INFORMATION AND COMPUTATION 78, 171–177 (1988)

A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases

TOSHIYA ITOH AND SHIGEO TSUJII

Department of Electrical and Electronic Engineering, Faculty of Engineering, Tokyo Institute of Technology, Tokyo 152, Japan

This paper proposes a fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. Normal bases have the following useful property: In the case that an element x in $GF(2^m)$ is represented by normal bases, 2^k power operation of an element x in $GF(2^m)$ can be carried out by k times cyclic shift of its vector representation. C. C. Wang *et al.* proposed an algorithm for computing multiplicative inverses using normal bases, which requires $(m-2)$ multiplications in $GF(2^m)$ and $(m-1)$ cyclic shifts. The fast algorithm proposed in this paper also uses normal bases, and computes multiplicative inverses iterating multiplications in $GF(2^m)$. It requires at most $2[\log_2(m-1)]$ multiplications in $GF(2^m)$ and $(m-1)$ cyclic shifts, which are much less than those required in the Wang's method. The same idea of the proposed fast algorithm is applicable to the general power operation in $GF(2^m)$ and the computation of multiplicative inverses in $GF(q^m)$ $(q=2^n)$.

1. INTRODUCTION

Finite field arithmetic is widely used in various fields, such as coding theory and cryptography and so on. Most of public-key cryptosystems are constructed over finite fields of large order, hence their running-time of encryption and decryption is dominated by multiplication and division. Therefore, it is very important in a practical sense to develop a fast algorithm for carrying out such operations.

This paper proposes a fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. C. C. Wang *et al.* proposed an algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases, which requires $(m-2)$ multiplications in $GF(2^m)$ and $(m-1)$ cyclic shifts. The algorithm proposed in this paper also uses normal bases in $GF(2^m)$, and requires at most $2[\log_2(m-1)]$ ($[x]$: Gauss' symbol) multiplications in $GF(2^m)$ and $(m-1)$ cyclic shifts to compute multiplicative inverses in $GF(2^m)$. It is also shown that the same idea of the proposed algorithm is applicable to the computation of multiplicative inverses in $GF(q^m)$ $(q=2^n)$.

0890-5401/88 $3.00

2. Preliminaries

Definition (MacWilliams and Sloane, 1979). A normal basis of $GF(q^m)$ $(q=2^n)$ over $GF(q)$ is a basis of the form

$$a, a^q, a^{q^2}, ..., a^{q^{m-1}}, \tag{1}$$

where "a" is a non-zero element in $GF(q^m)$ $(q=2^n)$. (#)

Lemma 1 (Itoh and Tsujii, 1986). *Let an element x in* $GF(q^m)$ $(q=2^n)$ *be represented by a normal basis* (Eq. (1)) *in the form*

$$x = x_0 a + x_1 a^q + \cdots + a_{m-1} a^{q^{m-1}} = [x_0, x_1, ..., x_{m-1}], \tag{2}$$

where $\{a, a^q, ..., a^{q^{m-1}}\}$: *normal bases over* $GF(q)$. *Then,* x^{q^k} *can be computed by k cyclic shifts of Eq.* (2) *such that*

$$x^{q^k} = [x_{m-k}, x_{m-k+1}, ..., x_{m-1}, x_0, ..., x_{m-k-1}]. \tag{3}$$

We call the cyclic shift in Eq. (3) "cyclic shift over $GF(q)$" in the rest of this paper.

Lemma 2 (MacWilliams and Sloane, 1979). *Every element e in* $GF(q^m)$ $(q=2^n)$ *satisfies the identity*

$$e^{q^m} = e. \tag{4}$$

3. The Wang's Method

(Wang *et al.*, 1985). A non-zero element x in $GF(2^m)$ has an unique multiplicative inverse x^{-1}. Since the non-zero element x also satisfies Lemma 2, i.e., $x^{2^m} = x$, x^{-1} is given by $x^{-1} = x^{2^m-2}$. Here 2^m-2 can be represented by $2^m - 2 = 2 + 2^2 + \cdots + 2^{m-1}$, hence x^{-1} can be computed by

$$x^{-1} = (x^2)(x^{2^2}) \cdots (x^{2^{m-1}}). \tag{5}$$

The following algorithm shows the procedure of computing Eq. (5).

Algorithm 1.

