ACTA ARITHMETICA
XLVII (1986)

A polynomial representation for logarithms in GF(q)

by

GARY L. MULLEN (University Park, Pa.) and DAVID WHITE (Logan, Ut.)

1. Introduction. Let $F_q = \mathrm{GF}(q)$ denote the finite field of order $q = p^n$ where p is prime and $n \geqslant 1$. The field F_q may be viewed as the set of all polynomials in α of degree $< n$ with coefficients in F_p where α is a root of an irreducible polynomial of degree n over F_p. If $c \in F_q$ is a primitive element and $\beta \in F_q^*$, the multiplicative group of nonzero elements of F_q, then $\beta = c^k$ for some $0 \leqslant k \leqslant q-2$ and we say that k is the logarithm of β to the base c, denoted by $\log_c \beta = k$. Hence the logarithm function is a homomorphism from the multiplicative group F_q^* onto the additive group Z_{q-1} of integers modulo $q-1$.

In this paper we explicitly determine the coefficients of a polynomial $P_c(x) \in F_q[x]$ with the property that if $\beta \in F_q^*$ and

$$P_c(\beta) = \sum_{i=0}^{n-1} a_i \alpha^i \quad \text{for some } (a_0, \ldots, a_{n-1}) \in F_p^n \tag{1}$$

then

$$\log_c \beta = \sum_{i=0}^{n-1} a_i p^i. \tag{2}$$

In particular if $P_c(x) = \sum_{i=0}^{q-1} b_i x^i$ then

$$b_i = \begin{cases} -\sum_{j=0}^{n-1} \alpha^j & \text{if } i = 0, \\ \sum_{j=0}^{n-1} \dfrac{\alpha^j}{c^{p^j(q-1-i)} - 1} & \text{if } 1 \leqslant i \leqslant q-2, \\ 0 & \text{if } i = q-1. \end{cases} \tag{3}$$

In the special case when $n = 1$ we have

$$\log_c \beta = -1 + \sum_{i=1}^{p-2} (c^{p-1-i} - 1)^{-1} \beta^i \quad \text{for all } \beta \in F_p^*. \tag{4}$$

This is in contrast to previous work on the problem of computing logarithms in finite fields, the so called discrete logarithm problem, which has focused on producing efficient algorithms for the computation of logarithms. As indicated in [2] the problem of computing logarithms in finite fields has applications in a variety of areas. Some of these areas include the key distribution problem for encipherment systems as described by Diffie and Hellman in [4], authentication and verification schemes, and in communications where the problem of determining the number of cycles between two states of a linear feedback shift register is equivalent to the computation of logarithms in an appropriate finite field.

In particular, Pohlig and Hellman in [11] describe a cryptographic scheme which is secure if and only if the computation of logarithms in the field F_p is infeasible. In [12] Scholtz and Welch studied a multiple access code and in [9] Merkle and Hellman constructed a public-key distribution system, both of which require the computation of logarithms in the field F_p.

Numerous authors have studied the discrete logarithm problem. Adleman [1] and Pohlig and Hellman [11] studied algorithms for computing logarithms in F_p while Coppersmith [3], Knuth [6], [7], and Blake, Fuji-Hara, Mullin, and Vanstone [2] studied algorithms for computing logarithms in fields of characteristic two.

The approach in this paper is upon the construction of an explicit formula for the logarithm of any element in F_q^*, rather than on the construction of an algorithm for the computation of logarithms as in the above papers.

2. Preparatory results. We now prove several lemmas which, while having straightforward proofs, will be very useful in the sequel.

LEMMA 1. *If $b\in F_{p^n}$ and $b^{p^i}\neq 1$ then*

$$\sum_{j=0}^{p-1} j(b^{p^i})^j = -b^{p^i}(b^{p^{i+1}}-1)/(b^{p^i}-1)^2.$$

Proof. If $b\neq 1$ then from the calculus of finite differences, see for example [10], p. 41,

$$\sum_{j=1}^{p-1} jb^j = \frac{pb^p}{b-1}-\frac{b^{p+1}-b}{(b-1)^2} = \frac{-b(b^p-1)}{(b-1)^2}.$$

The lemma now follows by substituting b^{p^i} for b.

LEMMA 2. *If $b\in F_{p^n}$ and $b^{p^i}\neq 1$ then*

$$\sum_{j=0}^{p-1} (b^{p^i})^j = (b^{p^{i+1}}-1)/(b^{p^i}-1).$$

Proof. If $x\neq 1$ then $\sum_{i=0}^{m} x^i = (x^{m+1}-1)/(x-1)$.

