Appl. Math. and Comp. Sci., 1998, Vol.8, No.3, 671–680

COMPUTING IN THE COMPOSITE $GF(q^m)$ OF CHARACTERISTIC 2 FORMED BY MEANS OF AN IRREDUCIBLE BINOMIAL

CZESŁAW KOŚCIELNY*

Since the operation of reduction modulo a polynomial needed for parallel computing in $GF(q^m)$ is the simplest possible in the case of a binomial, in this paper the main properties of irreducible binomials over $GF(q)$ of characteristic 2 are given. It is shown that $P(x) = x^m - P_0$ is irreducible over $GF(q)$ for $q = 2^s$, $s > 1$ if $m \geq 3$ divides $q - 1$. The method of performing all multiplicative operations in $GF(q^m)$ of characteristic 2 (multiplication, rising to an arbitrary power, multiplicative inversion) formed by means of an irreducible polynomial is also presented. The use of irreducible binomials may be attractive for those engineers and researches who deal with implementation of hardware and microprogrammed devices for computing in $GF(q^m)$, even if m and q are large.

1. Introduction

Computations in finite fields are important in such domains as error-control coding, signal processing, switching theory and cryptography, and it is now discussed from the point of view of developing efficient algorithms and parallel architectures for performing such computations. In this paper, the author shows how to determine irreducible binomials over certain composite Galois fields of characteristic 2 and presents the question of applying such binomials for implementing multiplicative operations in finite fields (since addition is trivial, only multiplicative operations are considered here). It is obvious that the operation of reduction modulo an irreducible binomial, needed for computing in $GF(q^m)$, is the simplest possible in comparison with reduction modulo irreducible polynomials having more than two terms. Therefore, the application of irreducible binomials as field polynomials remarkably simplifies algorithms in finite field arithmetics. The method presented here is applicable when $q = 2^s$, $s > 1$ and if $m \geq 3$ divides $q - 1$. This case is rather frequent (e.g. the desired conditions are fulfilled for more than 41% of all $GF(2^s)$, $2 \leq s \leq 128$). Since the roots of any irreducible binomial over a composite $GF(q)$ of characteristic 2 are linearly dependent, only the canonical basis of $GF(q^m)$ over $GF(q)$ is considered in the paper.

The author is of the opinion that the use of irreducible binomials can have some influence on the application research concerning implementation of hardware and micro-programmed devices of various structure and configuration for performing operations in large and huge finite fields of characteristic 2.

* Technical University of Zielona Góra, Department of Robotics and Software Engineering, ul. Podgórna 50, 65–246 Zielona Góra, Poland, e-mail: ckos@irio.pz.zgora.pl.

2. Finite Field Arithmetic in $GF(q^m)$ for $q=2^s$, $s>1$, $m\geq 3$ and $m\,|\,(q-1)$

Although the existence of irreducible binomials over finite fields was proved in the nineteenh century (Serret, 1866) and several irreducible binomials over composite Galois fields of characteristic 2 were probably calculated and noticed years ago (e.g. two such binomials are listed in Green and Taylor, 1974), the author has not found any paper regarding a possibility of their application. Thus, to initiate this practical question, the following theorem is formulated:

Theorem 1. *Let*

$$q = 2^s, \quad s > 1, \quad m \mid (q-1), \quad m \geq 3 \tag{1}$$

Then the binomial

$$P(x) = x^m - P_0 \tag{2}$$

where P_0 denotes an arbitrary primitive element of $GF(q)$, is irreducible over $GF(q)$.

Proof. To prove this theorem, it suffices to show that non-null elements of $GF(q)$ are not roots of the binomial (2). Let ω denote a primitive element of $GF(q^m)$, and α be a primitive element of $GF(q)$. Thus $\alpha = \omega^{(q^m-1)/(q-1)}$. The equation $P(\alpha^k) = 0$, where $0 \leq k \leq q-2$, has a solution if and only if $(\alpha^k)^m = \alpha$, viz. if $m\,k \equiv 1$ (mod $q-1$). It follows from the elementary number theory that this is impossible because $(m, q-1) > 1$. Therefore the roots of (2) are not elements of $GF(q)$ and this binomial is irreducible over $GF(q)$. ■

Corollary 1. *The binomial (2), belonging to the exponent $e = m(q-1)$, is the minimum function $m_{(q^m-1)/e}(x)$ for the element $\beta \in GF(q^m)$, where*

$$\beta = \omega^{1/m} \sum_{k=0}^{m-1} q^k \tag{3}$$

It should be noted that Theorem 1 is a particular case of a more general theorem proved by Serret (1866), where a field with characteristic ≥ 2 is considered and the term P_0 may also have an order different from $q-1$.