S1. $y := x$
S2. for $k := 1$ to $m-2$ do
S3. begin
S4. $z := y^2$ (one cyclic shift)
S5. $y := zx$ (multiplication in $GF(2^m)$)
S6. end
S7. $y := y^2$ (one cyclic shift)
S8. write y

By Lemma 1 and Algorithm 1, computing Eq. (5) requires $(m-2)$ multiplications in $\mathrm{GF}(2^m)$ and $(m-1)$ cyclic shifts over $\mathrm{GF}(2)$.

4. Proposed Fast Algorithm in $\mathrm{GF}(2^m)$

By Lemma 1, we have the following theorem.

Theorem 1. *Let x be a non-zero element in* $\mathrm{GF}(2^m)$ $(m=2^r+1)$. *Then, there exists an algorithm for computing x^{-1}, which requires*

number of multiplications in $\mathrm{GF}(2^m)$: $\mathrm{NM}=\log_2(m-1)=r$,

number of cyclic shifts over $\mathrm{GF}(2)$: $\mathrm{NS}=m-1=2^r$.

Proof. Represent 2^m-2 in binary form:

$$2^m-2=(\underbrace{1,1,...,1}_{m-1},0), \qquad \text{where} \quad m-1=2^r, \tag{6}$$

and define the following symbols to simplify the notation:

$$>t=(\underbrace{1,1,...,1}_{t}), \tag{7}$$

$$\wedge\, t=(\underbrace{1,1,...,1}_{2^t}), \tag{8}$$

$$\hat{\hat{}}\, t=2^t, \tag{9}$$

$$\uparrow t=2^{2^t}. \tag{10}$$

Let M_t and S_t be the number of multiplications in $\mathrm{GF}(2^m)$ and cyclic shifts over $\mathrm{GF}(2)$ to compute $x^{\wedge t}$ $(1\leqslant t\leqslant r)$, respectively. Since $x^{\wedge t}=(x^{\wedge(t-1)})^{(\uparrow(t-1))}(x^{\wedge(t-1)})$, we have $M_t=M_{t-1}+1$ and $S_t=S_{t-1}+2^{t-1}$, where $M_0=S_0=0$. Hence $M_r=r$ and $S_r=2^r-1$, and thus

$$NM=M_r=r=\log_2(m-1), \tag{11}$$

$$NS=S_r+1=2^r=m-1, \tag{12}$$

because $x^{-1}=(x^{\wedge r})^2$. ∎

Theorem 1 can be described by

Algorithm 2.

S1. $y:=x$
S2. for $k:=0$ to $r-1$ do
S3. begin
S4. $z:=y^{2^{2^k}}$ (2^k cyclic shifts)
S5. $y:=yz$ (multiplication in $\mathrm{GF}(2^m)$)
S6. end
S7. $y:=y^2$ (multiplicaton in $\mathrm{GF}(2^m)$)
S8. write y.

The following theorem is the generalization of Theorem 1.

THEOREM 2. *Let x be a non-zero element in* $\mathrm{GF}(2^m)$. *Then, there exists an algorithm for computing x^{-1}, which requires*

number of multiplications in $\mathrm{GF}(2^m)$:
$\mathrm{NM} = [\log_2(m-1)] + H_w(m-1) - 1 \leqslant 2[\log_2(m-1)]$,
number of cyclic shifts over $\mathrm{GF}(2)$: $\mathrm{NS} = m-1$,

where $[\ ] =$ *Gauss' symbol and* $H_w(\ ) =$ *Hamming weight.*

Proof. x^{-1} can be computed by

$$x^{-1} = (x^{>(m-1)})^2. \tag{13}$$

Suppose that $m-1$ is represented by

$$m-1 = \sum_{s=1}^{t} 2^{k_s}, \qquad \text{where} \quad k_1 > k_2 > \cdots > k_t, \tag{14}$$

and so we have

$$x^{-1} = \{(x^{\wedge k_1})^{\hat{\wedge} e_1}(x^{\wedge k_2})^{\hat{\wedge} e_2} \cdots (x^{\wedge k_t})^{\hat{\wedge} e_t}\}^2, \tag{15}$$

where $e_s = \sum_{i=s+1}^{t} 2^{k_i}$ and $e_t = 0$.