LEMMA 3. *If $b\in F_{p^n}$ and $b^{p^i}\neq 1$ then*

$$\sum_{(a_0,\dots,a_{n-1})\in F_p^n} a_i b^{a_0+\dots+a_{n-1}p^{n-1}} = -b^{p^i}/(b^{p^i}-1). \tag{5}$$

Proof. Let N_i denote the left-hand side of (5). Then

$$N_i = \sum_{a_0\in F_p} b^{a_0}\dots\sum_{a_i\in F_p} a_i(b^{p^i})^{a_i}\dots\sum_{a_{n-1}\in F_p}(b^{p^{n-1}})^{a_{n-1}}.$$

By repeated use of Lemma 2 we have

$$N_i = \frac{b^{p^n}-1}{b^{p^{i+1}}-1}\sum_{a_0\in F_p} b^{a_0}\dots\sum_{a_i\in F_p} a_i(b^{p^i})^{a_i}$$

which by Lemma 1 and Lemma 2 becomes

$$N_i = -b^{p^i}(b^{p^n}-1)/(b-1)(b^{p^i}-1).$$

But $b\in F_{p^n}$ so that $b^{p^n}=b$ and hence

$$N_i = -b^{p^i}/(b^{p^i}-1).$$

3. Construction of the polynomial. By the Lagrange Interpolation Formula for finite fields, every function $f\colon F_q\to F_q$ can be uniquely represented by a polynomial of degree $<q$ with coefficients in F_q; i.e. there exists a unique polynomial $P(x)\in F_q[x]$ of degree $<q$ such that $P(\beta)=f(\beta)$ for all $\beta\in F_q$. The polynomial $P(x)$ can be written in the form

$$P(x) = \sum_{\beta\in F_q} f(\beta)[1-(x-\beta)^{q-1}].$$

It is easy to check that if $q=p^n$ then the binomial coefficient

$$\binom{q-1}{i}\equiv(-1)^i \pmod p \quad \text{for} \quad i=0,1,\dots,q-1$$

so that we may rewrite $P(x)$ as

$$P(x) = \sum_{i=0}^{q-1} b_i x^i$$

where

$$b_i = \begin{cases} f(0) & \text{if } i=0,\\ -\sum_{\beta\in F_q} f(\beta)\beta^{q-1-i} & \text{if } 1\leqslant i\leqslant q-1. \end{cases} \tag{6}$$

Let $c\in F_{p^n}$ be a primitive element so that if $\beta\in F_q^*$ then $\beta=c^k$ for some $0\leqslant k\leqslant q-2$ and $\log_c\beta=k$. We wish to construct a polynomial $P_c(x)\in F_q[x]$ with the property that if $P_c(\beta)=\sum_{i=0}^{n-1} a_i\alpha^i$ for some

$(a_0, \ldots, a_{n-1}) \in F_p^n$ then $\log_c \beta = \sum_{i=0}^{n-1} a_i p^i$. Moreover, we want $P_c(0) = (p-1)\sum_{i=0}^{n-1} \alpha^i$ so that $P_c(x)$ is a permutation of F_q.

Suppose $P_c(x) = \sum_{i=0}^{q-1} b_i x^i \in F_q[x]$. Clearly $b_0 = P_c(0) = (p-1)\sum_{i=0}^{n-1} \alpha^i$. Since no permutation of F_q can have degree dividing $q-1$ we have $b_{q-1} = 0$. Moreover from (6)

$$b_i = -\sum_{\beta \in F_q^*} f(\beta)\beta^{q-1-i}, \quad 1 \leqslant i \leqslant q-2.$$

In order to sum over all $\beta \in F_q^*$, we may sum over all $(a_0, \ldots, a_{n-1}) \in F_p^n$ such that $0 \leqslant \sum_{i=0}^{n-1} a_i p^i \leqslant q-2$, i.e. we may sum over all $(a_0, \ldots, a_{n-1}) \in F_p^n$ except $(p-1, \ldots, p-1)$. Thus for $1 \leqslant i \leqslant q-2$ we have

$$b_i = -\sum_{\substack{(a_0,\ldots,a_{n-1})\in F_p^n \\ \neq (p-1,\ldots,p-1)}} c^{(a_0+\ldots+a_{n-1}p^{n-1})(q-1-i)}[a_0+\ldots+a_{n-1}\alpha^{n-1}].$$