To discuss how to perform operations in $GF(q^m)$ constructed by means of an irreducible binomial, let the polynomials over $GF(q)$

$$\begin{aligned} A(x) &= A_0 + A_1 x + \cdots + A_{m-1} x^{m-1} \\ B(x) &= B_0 + B_1 x + \cdots + B_{m-1} x^{m-1} \end{aligned} \tag{4}$$

be two arbitrary elements of $GF(q^m)$, and let

$$\begin{aligned} PD(x) &= PD_0 + PD_1 x + \cdots + PD_{m-1} x^{m-1} \\ SQ(x) &= SQ_0 + SQ_1 x + \cdots + SQ_{m-1} x^{m-1} \end{aligned} \tag{5}$$

denote the product of elements (4) and the square of $A(x)$, respectively. It is clear that (5) is computed according to

$$\begin{aligned} PD(x) &\equiv A(x)B(x) \quad (\mathrm{mod}\ P(x)) \\ SQ(x) &\equiv (A(x))^2 \quad (\mathrm{mod}\ P(x)) \end{aligned} \tag{6}$$

over $GF(q)$, where $P(x)$ is as in Theorem 1.

The author determined (5) for $m = 3, 5, \ldots, 13$ and observed that the components of $PD(x)$ and $SQ(x)$ can be expressed as simply as in the following theorem:

Theorem 2. *Let q and m satisfy the conditions of Theorem 1. Then, for any odd $m > 1$ the operations of multiplication and squaring in $GF(q^m)$ are described by means of the equations*

$$PD_i = \sum_{j+k=i} A_j B_k + \sum_{j+k=m+i} A_j B_k P_0 \tag{7}$$

for $i, j, k \in \{0, 1, \ldots, m-1\}$,

$$\begin{aligned} SQ_{2i} &= A_i^2 && \text{for } i \in \{0, 1, \ldots, (m-1)/2\} \\ SQ_{2i+1} &= A_{(m+1)/2+i}^2 P_0 && \text{for } i \in \{0, 1, \ldots, (m-3)/2\} \end{aligned} \tag{8}$$

The proof by induction of eqns. (7) and (8) is omitted.

The direct writing out of (7) and (8) for $m = 3$ and $m = 5$ reveals their astonishing simplicity and regularity:

$$\begin{aligned} PD_0 &= A_0B_0 + A_2B_1P_0 + A_1B_2P_0 \\ PD_1 &= A_1B_0 + A_0B_1 + A_2B_2P_0 \\ PD_2 &= A_2B_0 + A_1B_1 + A_0B_2 \end{aligned} \tag{9}$$

$$\begin{aligned} SQ_0 &= A_0^2 \\ SQ_1 &= A_2^2 P_0 \\ SQ_2 &= A_1^2 \end{aligned} \tag{10}$$

$$\begin{aligned} PD_0 &= A_0B_0 + A_4B_1P_0 + A_3B_2P_0 + A_2B_3P_0 + A_1B_4P_0 \\ PD_1 &= A_1B_0 + A_0B_1 + A_4B_2P_0 + A_3B_3P_0 + A_2B_4P_0 \\ PD_2 &= A_2B_0 + A_1B_1 + A_0B_2 + A_4B_3P_0 + A_3B_4P_0 \\ PD_3 &= A_3B_0 + A_2B_1 + A_1B_2 + A_0B_3 + A_4B_4P_0 \\ PD_4 &= A_4B_0 + A_3B_1 + A_2B_2 + A_1B_3 + A_0B_4 \end{aligned} \tag{11}$$

$$\begin{aligned}SQ_0 &= A_0^2\\ SQ_1 &= A_3^2P_0\\ SQ_2 &= A_1^2\\ SQ_3 &= A_4^2P_0\\ SQ_4 &= A_2^2\end{aligned} \tag{12}$$