Reordering the terms in Eq. (15),

$$x^{-1} = \{(x^{\wedge k_t})\{(x^{\wedge k_{t-1}}) \cdots ((x^{\wedge k_2})(x^{\wedge k_1})^{\uparrow k_2})^{\uparrow k_3} \cdots\}^{\uparrow k_t}\}^2. \tag{16}$$

Let $M(k_1)$ and $S(k_1)$ be the number of multiplications in $\mathrm{GF}(2^m)$ and cyclic shifts over $\mathrm{GF}(2)$ to compute $x^{\wedge k_1}$, respectively. Here we have $M(k_1) = k_1$ and $S(k_1) = 2^{k_1} - 1$. Since every term $x^{\wedge k_s}$ $(2 \leqslant s \leqslant n)$ is already computed in the procedure of computing $x^{\wedge k_1}$ (see proof of Theorem 1), we have $\mathrm{NM} = k_1 + n - 1$ and $\mathrm{NS} = 2^{k_1} - 1 + \sum_{s=2}^{n} 2^{k_s} + 1$. By the the fact that $[\log_2(m-1)] = k_1$ and $H_w(m-1) = n$, thus

$$\mathrm{NM} = [\log_2(m-1)] + H_w(m-1) - 1 \leqslant 2[\log_2(m-1)], \tag{17}$$

$$\mathrm{NS} = \sum_{s=1}^{n} 2^{k_s} = m-1. \quad \blacksquare \tag{18}$$

A result similar to that of Theorem 2 has been found independently by S. A. Vanstone (1987).

5. EXAMPLE

The following example confirms Theorem 2:

Let x be a non-zero element in $\mathrm{GF}(2^{11})$. Here x^{-1} is given by $x^{-1} = x^{2^{11}-2} = x^{2046}$, hence x^{-1} can be computed by the following procedure:

S1. $(x)^2 = x^2$: 1 cyclic shift over GF(2)
S2. $x^2 x = x^3$: 1 multiplication in $\mathrm{GF}(2^{11})$
S3. $(x^3)^{2^2} = x^{12}$: 2 cyclic shifts over GF(2)
S4. $x^{12} x^3 = x^{15}$: 1 multiplication in $\mathrm{GF}(2^{11})$
S5. $(x^{15})^{2^4} = x^{240}$: 4 cyclic shifts over GF(2)
S6. $x^{240} x^{15} = x^{255}$: 1 multiplication in $\mathrm{GF}(2^{11})$
S7. $(x^{255})^{2^2} = x^{1020}$: 2 cyclic shifts over GF(2)
S8. $x^{1020} x^3 = x^{1023}$: 1 multiplication in $\mathrm{GF}(2^{11})$
S9. $(x^{1023})^2 = x^{2046}$: 1 cyclic shift over GF(2)
$= x^{-1}$

Observing the above procedure, the number of multiplications in $\mathrm{GF}(2^{11})$ and cyclic shifts over GF(2) are as follows:

4 multiplications (in $\mathrm{GF}(2^{11})$) in S2, S4, S6, and S8,

10 cyclic shifts (over GF(2)) in S1, S3, S5, S7, and S9.

On the other hand, since $[\log_2(11-1)] = 3$ and $H_w(11-1) = 2$, we have $\mathrm{NM}(= [\log_2(11-1)] + H_w(11-1) - 1) = 4$ and $\mathrm{NS}(= 11-1) = 10$, and this example confirms Theorem 2.

6. Proposed Fast Algorithm in $\mathrm{GF}(q^m)$ $(q = 2^n)$

This section shows a fast algorithm for computing multiplicative inverses in $\mathrm{GF}(q^m)$ $(q = 2^n)$ using normal bases.

THEOREM 3. *Let x be a non-zero element in* $\mathrm{GF}(q^m)$ $(q = 2^n)$. *Then, there exists an algorithm for computing x^{-1}, which requires*

number of multiplications in $\mathrm{GF}(q^m)$:
$$\mathrm{NM}_1(m) = [\log_2(m-1)] + H_w(m-1),$$
number of cyclic shifts over $\mathrm{GF}(q)$: $\mathrm{NS}_1(m) = m - 1$,

number of multiplications in $\mathrm{GF}(q)$ $(q = 2^n)$:
$$\mathrm{NM}_2(n) = [\log_2(n-1)] + H_w(n-1) - 1,$$
number of cyclic shifts over GF(2): $\mathrm{NS}_2(n) = n - 1$,

