CYCLIC CONVOLUTION ALGORITHMS OVER FINITE FIELDS: MULTIDIMENSIONAL CONSIDERATIONS†

Meghanad D. Wagh *   Salvatore D. Morgera

Concordia University, Department of Electrical Engineering
1455 de Maisonneuve Blvd. West, Montréal H3G 1M8
Québec, Canada

ABSTRACT

By making an example of the earlier proposed cyclic convolution algorithms, the computational efficiency of the multidimensional techniques over finite fields is investigated. It is shown that the multidimensional techniques are inferior to the directly designed algorithms for all lengths except when applied to lengths whose exponents are relatively prime. Relations between the complexities of the directly designed algorithms and those derived through the multidimensional techniques are also established in various cases.

1. INTRODUCTION

It is well known that some practically important algorithms (such as the discrete Fourier transform or the cyclic convolution algorithms) of large lengths can be constructed from small factor length algorithms using the multidimensional techniques [1,2,3]. This procedure, applicable when the factor lengths are relatively prime, is generally taken to be quite efficient and has a multiplicative complexity equal to the product of the multiplicative complexities of the factor algorithms.

Recently, the authors have developed cyclic convolution algorithms over finite fields [4]. These algorithms can be constructed for all lengths not divisible by the field characteristics. In this paper, we develop an expression for the multiplicative complexity of these algorithms of composite lengths. Then, making an example of these algorithms, we examine the efficiency of the multidimensional techniques to compute cyclic convolutions over finite fields.

We are able to show that for the multidimensional technique to be efficient, not only should the factor lengths be relatively prime, but so should be their <u>exponents</u> defined in terms of the field characteristics. Thus the efficiency of a multidimensional technique is also dependent upon the field over which the convolution is being computed.

2. COMPUTATIONAL COMPLEXITY

We assume here that the input vectors are from $GF(p^m)$ for an arbitrary m and the field of constants is $GF(p)$. $M(N)$ denotes the complexity‡ of the cyclic convolution of length N and $R(N)$, the complexity of multiplication of two $N-1$ degree (i.e., with N coefficients) polynomials. The exponent of an integer N with respect to a prime p $(p\nmid N)$ is defined as the smallest integer e such that $N|(p^e-1)$. For example, with respect to 2, the exponents of 3,5,7, and 9 are 2,4,3, and 6, respectively. When $N=N_1\cdot N_2$ with gcd $(N_1,N_2)=1$, N_1 and N_2 are called the factor lengths of N. The quantities e, e_1, and e_2 always denote the exponents of N, N_1, and N_2, respectively, with respect to the prime p determined by the field of constants $GF(p)$.

Further, the integers $\{j(p^e-1)/N,\ 1\le j\le N-1\}$ are partitioned into subsets $S_{i_1}, S_{i_2},\ldots$ A subset S_i is defined by the smallest element i (from the set $\{j(p^e-1)/N,\ 1\le j\le N-1\}$) not covered by previous subsets and is constructed as $S_i=\{i, ip, ip^2, \ldots\}$, where each element is evaluated modulo (p^e-1). The order of S_i, $|S_i|$, is denoted by σ_i and the set $\{i_1, i_2, \ldots\}$ containing the first element of each subset by S_N.

With this notation we then have [4]:

$$M(N) = 1 + \sum_{i\varepsilon S_N} R(\sigma_i) \qquad (1)$$

Obviously, to appreciate this expression one should look into the properties of the functions σ_i and $R(N)$. We list below some of the properties which are important for further analysis. The proofs of these properties are given in [6].

(P1) $R(s\cdot t) = R(s)\cdot R(t)$ for <u>any</u> integers s and t

(P2) $\sigma_i|e$ for all $i\varepsilon S_N$

(P3) For any N, at least for one $i\varepsilon S_N$, $\sigma_i=e$

(P4) For prime N, $\sigma_i=e$ for all $i\varepsilon S_N$.

(P5) $\sum_{i\varepsilon S_N} \sigma_i = N-1$

(P6) If $N=q^n$ where q is a prime (different from p), then any σ_i, $i\varepsilon S_N$, is of the type
$$\sigma_i = e'q^{\ell}$$
where e' is the exponent of q and ℓ is an integer $0\le\ell\le n-1$.