As is known, formulae (7) and (8) can be successfully used in designing both efficient algorithms and compact hardware or micro-programed devices for performing all multiplicative operations in a composite $GF(q^m)$ of characteristic 2 satisfying the conditions of Theorem 1, under the assumption that one has a possibility of carrying out all the operations in $GF(q)$. The operation of inversion in $GF(q^m)$ can be either realized as the $(q^m - 2)$-th power of an element or, alternatively, calculated from (7) as described in what follows. Let

$$\begin{aligned}INV(x) &\equiv 1/A(x) \pmod{P(x)}\\ INV(x) &= INV_0 + INV_1x + \cdots + INV_{m-1}\,x^{m-1}\end{aligned} \tag{13}$$

denote the inverse of a non-null $A(x)$. Then by substituting $B(x) = INV(x)$ into (7) and taking into account that $A(x)\,INV(x) = 1$, the system of linear equations over $GF(q)$

$$M\begin{bmatrix} INV_0\\ INV_1\\ \vdots\\ INV_{m-1}\end{bmatrix} = \begin{bmatrix}1\\ 0\\ \vdots\\ 0\end{bmatrix} \tag{14}$$

is obtained, where M is an $m \times m$ matrix with elements being functions in A_i and P_0. The solution of (14) directly yields the components of (13).

In some cases, by applying algorithms for efficient polynomial multiplication (Knuth, 1981; Sedgewick, 1990), a considerable reduction in the number of gates in the implemented hardware is possible when compared with the straightforward approach. The reduction results from saving some multiplications in $GF(q)$ at the cost of extra additions. For example, in (9) one must compute nine different products A_iB_j. By rewriting these equations in the form

$$\begin{aligned}PD_0 &= ((A_1 + A_2)(B_1 + B_2) + A_1B_1 + A_2B_2)P_0 + A_0B_0\\ PD_1 &= (A_0 + A_1)(B_0 + B_1) + A_1B_1 + A_0B_0 + A_2B_2P_0\\ PD_2 &= (A_0 + A_2)(B_0 + B_2) + A_0B_0 + A_2B_2\end{aligned}$$

the number of needed different products A_iB_j can be reduced to six (A_0B_0, A_1B_1, A_2B_2, $(A_1 + A_2)(B_1 + B_2)$, $(A_0 + A_1)(B_0 + B_1)$, $(A_0 + A_2)(B_0 + B_2)$).

3. Example

As an example, a problem of computing a product, a square, powers from 2 to 5 and an inverse in a composite $GF(q^3)$ of characteristic 2 is presented. Thus now $P(x) = x^3 + P_0$, P_0 is a primitive element of $GF(q)$, and the polynomials $A(x) = A_0+A_1x+A_2x^2$, $B(x) = B_0+B_1x+B_2x^2$ represent two arbitrary elements of $GF(q^3)$.

Let

$$\begin{aligned} PD(x) &\equiv A(x)B(x) && (\text{mod } P(x)) = PD_0 + PD_1x + PD_2x^2 \\ SQ(x) &\equiv (A(x))^2 && (\text{mod } P(x)) = SQ_0 + SQ_1x + SQ_2x^2 \\ CUB(x) &\equiv (A(x))^3 && (\text{mod } P(x)) = CUB_0 + CUB_1x + CUB_2x^2 \\ DG4(x) &\equiv (A(x))^4 && (\text{mod } P(x)) = DG4_0 + DG4_1x + DG4_2x^2 \\ DG5(x) &\equiv (A(x))^5 && (\text{mod } P(x)) = DG5_0 + DG5_1x + DG5_2x^2 \\ INV(x) &\equiv 1/A(x) && (\text{mod } P(x)) = INV_0 + INV_1x + INV_2x^2 \end{aligned} \tag{15}$$

denote the product of two elements, the first four powers and the inverse of $A(x)$, respectively, in any $GF(q^3)$ of characteristic 2 satisfying (1). Since now $m = 3$, a product and a square in $GF(q^3)$ may be computed from (9) and (10). By assuming that $B(x) = SQ(x)$ and substituting it into (9), the formula for rising to the third power in $GF(q^3)$ can be obtained:

$$\begin{aligned} CUB_0 &= A_0^3 + A_1^3P_0 + A_2^3P_0^2 \\ CUB_1 &= A_0^2A_1 + A_0A_2^2P_0 + A_1^2A_2P_0 \\ CUB_2 &= A_0A_1^2 + A_0^2A_2 + A_1A_2^2P_0 \end{aligned} \tag{16}$$