where [ ] = *Gauss' symbol and* $H_w(\ )$ = *Hamming weight.* ∎

Proof. For a non-zero element x in $\mathrm{GF}(q^m)$ $(q = 2^n)$, x^{-1} is given by $x^{-1} = x^{q^m - 2}$. Here $q^m - 2$ can be decomposed by

$$q^m - 2 = (q-2) \sum_{i=0}^{m-1} q^i + \sum_{j=1}^{m-1} q^j. \tag{19}$$

For the simplicity of the notation, define $a = \sum_{i=0}^{m-1} q^i$ and $b = \sum_{j=1}^{m-1} q^j$, and we have $x^{-1} = y^{(p-2)}z$, where $y = x^a$ and $z = x^b$. Note that $y = zx$. Applying the similar procedure in Section 4 (proof of Theorem 2), $\mathrm{NM}_1(m)$ (number of multiplications in $\mathrm{GF}(q^m)$) and $\mathrm{NS}_1(m)$ (number of cyclic shifts over $\mathrm{GF}(q)$) to compute z and y are

$$\mathrm{NM}_1(m) = [\log_2(m-1)] + H_w(m-1), \tag{20}$$

$$\mathrm{NS}_1(m) = m-1. \tag{21}$$

Since y is norm of x (Lidl and Niederreiter, 1983), y is an element of $\mathrm{GF}(q)$. Hence, $y^{q-2} = y^{-1}$, and by Theorem 2, $\mathrm{NM}_2(n)$ (number of multiplications in $\mathrm{GF}(q)$ $(q = 2^n)$) and $\mathrm{NS}_2(n)$ (number of cyclic shifts over $\mathrm{GF}(2)$) to compute $y^{-1} (= y^{q-2} = y^{2^n-2})$ are

$$\mathrm{NM}_2(n) = [\log_2(n-1)] + H_w(n-1) - 1, \tag{22}$$

$$\mathrm{NS}_2(n) = n-1. \quad \blacksquare \tag{23}$$

7. Conclusions

A fast algorithm for computing multiplicative inverses in $\mathrm{GF}(2^m)$ using normal basis has been proposed. This algorithm requires at most $2[\log_2(m-1)]$ multiplications in $\mathrm{GF}(2^m)$ and $(m-1)$ cyclic shifts over $\mathrm{GF}(2)$ to compute multiplicative inverses, which are much less than those required in the Wang's method. The algorithm proposed in this paper computes multiplicative inverses in $\mathrm{GF}(2^m)$ by iterating multiplications in $\mathrm{GF}(2^m)$ and cyclic shifts over $\mathrm{GF}(2)$ in turn. Hence, the number of cyclic shifts is reduced to $[\log_2(m-1)] + H_w(m-1)$, using special hardware which carries out k cyclic shifts over $\mathrm{GF}(2)$ in one machine cycle (Itoh and Tsujii, 1986). It has been also shown that the same idea of the proposed algorithm in $\mathrm{GF}(2^m)$ is applicable to the computation of multiplicative inverses in $\mathrm{GF}(q^m)$ $(q = 2^n)$. It is clear that the computation of multiplicative inverses in $\mathrm{GF}(p^m)$ (p: odd prime) can be carried out similarly in the case of $\mathrm{GF}(q^m)$ $(q = 2^n)$ (Itoh and Tsujii, 1986).

Furthermore, an idea similar to the proposed algorithm can be applied to general power operation in $\mathrm{GF}(2^m)$, which was pointed out by S. A. Vanstone (1987).

Acknowledgments

The authors wish to thank Professor S. A. Vanstone of the University of Waterloo for his valuable discussions.

Received July 8, 1987; accepted January 12, 1988

REFERENCES

ITOH, T., AND TSUJII, S. (1986), "A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^t)$ Using Normal Bases," Paper of Technical Group, TGIT86-44, pp. 31–36, IECE, Japan.

LIDL, R., AND NIEDERREITER, H. (1983), "Finite Fields," Addison–Wesley, Reading, MA.

MACWILLIAMS, F. J., AND SLOANE, N. J. A. (1979), "The Theory of Error-Correcting Codes," North-Holland, Amsterdam.

VANSTONE, S. A. (1987), Unpublished manuscript, lecture at NTT.

WANG, C. C., TRUONG, T. K., SHAO, H. M., DEUTSCH, L. J., OMURA, J. K., AND REED, I. R. (1985), VLSI architectures for computing multiplications and inverses in $GF(2^m)$, *IEEE Trans. Comput.* **C-34**, No. 8, 709–716.