(P7) If $N=N_1\cdot N_2$ with $\gcd(N_1,N_2) = 1$, one can fully characterize the set
$$\Sigma \equiv \{\sigma_i | i\varepsilon S_N\} \text{ from the sets}$$
$$\Sigma_1 \equiv \{\sigma_{i_1} | i_1\varepsilon S_{N_1}\} \text{ and } \Sigma_2 \equiv \{\sigma_{i_2} | i_2\varepsilon S_{N_2}\}$$

First construct a set Σ' in which for every pair $\sigma_{i_1}\varepsilon\Sigma_1, \sigma_{i_2}\varepsilon\Sigma_2$, one has $\gcd(\sigma_{i_2},\sigma_{i_2})$ occurrences of $\mathrm{lcm}(\sigma_{i_1},\sigma_{i_2})$. Then

---

† This work was supported by NSERC Grant A0912.

* Now at Old Dominion University, Norfolk, VA 23508

‡ In this work, by complexity of an algorithm, we always mean the multiplicative complexity. In addition, the multiplications by the elements from the field of constants are not counted.

CH1610-5/81/0000-0327 $00.75 © 1981 IEEE

$\Sigma = \Sigma' \cup \Sigma_1 \cup \Sigma_2$.

For p=2, the set Σ (corresponding to N=9·25) can be obtained from the sets $\Sigma_1=\{6,2\}$ and $\Sigma_2=\{20,4\}$ (corresponding to $N_1=9$ and $N_2=25$); thus, Σ' has

gcd(6,20) = 2 occurrences of lcm(20,6) = 60
gcd(6,4) = 2 occurrences of lcm(6,4) = 12
gcd(2,20) = 2 occurrences of lcm(2,20) = 20 and
gcd(2,4) = 2 occurrences of lcm(2,4) = 4 or,

$\Sigma' = \{60,60,12,12,20,20,4,4\}$

Finally,

$\Sigma = \{60,60,12,12,20,20,4,4,6,2,20,4\}$

We end this section by giving the following lemma which illustrates the applicability of the properties (P1) through (P6).

Lemma 1: If N is prime with exponent e, then

$$M(N) = 1 + \frac{R(e)}{e}(N-1)$$

Proof: Using (P4) and (P5), $|S_N| = (N-1)/e$ for prime N. Also using (P4) in (1)

$$M(N) = 1 + R(e)\,|S_N|$$

which directly leads to the result. ∎

3. CENTRAL RESULT

We now examine the complexities of algorithms of composite lengths. Of particular importance is the following theorem which compares the complexity of the length $N_1 \cdot N_2$ algorithm generated directly with that of the same length algorithm generated from length N_1 and N_2 algorithms using multidimensional techniques.

Theorem 1: Given N_1 and N_2 relatively prime, with exponents e_1 and e_2, respectively,

$$M(N_1N_2) = M(N_1)\cdot M(N_2) \quad \text{if} \quad \gcd(e_1,e_2) = 1$$

and

$$M(N_1N_2) < M(N_1)\cdot M(N_2) \quad \text{if} \quad \gcd(e_1,e_2) > 1$$

Proof: We have from (1),

$$M(N_1N_2) = 1 + \sum_{i\varepsilon S_{N_1N_2}} R(\sigma_i)$$

$$= 1 + \sum_{i_1\varepsilon S_{N_1}} R(\sigma_{i_1}) + \sum_{i_2\varepsilon S_{N_2}} R(\sigma_{i_2})$$

$$+ \sum_{i_1\varepsilon S_{N_1}} \sum_{i_2\varepsilon S_{N_2}} [\gcd(\sigma_{i_1},\sigma_{i_2})\cdot R(\mathrm{lcm}(\sigma_{i_1},\sigma_{i_2})]$$

where use is made of (P7) to separate the σ_i, $i\varepsilon S_{N_1N_2}$ into three groups. Now,

$$R(\mathrm{lcm}(\sigma_{i_1},\sigma_{i_2}) = R\left(\frac{\sigma_{i_1}\sigma_{i_2}}{\gcd(\sigma_{i_1},\sigma_{i_2})}\right)$$

$$= \frac{R(\sigma_{i_1})\cdot R(\sigma_{i_2})}{R(\gcd(\sigma_{i_1},\sigma_{i_2}))} \quad \text{from (P1)}.$$

Using this, we obtain

$$M(N_1N_2) = 1 + \sum_{i_1\varepsilon S_{N_1}} R(\sigma_{i_1}) + \sum_{i_2\varepsilon S_{N_2}} R(\sigma_{i_2})$$

$$+ \sum_{i_1\varepsilon S_{N_1}} \sum_{i_2\varepsilon S_{N_2}} \frac{\gcd(\sigma_{i_1},\sigma_{i_2})}{R(\gcd(\sigma_{i_1},\sigma_{i_2}))}\cdot R(\sigma_{i_1})R(\sigma_{i_2})$$