Similarly, by applying properly (9) and (10), one gets

$$\begin{aligned} DG4_0 &= A_0^4 \\ DG4_1 &= A_1^4P_0 \\ DG4_2 &= A_2^4P_0^2 \end{aligned} \tag{17}$$

and

$$\begin{aligned} DG5_0 &= A_0^5 + A_1^4A_2P_0^2 + A_1A_2^4P_0^3 \\ DG5_1 &= A_0^4A_1 + A_0A_1^4P_0 + A_2^5P_0^3 \\ DG5_2 &= A_0^4A_2 + A_1^5P_0 + A_0A_2^4P_0^2 \end{aligned} \tag{18}$$

When applying (9) for computing the components of inversion over $GF(q^3)$, one must substitute $B(x) = INV(x)$ and $PD(x) = 1$ in (9), which yields the following system of linear equations with unknowns INV_0, INV_1 and INV_2:

$$\begin{bmatrix} A_0 & A_2P_0 & A_1P_0 \\ A_1 & A_0 & A_2P_0 \\ A_2 & A_1 & A_0 \end{bmatrix} \begin{bmatrix} INV_0 \\ INV_1 \\ INV_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \tag{19}$$

The solution of (19) gives

$$\begin{aligned} INV_0 &= D_0/D \\ INV_1 &= D_1/D \\ INV_2 &= D_2/D \end{aligned} \tag{20}$$

where

$$D = \begin{vmatrix} A_0 & A_2P_0 & A_1P_0 \\ A_1 & A_0 & A_2P_0 \\ A_2 & A_1 & A_0 \end{vmatrix}, \quad D_0 = \begin{vmatrix} 1 & A_2P_0 & A_1P_0 \\ 0 & A_0 & A_2P_0 \\ 0 & A_1 & A_0 \end{vmatrix} \tag{21}$$

$$D_1 = \begin{vmatrix} A_0 & 1 & A_1P_0 \\ A_1 & 0 & A_2P_0 \\ A_2 & 0 & A_0 \end{vmatrix}, \quad D_2 = \begin{vmatrix} A_0 & A_2P_0 & 1 \\ A_1 & A_0 & 0 \\ A_2 & A_1 & 0 \end{vmatrix} \tag{22}$$

and finally

$$\begin{aligned} INV_0 &= (A_0^2 + A_1A_2P_0)/(A_0^3 + A_1^3P_0 + A_2^3P_0^2 + A_0A_1A_2P_0) \\ INV_1 &= (A_0A_1 + A_2^2P_0)/(A_0^3 + A_1^3P_0 + A_2^3P_0^2 + A_0A_1A_2P_0) \\ INV_2 &= (A_1^2 + A_0A_2)/(A_0^3 + A_1^3P_0 + A_2^3P_0^2 + A_0A_1A_2P_0) \end{aligned} \tag{23}$$

In (16)–(23) the variables A_i, B_i, P_0 are elements of $GF(q)$ and all the operations are performed on these variables over $GF(q)$. The parameter q may be arbitrarily chosen, but under the assumption that the condition (1) is fulfilled.

To explain the method in detail, suppose that $q = 4$ and that the implementation of operations in $GF(4^3)$ is to be made. In this case, modules for performing all the operations in $GF(4)$ are needed. Therefore, one ought to design an adder, a multiplier, non-trivial scalers (multipliers by a constant greater than 1), a squarer and an inverter in $GF(4)$. The field $GF(4)$ is formed by means of the unique primitive polynomial of degree 2 over $GF(2)$

$$p(x) = x^2 + x + 1$$

and two elements $a, b \in GF(4)$ can be represented as two-dimensional vectors over $GF(2)$,

$$a = [a_0\, a_1], \quad b = [b_0\, b_1]$$

corresponding to the polynomials

$$a(x) = a_0 + a_1x, \quad b(x) = b_0 + b_1x$$

In order to simplify the notation for further consideration, let us assume now that $GF(4) = \langle\{0,1,2,3\},+,\cdot\rangle$, where $0 = [00]$, $1 = [10]$, $2 = [01]$ and $3 = [11]$. The tables of addition and multiplication in $GF(4)$, according to this notation, are given in Table 1.