Hence if we let $b = c^{q-1-i}$ to simplify the notation, we obtain

$$b_i = -\Big[\sum_{(a_0,\ldots,a_{n-1})\in F_p^n} b^{a_0+\ldots+a_{n-1}p^{n-1}}[a_0+\ldots+a_{n-1}\alpha^{n-1}]\Big]-1-\ldots-\alpha^{n-1}$$

which may be rewritten as

$$b_i = -\sum_{j=0}^{n-1}\alpha^j \sum_{(a_0,\ldots,a_{n-1})\in F_p^n} a_j b^{a_0+\ldots+a_{n-1}p^{n-1}} - \sum_{j=0}^{n-1}\alpha^j, \quad 1 \leqslant i \leqslant q-2.$$

By Lemma 3 with $j = 0, 1, \ldots, n-1$ we get

$$b_i = \sum_{j=0}^{n-1}\frac{\alpha^j b^{p^j}}{b^{p^j}-1} - \sum_{j=0}^{n-1}\alpha^j = \sum_{j=0}^{n-1}\frac{\alpha^j}{b^{p^j}-1}, \quad 1 \leqslant i \leqslant q-2.$$

Since $b = c^{q-1-i}$, we finally get

$$b_i = \begin{cases} -\sum_{j=0}^{n-1}\alpha^j & \text{if } i = 0, \\ \sum_{j=0}^{n-1}\dfrac{\alpha^j}{c^{p^j(q-1-i)}-1} & \text{if } 1 \leqslant i \leqslant q-2, \\ 0 & \text{if } i = q-1, \end{cases} \tag{6}$$

so that we may state

THEOREM 4. *Suppose $c \in F_q$ is a primitive element, $\beta \in F_q^*$, and*

$$P_c(\beta) = \sum_{j=0}^{n-1} a_j \alpha^j \quad \textit{for some } (a_0, \ldots, a_{n-1}) \in F_p^n$$

where the coefficients of $P_c(x)$ are given by (6). Then

$$\log_c \beta = \sum_{j=0}^{n-1} a_j p^j. \tag{7}$$

The following corollary is of interest in its own right.

COROLLARY 5. *If $q = p$ an odd prime, $c \in F_p$ is a primitive element, and $\beta \in F_p^*$, then*

$$\log_c \beta = -1 + \sum_{i=1}^{p-2}(c^{p-1-i}-1)^{-1}\beta^i. \tag{8}$$

The next corollary illustrates several interesting properties of the coefficients of the polynomial representing $\log_c x$ in the field F_p, p an odd prime.

COROLLARY 6. *If p is an odd prime and $c \in F_p$ is a primitive element then*

(i) $b_i + b_{p-1-i} = p-1$ *for* $0 \leqslant i \leqslant p-1$,

(ii) $b_{(p-1)/2} = (p-1)/2$,

(iii) $\{b_0, b_1, \ldots, b_{p-1}\} = F_p$,

(iv) *If m is a positive divisor of $p-1$, let $\mathscr{C}(c, m)$ denote the set of coefficients in $P_c(x)$ corresponding to those exponents that are divisible by m. If c_1 is another primitive element of F_p, then $\mathscr{C}(c_1, m) = \mathscr{C}(c, m)$.*

Proof. Cases (i) and (ii) are easy and for case (iii), suppose that for $0 < i, j < p-1$ with $i < j$ we have $b_i = b_j$. Then $c^{p-1-i} = c^{p-1-j}$ so that $c^{j-i} = 1$, a contradiction since c is a primitive element in F_p. To prove (iv), for a fixed primitive element c, consider c^{p-1-i} for each $0 \leqslant i \leqslant p-2$. If c_1 is another primitive element so that $c_1 = c^k$ with $(k, p-1) = 1$, then the set of elements c_1^{p-1-j} for $0 \leqslant j \leqslant p-2$ runs through F_p^* and hence for each i there exists a unique j such that $c_1^{p-1-j} = c^{p-1-i}$. Suppose that $c_1 = c^k$ with $(k, p-1) = 1$ so that if m is a positive divisor of $p-1$ then $(k, m) = 1$. Thus we have $c^{k(p-1-j)-(p-1-i)} = 1$ so that $i - kj \equiv 0 \pmod{p-1}$ and hence $i - kj \equiv 0 \pmod{m}$. Thus $i = kj + ms$ for some integer s so that since $(k, m) = 1$, we have that m divides i if and only if m divides j. Hence we have shown that $a = (c^{p-1-i}-1)^{-1} \in \mathscr{C}(c, m)$ if and only if $a \in \mathscr{C}(c_1, m)$.