But $M(N_1) = 1 + \sum_{i_1\varepsilon S_{N_1}} R(\sigma_{i_1})$

and $M(N_2) = 1 + \sum_{i_2\varepsilon S_{N_2}} R(\sigma_{i_2})$ giving

$$M(N_1N_2) = M(N_2) - 1$$

$$+ \sum_{i_1\varepsilon S_{N_1}} \sum_{i_2\varepsilon S_{N_2}} \frac{\gcd(\sigma_{i_1},\sigma_{i_2})}{R(\gcd(\sigma_{i_1},\sigma_{i_2}))} R(\sigma_{i_1})R(\sigma_{i_2}) \tag{2}$$

If

$\gcd(e_1,e_2) = 1$, from (P2),

$\gcd(\sigma_{i_1},\sigma_{i_2}) = 1$, for all $i_1\varepsilon S_{N_1}$, $i_2\varepsilon S_{N_2}$

Using the fact that R(1) = 1, we have in this case

$$M(N_1N_2) = M(N_1) + M(N_2) - 1$$

$$+ \sum_{i_1\varepsilon S_{N_1}} \sum_{i_2\varepsilon S_{N_2}} R(\sigma_{i_1})\, R(\sigma_{i_2})$$

$$= M(N_1)+M(N_2)-1+(M(N_1)-1)(M(N_2)-1) = M(N_1)\cdot M(N_2)$$

On the other hand, if $\gcd(e_1,e_2)>1$, at least for one $i_1\varepsilon S_{N_1}$ and $i_2\varepsilon S_{N_2}$, $\sigma_{i_1}=e_1$ and $\sigma_{i_2}=e_2$ from (P3). For this i_1,i_2 pair, the ratio

$$\frac{\gcd(\sigma_{i_1},\sigma_{i_2})}{R(\gcd(\sigma_{i_1},\sigma_{i_2}))} < 1.$$

as R(L)>L if L>1. Moreover, for other i_1,i_2 pairs,

$$\frac{\gcd(\sigma_{i_1},\sigma_{i_2})}{R(\gcd(\sigma_{i_1},\sigma_{i_2}))} \leq 1$$

Thus, in this case, the summation over i_1 and i_2 is strictly less than $(M(N_1)-1)\cdot(M(N_2)-1)$. As a result, we have

$$M(N_1N_2) < M(N_1)\cdot M(N_2)$$ ∎

Theorem 1 states that a directly designed convolution algorithm (with complexity $M(N_1N_2)$ is computationally superior to the one obtained through multidimensional techniques (with complexity $M(N_1)\cdot M(N_2)$). Using the properties (P1) through (P7), it is also possible to determine in many cases the exact value of $M(N_1N_2)$. This gives a clearer picture of the computational efficiency of the multidimensional techniques. The following two corollaries are typical amongst these results. The proofs of these corollaries may be found in [6].

Corollary 1 Let $N_1=p_1^n$ and $N_2=p_2^m$ where p_1 and p_2 are primes (different from p) with exponents e_1' and e_2', respectively. If

$\gcd(p_1^{n-1}, e_2') = 1$

and

$\gcd(p_2^{m-1}, e_1') = 1$

then

$$M(N_1N_2) = M(N_1)\cdot M(N_2) - \left(1 - \frac{\gcd(e_1',e_2')}{R(\gcd(e_1',e_2'))}\right)$$

$$\cdot\ (M(N_1)-1)(M(N_2)-1)$$

Corollary 2 Let $N_1=p_1^n$ and $N_2=p_2^m$ where p_1 and p_2 are primes (different from p) with exponents e_1' and e_2', respectively. If

$$p_1^{n-1} \mid e_2'$$

and

$$p_2^{m-1} \mid e_1'$$

Then

$$M(N_1N_2)=M(N_1)\cdot M(N_2)-[(M(N_1)-1)(M(N_2)-1)-(N_1-1)(N_2-1)\cdot\frac{R(\mathrm{lcm}(e_1',e_2'))}{\mathrm{lcm}(e_1',e_2')}]$$

Note that if either N_1 or N_2 is a prime, then one condition in each corollary is trivially satisfied and only one condition needs to be checked. Interestingly, if both N_1 and N_2 are prime, then both the conditions in both the corollaries are satisfied trivially and the same complexity would be obtained from either of the corollaries.

Tables I and II compare the computational complexity of the algorithms derived by the multidimensional techniques with those derived directly.