Table 1. Tables of operations in $GF(4)$.

+	0 1 2 3	·	0 1 2 3
0	0 1 2 3	0	0 0 0 0
1	1 0 3 2	1	0 1 2 3
2	2 3 0 1	2	0 2 3 1
3	3 2 1 0	3	0 3 1 2

It can be easily seen that in $GF(4)$ with a canonical basis a multiplier, a squarer, an inverter, a multiplier by 2 and a multiplier by 3 are determined by the equations

$$\begin{aligned} pd(x) &\equiv a(x)b(x) && \pmod{p(x)} = pd_0 + pd_1 x \\ sq(x) &\equiv (a(x))^2 && \pmod{p(x)} = sq_0 + sq_1 x \\ inv(x) &\equiv 1/a(x) && \pmod{p(x)} = inv_0 + inv_1 x \\ mb2(x) &\equiv xa(x) && \pmod{p(x)} = mb2_0 + mb2_1 x \\ mb3(x) &\equiv (x+1)a(x) && \pmod{p(x)} = mb3_0 + mb3_1 x \end{aligned} \tag{24}$$

which correspond to the vector notation

$$\begin{aligned} a \cdot b &= [pd_0 \;\; pd_1] \\ a^2 &= [sq_0 \;\; sq_1] \\ 1/a &= [inv_0 \;\; inv_1] \\ 2 \cdot a &= [mb2_0 \;\; mb2_1] \\ 3 \cdot a &= [mb3_0 \;\; mb3_1] \end{aligned} \tag{25}$$

where

$$\begin{aligned} pd_0 &= a_0 b_0 + a_1 b_1 \\ pd_1 &= a_0 b_1 + a_1 b_0 + a_1 b_1 \\ sq_0 &= inv_0 = mb2_1 = mb3_0 = a_0 + a_1 \\ sq_1 &= inv_1 = mb2_0 = a_1 \\ mb3_1 &= a_0 \end{aligned} \tag{26}$$

The operations of addition and multiplication in (26) are performed, of course, over $GF(2)$.

To apply (16)–(20) and (23) in the particular case under consideration, one must take into account that $q = 4$. This implies the following substitutions into (16)–(20) and (23):

$$P_0 = 2, \quad P_0^2 = 2^2 = 3, \quad P_0^3 = 2^3 = 1, \quad A_i^4 = A_i, \quad A_i^5 = A_i^2 \tag{27}$$

where 2 and 3 denote, according to the notation introduced, elements of $GF(4)$, which are both primitive. One should also remember that

$$\forall\beta\in GF(4)\quad \beta^3=\begin{cases}1 & \text{if}\,\beta\neq 0\\ 0 & \text{if}\,\beta=0\end{cases}\tag{28}$$

which means that the operation of rising a variable to the third power in $GF(4)$ may be simply implemented by one two-input OR gate. After substitution of (27) into (16)–(20) and (23), they can be directly used to a logical design of the desired devices for performing operations in $GF(4^3)$.

In order to make it possible for the reader to verify the formulae for computing in $GF(4^3)$, the multiplicative group of $GF(4^3)$ is shown in Table 2.

Table 2. Multiplicative group of $GF(4^3)$ (field polynomial: x^3+2 over $GF(4)$, primitive element of $GF(4^3)$: $\omega = 1+\alpha^2$, α is a root of the field polynomial).