4. Illustrations. As an illustration of the above theory consider the field $F_4 = \{0, 1, \alpha, \alpha+1\}$ where $\alpha^2 = \alpha+1$. Let c be a primitive element so that $c = \alpha$ or $c = \alpha+1$. Clearly $b_0 = 1+\alpha$ and $b_3 = 0$ while from (6)

$$b_i = \frac{1}{c^{3-i}-1} + \frac{\alpha}{c^{2(3-i)}-1}, \quad i = 1, 2.$$

If $c = \alpha$ then $b_1 = 0$ and $b_2 = \alpha+1$ so that

$$P_\alpha(x) = (\alpha+1)x^2+(\alpha+1).$$

Hence

$$P_\alpha(1) = 0 \quad \text{so that} \quad \log_\alpha 1 = 0\cdot 2+0 = 0,$$
$$P_\alpha(\alpha) = 1 \quad \text{so that} \quad \log_\alpha \alpha = 0\cdot 2+1 = 1,$$
$$P_\alpha(\alpha+1) = \alpha \quad \text{so that} \quad \log_\alpha(\alpha+1) = 1\cdot 2+0 = 2.$$

If $c = \alpha+1$ then $P_{\alpha+1}(x) = (\alpha+1)x+(\alpha+1)$ so that

$$\log_{\alpha+1}(1) = 0, \quad \log_{\alpha+1}(\alpha) = 2, \quad \text{and} \quad \log_{\alpha+1}(\alpha+1) = 1.$$

As an illustration of the results in Corollaries 5 and 6 let $p = 7$ and $c = 3$. Then we have

$$\log_3 x = 4x^5+x^4+3x^3+5x^2+2x+6.$$

Similarly if $c = 5$ we obtain

$$\log_5 x = 2x^5+5x^4+3x^3+x^2+4x+6$$

so that

$$\mathscr{C}(3, 1) = F_7 = \mathscr{C}(5, 1),$$
$$\mathscr{C}(3, 2) = \{0, 1, 5, 6\} = \mathscr{C}(5, 2),$$
$$\mathscr{C}(3, 3) = \{0, 3, 6\} = \mathscr{C}(5, 3),$$
$$\mathscr{C}(3, 6) = \{0, 6\} = \mathscr{C}(5, 6).$$

Acknowledgment. The authors would like to thank the referee for several helpful comments which strengthened the statement of Corollary 6. Thanks are also due Gerald McKenna for use of his finite field software package and Tung Dang for computer assistance.

References

[1] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with application to cryptography*, Proc. IEEE 20th Annual Symposium on Foundations of Computer Science, 1979, pp. 55–60.

[2] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, *Computing logarithms in finite fields of characteristic two*, Siam. J. Alg. Disc. Meth. 5 (1984), pp. 276–285.

[3] D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inform. Theory, IT-30 (1984), pp. 587–594.

[4] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, IT-22 (1976), pp. 644–654.

[5] M. E. Hellman and J. M. Reyneri, *Fast computation of discrete logarithms in* GF(q), *Advances in Cryptography: Proceedings of CRYPTO '82*, D. Chaum, R. Rivest, and A. Sherman, Eds., Plenum, New York 1983, pp. 3–13.

[6] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, New York 1971.

[7] — *The Art of Computer Programming*, Vol. 3, Addison-Wesley, New York 1973.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Pub. Co., Reading, Mass. 1983.

[9] R. Merkle and M. E. Hellman, *Hiding information and signatures in trapdoor knapsacks*, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 525–530.

[10] L. M. Milne-Thomson, *The Calculus of Finite Differences*, Macmillan and Co., London 1933.

[11] S. C. Pohlig and M. E. Hellman, *An improved algorithm for computing logarithms over* GF(p) *and its cryptographic significance*, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 106–110.

[12] R. A. Scholtz and L. R. Welch, *Generalized residue sequence*, Proc. Internat. Conf. Comm., Seattle, Washington, June 1973.

DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802

DEPARTMENT OF APPLIED STATISTICS
UTAH STATE UNIVERSITY
LOGAN, UTAH 84322

Received on 21.1.1985
and in revised form on 8.7.1985 (1489)