The ratio $M(N)/(M(N_1)M(N_2))$ in the last column of these tables allows one to determine the computational efficiency of the multidimensional techniques. It is possible to get an approximate idea of this ratio easily from the corollaries. For example, under the conditions of corollary 1,

$$\frac{M(N)}{M(N_1)M(N_2)} \simeq \frac{\gcd(e_1', e_2')}{R(\gcd(e_1', e_2'))},$$

and under the conditions of corollary 2,

$$\frac{M(N)}{M(N_1)M(N_2)} \simeq \frac{N_1}{M(N_1)}\cdot\frac{N_2}{M(N_2)}\cdot\frac{R(\mathrm{lcm}(e_1',e_2'))}{\mathrm{lcm}(e_1',e_2')}$$

Many more results in this direction may be obtained by making use of the principles developed earlier. We give below just two of these. The proofs of these corollaries may be found in [6].

<u>Corollary 3</u> If $N_1=p-1$, then the ratio

$$\frac{M(N)}{M(N_1)M(N_2)} = 1$$

<u>Corollary 4</u> If $N_1=p+1$ and N_2, a prime power q^n, then

$$\frac{M(N)}{M(N_1)M(N_2)} = 1 \text{ if } e_2 \text{ is odd}$$
$$\simeq N_1/M(N_1) \text{ if } e_2 \text{ is even}$$

In corollary 4, $M(N_1)$ equals $1+3p/2$ or $(3p+1)/2$ depending on whether p equals 2 or an odd prime. Both of these can be incorporated in $M(N_1)=1+\lfloor 3p/2\rfloor$ to refine $M(N_1N_2)$ to

$$M(N_1N_2) = N_1M(N_2) + \lfloor p/2\rfloor$$

This is an interesting expression because it shows that increasing the length N_1 times increases the multiplicative complexity by only N_1 times (approximately).

When N can be factored in more than one way, Theorem 1 can sometimes be used to determine the 'best' factorization for applying the multidimensional technique (factorization resulting in the least computational complexity) as the following corollary demonstrates:

<u>Corollary 5</u> If $N=N_1N_2\cdots N_r$ such that the factors are relatively prime pairwise and

$$\gcd(e_1,e_i) = 1 \quad \text{for } i=2,3,4,\ldots,r$$

then the 'best' factorization of N is

$$N = N_1\cdot(N_2N_3\cdots N_r)$$

To illustrate Corollary 5, consider N=595=5x7x41. If N is factored as 35x17, 119x5 or 85x7 one requires 7150, 7150 or 3640 multiplications for the cyclic convolution using multidimensional techniques over GF(2). The 'best' factorization 85x7 could have been predicted from Corollary 5, since the exponents of 5,7, and 17 are 4,3, and 8, respectively. Another example over GF(2) is that of N=1533=3x7x73 which calls for 15028, 15028 and 8116 multiplications using multidimensional techniques with N factored as 73x21, 219x7, and 511x3, respectively. Again the 'best' factorization 511x3 could be obtained from Corollary 5 since exponents 3,7 and 73 and 2,3, and 9, respectively. Over GF(3), one may consider N=2665=5x13x41. The exponents of 5,13, and 41 are 4,3, and 8, respectively, and accordingly, the factorization 205x13 is best. By actual evaluation, one finds that the multidimensional techniques call for 34000, 34000, and 17125 multiplications when N is factored as 533x5, 65x41, and 205x13, respectively.

4. CONCLUSIONS

In previous work [4], a structured design method for efficiently performing cyclic convolution over finite fields was presented. These algorithms are applicable to lengths not divisible by the field characteristic. In this paper, further results are obtained on the computational complexities of these new algorithms. It is already been shown in [4] that the directly designed new algorithms are more efficient than the conventional convolution algorithms [1,5]. Furthermore, it is now shown that the use of small size new algorithms and multidimensional techniques are inferior to the directly designed large algorithms except for lengths whose exponents are relatively prime. This result is contained in Theorem 1 of this paper. For specific cases, several corollaries are presented which express the multiplicative complexity of the large length algorithms in terms of the complexities of the factor length algorithms. Results related to the 'best' factorization in terms of computational complexity are presented. Finally, comparisons of multiplicative complexities of length N cyclic convolutions obtained directly, with those obtained through multidimensional techniques are made for N in the range of 10 to 6000 and fieldsof constants GF(2) and GF(3). These results illustrate the dependence of the efficiency of the multidimensional techniques on the field of constants. For example, for a convolution of length 455 over GF(2), the direct-to-multidimensional complexity ratio is 56%; whereas, over GF(3), it is 73%. Note that the direct approach offers considerable savings over both fields. In this example, the 'best' factorization turns out to be different for each field. In the case of length 55, the 'best' factorization is the same, and over GF(2), the ratio is 71%; whereas, both techniques are equivalent over GF(3). This work, in conjunction with the previous work [4] demonstrates that the direct approach should be used whenever possible, and isolates those cases when the multidimensional techniques are equivalent to the direct approach in complexity.