$\omega^0=[100]$	$\omega^1=[101]$	$\omega^2=[120]$	$\omega^3=[221]$	$\omega^4=[103]$	$\omega^5=[112]$	$\omega^6=[323]$
$\omega^7=[030]$	$\omega^8=[130]$	$\omega^9=[031]$	$\omega^{10}=[111]$	$\omega^{11}=[330]$	$\omega^{12}=[233]$	$\omega^{13}=[321]$
$\omega^{14}=[002]$	$\omega^{15}=[032]$	$\omega^{16}=[102]$	$\omega^{17}=[133]$	$\omega^{18}=[022]$	$\omega^{19}=[312]$	$\omega^{20}=[121]$
$\omega^{21}=[200]$	$\omega^{22}=[202]$	$\omega^{23}=[230]$	$\omega^{24}=[332]$	$\omega^{25}=[201]$	$\omega^{26}=[223]$	$\omega^{27}=[131]$
$\omega^{28}=[010]$	$\omega^{29}=[210]$	$\omega^{30}=[012]$	$\omega^{31}=[222]$	$\omega^{32}=[110]$	$\omega^{33}=[311]$	$\omega^{34}=[132]$
$\omega^{35}=[003]$	$\omega^{36}=[013]$	$\omega^{37}=[203]$	$\omega^{38}=[211]$	$\omega^{39}=[033]$	$\omega^{40}=[123]$	$\omega^{41}=[232]$
$\omega^{42}=[300]$	$\omega^{43}=[303]$	$\omega^{44}=[310]$	$\omega^{45}=[113]$	$\omega^{46}=[302]$	$\omega^{47}=[331]$	$\omega^{48}=[212]$
$\omega^{49}=[020]$	$\omega^{50}=[320]$	$\omega^{51}=[023]$	$\omega^{52}=[333]$	$\omega^{53}=[220]$	$\omega^{54}=[122]$	$\omega^{55}=[213]$
$\omega^{56}=[001]$	$\omega^{57}=[021]$	$\omega^{58}=[301]$	$\omega^{59}=[322]$	$\omega^{60}=[011]$	$\omega^{61}=[231]$	$\omega^{62}=[313]$

This group has been generated according to

$$\omega^i=[A_{i,0}\;A_{i,1}\;A_{i,2}],\qquad i=0,1,\ldots,62\tag{29}$$

where

$$(1+x^2)^i\equiv A_{i,0}+A_{i,1}x+A_{i,2}x^2\pmod{x^3+2}\tag{30}$$

is computed over $GF(4)$ by using Table 1, since α^2+1 is a primitive element of $GF(4^3)$ (α is a root of the field polynomial).

It is possible to proceed in a similar manner if $q=4^k$, $k=2,3,\ldots$, no matter how large q is, provided that one is capable of performing all the operations in $GF(q)$. However, if $q\geq 16$, then there are many possible representations of this field and, accordingly, many equivalent circuits or algorithms with a different degree of complexity can be designed.

From a practical point of view it is important to examine the degree of complexity of the multiplicative operations in the fields $GF(q^m)$ formed by means of an irreducible binomial and an irreducible trinomial. Generally, this question seems to be difficult, but the case of $GF(4^3)$ can be analysed. It can be verified that the simplest trinomial over $GF(4)$, $F(x) = x^3 + x + 1$, is irreducible and belongs to the exponent 7. By using this trinomial to form $GF(4^3)$, one can get the following equivalents of eqns. (9), (10), (16)–(18) and (23), respectively:

$$\begin{aligned} PD_0 &= A_0B_0 + A_2B_1 + A_1B_2 \\ PD_1 &= A_1B_0 + A_0B_1 + A_2B_1 + A_1B_2 + A_2B_2 \\ PD_2 &= A_2B_0 + A_1B_1 + A_0B_2 + A_2B_2 \end{aligned} \tag{31}$$

$$\begin{aligned} SQ_0 &= A_0^2 \\ SQ_1 &= A_2^2 \\ SQ_2 &= A_1^2 + A_2^2 \end{aligned} \tag{32}$$

$$\begin{aligned} CUB_0 &= A_0^3 + A_1^3 + A_1A_2^2 + A_2^3 \\ CUB_1 &= A_0^2A_1 + A_1^3 + A_1^2A_2 + A_0A_2^2 + A_1A_2^2 \\ CUB_2 &= A_0A_1^2 + A_0^2A_2 + A_1^2A_2 + A_0A_2^2 + A_1A_2^2 + A_2^3 \end{aligned} \tag{33}$$

$$\begin{aligned} DG4_0 &= A_0 \\ DG4_1 &= A_1 + A_2 \\ DG4_2 &= A_1 \end{aligned} \tag{34}$$

$$\begin{aligned} DG5_0 &= A_0^2 + A_1^2 + A_1A_2 + A_2^2 \\ DG5_1 &= A_1^2 + A_0A_2 + A_2^2 \\ DG5_2 &= A_0A_1 + A_1^2 + A_0A_2 \end{aligned} \tag{35}$$

$$\begin{aligned} INV_0 &= (A_0^2 + A_1^2 + A_1A_2 + A_2^2)/D \\ INV_1 &= (A_0A_1 + A_2^2)/D \\ INV_2 &= (A_1^2 + A_0A_2 + A_2^2)/D \end{aligned} \tag{36}$$

where

$$D = A_0^3 + A_0A_1^2 + A_1^3 + A_0A_1A_2 + A_0A_2^2 + A_1A_2^2 + A_2^3 \tag{37}$$

The comparison of (31)–(36) with the formulae obtained by means of the proposed method is left to the reader who can also verify the correctness of (31)–(36) using Tables 1 and 3.

