of irreducible trinomials $x^m - x^n - 1$. Except for $p = 3$ and $p = 5$ we have found numerous such polynomials. For instance, for $p = 65537$, $m \leq 1024$ and some $n < m$, we found 342. Out of these, 242 have the property that $n < \frac{m}{2}$.

References


S. Baktir and B. Sunar,*Achieving efficient polynomial multiplication in Fermat fields using the Fast Fourier Transform,* ACM Southeast Regional Conference Proceedings of the 44th annual Southeast regional conference, ACM Press, 2006, 549–554.


S. Baktir and B. Sunar,*Frequency Domain Finite Field Arithmetic for Elliptic Curve Cryptography,* ece.wpi.edu/ sunar/preprints/jrnl-paper.pdf


B. Sunar and C. K. Koc. *Mastrovito multiplier for all trinomials,* IEEE Transactions on Computers, 48(5):522-527, May 1999.


E. Ferrer, D. Bollman, and O. Moreno, *A Fast Finite Field Multiplier,* Reconfigurable Computing: Architectures, Tools and Applications, LNCS 4419, 2007, 238–246.


A. Halbutogullari, C. K. Koc, *Mastrovito Multiplier for General Irreducible Polynomials,* IEEE Transactions on Computers, Vol. 49, No 5, 503–518,2000.