REFERENCES

[1] R.C.Agarwal and J.W. Cooley, "New algorithms for digital convolution," IEEE Trans. Acoust., Speech, Signal Processing, Vol. ASSP-25, pp. 392-410, Oct. 1977.

[2] S. Winograd, "On computing the discrete Fourier transform," Math Comput., Vol. 32, pp. 175-199, Jan. 1978.

[3] C.S. Burrus, "Index mappings for multidimensional formulation of the DFT and convolution," IEEE Trans. Acoust., Speech, Signal Processing, Vol. ASSP-25, pp. 239-242, June 1977.

[4] M.D. Wagh and S.D. Morgera, "Structured design method for convolutions over finite fields," IEEE Trans. Info. Theory, in review.

[5] R.C. Agarwal and C.S. Burrus, "Fast one dimensional convolution by multidimensional techniques," IEEE Trans. Acoust., Speech, Signal Processing, Vol. ASSP-22, pp. 1-10, Feb. 1974.

[6] M.D. Wagh and S.D. Morgera, "On the Multidimensional Techniques for Algorithms over Finite Fields," IEEE Trans. Acoust., Speech, and Sig. Proc., in review.

TABLE 1

A COMPARISON OF THE MULTIPLICATIVE COMPLEXITIES OF LENGTH N CYCLIC CONVOLUTION ALGORITHMS OBTAINED DIRECTLY, $M(N)$, AND THOSE OBTAINED THROUGH THE MULTIDIMENSIONAL TECHNIQUES, $M_D(N)$, OVER GF(2).

N	N_1	N_2	E_1	E_2	$M(N_1)$	$M(N_2)$	$M_D(N)$	$M(N)$	RATIO
15	5	3	4	2	10	4	40	31	.7778
33	11	3	10	2	49	4	196	148	.7551
35	7	5	3	4	13	10	130	130	1.0
51	17	3	8	2	55	4	220	166	.7545
55	11	5	10	4	49	10	490	346	.7061
85	17	5	8	4	55	10	550	280	.5091
91	13	7	12	3	55	13	715	391	.5469
93	31	3	5	2	97	4	388	388	1.0
117	13	9	12	6	55	22	1210	508	.4198
205	41	5	20	4	289	10	2890	1450	.5017
315	63	5	6	4	178	10	1780	1285	.7219
455	65	7	12	3	280	13	3640	2020	.5550
511	73	7	9	3	289	13	3757	2029	.5401
663	221	3	24	2	1405	4	5620	4216	.7502
765	85	9	8	6	280	22	6160	4207	.6830
949	73	13	9	12	289	55	15895	8119	.5108
1989	117	17	12	8	500	55	27940	12982	.4646
6643	949	7	36	3	8119	13	105547	56839	.5385

TABLE 2

A COMPARISON OF THE MULTIPLICATIVE COMPLEXITIES OF LENGTH N CYCLIC CONVOLUTION ALGORITHMS OBTAINED DIRECTLY, $M(N)$, AND THOSE OBTAINED THROUGH THE MULTIDIMENSIONAL TECHNIQUES, $M_D(N)$, OVER GF(3).

N	N_1	N_2	E_1	E_2	$M(N_1)$	$M(N_2)$	$M_D(N)$	$M(N)$	RATIO
10	5	2	4	1	10	2	20	20	1.0
20	5	4	4	2	10	5	50	41	.82
28	7	4	6	2	19	5	95	77	.8105
34	17	2	16	1	82	2	164	164	1.0
35	7	5	6	4	19	10	190	136	.7158
40	8	5	2	4	11	10	110	83	.7545
44	11	4	5	2	33	5	165	165	1.0
55	11	5	5	4	33	10	330	330	1.0
56	8	7	2	6	11	19	209	155	.7416
68	17	4	16	2	82	5	410	329	.8024
85	17	5	16	4	82	10	820	415	.5061
91	13	7	3	6	25	19	475	259	.5453
205	41	5	8	4	136	10	1360	685	.5037
455	91	5	6	4	259	10	2590	1888	.7290
656	41	16	8	4	136	29	3944	2189	.5550
697	41	17	8	16	136	82	11152	3457	.3100
5299	757	7	9	6	3025	19	57475	30259	.5265
6056	757	8	9	2	3025	11	33275	33275	1.0