Table 3. Multiplicative group of $GF(4^3)$ (field polynomial: x^3+x+1 over $GF(4)$, primitive element of $GF(4^3)$: $\omega = 1+2\,\alpha$, α—a root of the field polynomial).

$\omega^0=[100]$	$\omega^1=[120]$	$\omega^2=[103]$	$\omega^3=[033]$	$\omega^4=[122]$	$\omega^5=[231]$	$\omega^6=[020]$
$\omega^7=[023]$	$\omega^8=[130]$	$\omega^9=[111]$	$\omega^{10}=[313]$	$\omega^{11}=[211]$	$\omega^{12}=[003]$	$\omega^{13}=[113]$
$\omega^{14}=[021]$	$\omega^{15}=[202]$	$\omega^{16}=[102]$	$\omega^{17}=[212]$	$\omega^{18}=[110]$	$\omega^{19}=[132]$	$\omega^{20}=[223]$
$\omega^{21}=[300]$	$\omega^{22}=[310]$	$\omega^{23}=[302]$	$\omega^{24}=[022]$	$\omega^{25}=[311]$	$\omega^{26}=[123]$	$\omega^{27}=[010]$
$\omega^{28}=[012]$	$\omega^{29}=[320]$	$\omega^{30}=[333]$	$\omega^{31}=[232]$	$\omega^{32}=[133]$	$\omega^{33}=[002]$	$\omega^{34}=[332]$
$\omega^{35}=[013]$	$\omega^{36}=[101]$	$\omega^{37}=[301]$	$\omega^{38}=[131]$	$\omega^{39}=[330]$	$\omega^{40}=[321]$	$\omega^{41}=[112]$
$\omega^{42}=[200]$	$\omega^{43}=[230]$	$\omega^{44}=[201]$	$\omega^{45}=[011]$	$\omega^{46}=[233]$	$\omega^{47}=[312]$	$\omega^{48}=[030]$
$\omega^{49}=[031]$	$\omega^{50}=[210]$	$\omega^{51}=[222]$	$\omega^{52}=[121]$	$\omega^{53}=[322]$	$\omega^{54}=[001]$	$\omega^{55}=[221]$
$\omega^{56}=[032]$	$\omega^{57}=[303]$	$\omega^{58}=[203]$	$\omega^{59}=[323]$	$\omega^{60}=[220]$	$\omega^{61}=[213]$	$\omega^{62}=[331]$

4. Conclusion

A remarkable simplification resulting from the use of binomials as field polynomials makes it possible to easily implement any multiplicative operation in a class $GF(q^m)$ satisfying (1), even for higher q and m. Equations (7) and (8), describing multiplications and squaring in $GF(q^m)$, which may be used to realize any multiplicative operation (e.g. exponentiation to an arbitrary power by applying the repeated square-and-multiply method), are regular, very simple and slowly grow versus m.

Although the method proposed is applicable for both software and hardware implementations, in the author's opinion it can be almost directly used in designing micro-programmed devices of different structures or microprocessor systems for performing operations in large and huge composite finite fields. However, to make the method suitable for a VLSI implementation, one ought to resolve many practical questions.

References

Green D.H. and Taylor I.S. (1974): *Irreducible polynomials over composite Galois fields and their applications in coding techniques.* — Proc. IEEE, Vol.121, No.9, pp.935–939.

Knuth D.E. (1981): *The Art of Computer Programming. Volume 2: Seminumerical algorithms.* — Reading: Addison-Wesley.

Sedgewick R. (1990): *Algorithms in C.* — Reading: Addison-Wesley.

Serret J.A. (1866): *Cours d'algèbre supérieure.* — Paris: Gauthier-Villars.

Received: 11 October 1996
Revised: 12 June 1997