A polynomial representation for logarithms in GF(q)

by

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

1. Introduction. Let \( F_q = GF(q) \) denote the finite field of order \( q = p^n \) where \( p \) is prime and \( n \geq 1 \). The field \( F_q \) may be viewed as the set of all polynomials in \( \alpha \) of degree \( < n \) with coefficients in \( F_p \) where \( \alpha \) 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 \( 0 \leq k \leq q-2 \) and we say that \( k \) is the logarithm of \( \beta \) 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

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

then

\[
\log_c \beta = \sum_{i=0}^{n-1} a_i p^i.
\]

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

\[
b_i = \begin{cases} 
-\sum_{j=0}^{i-1} \alpha^j & \text{if } i = 0, \\
\sum_{j=0}^{n-1} \frac{\alpha^j}{c^{\sigma(q-1-i)-1}} & \text{if } 1 \leq i \leq q-2, \\
0 & \text{if } i = q-1.
\end{cases}
\]

In the special case when \( n = 1 \) we have

\[
\log_c \beta = -1 + \sum_{i=1}^{q-2} (c^{p-1-i}-1)^{-1} \beta^i \quad \text{for all } \beta \in F_q^*.
\]
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 $F_p^*$, 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 $b \in F_p^*$ and $b \neq 1$ then
\[ \sum_{j=0}^{p-1} j(b^j)^j = -b^p (b^{p+1} - 1)/(b^p - 1)^2. \]

**Proof.** If $b \neq 1$ then from the calculus of finite differences, see for example [10], p. 41,
\[ \sum_{j=1}^{p-1} j(b^j)^j = \frac{pb^p}{b-1} - \frac{b^{p+1} - b}{(b-1)^2} = -b(b^p - 1)/(b-1)^2. \]

The lemma now follows by substituting $b^j$ for $b$.

**Lemma 2.** If $b \in F_p^*$ and $b \neq 1$ then
\[ \sum_{j=0}^{p-1} (b^j)^j = (b^{p+1} - 1)/(b^p - 1). \]

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

**Lemma 3.** If $b \in F_p^*$ and $b \neq 1$ then
\[ \sum_{j=0}^{p-1} a_j b^{a_j + \cdots + a_1 a_0 - 1} = -b^{a_j}/(b^{a_j} - 1). \]

**Proof.** Let $N_i$ denote the left-hand side of (5). Then
\[ N_i = \sum_{a \in F_p} \sum_{b \in F_p} a_i b^{a_j} \cdots \sum_{a_0 \in F_p} a_0 b^{a_0 - 1}. \]

By repeated use of Lemma 2 we have
\[ N_i = \frac{b^{a_j} - 1}{b^{a_j + 1} - 1} \sum_{a_j \in F_p} \sum_{a \in F_p} a_i b^{a_j} \cdots \sum_{a_0 \in F_p} a_0 b^{a_0 - 1}. \]

which by Lemma 1 and Lemma 2 becomes
\[ N_i = -b^{a_j}/(b^{a_j} - 1). \]

But $b \in F_p^*$ so that $b^{a_j} = b$ and hence
\[ N_i = -b^{a_j}/(b^{a_j} - 1). \]

3. Construction of the polynomial. By the Lagrange Interpolation Formula for finite fields, every function $f : F_q \rightarrow F_q$ 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
\[ P(x) = \sum_{\beta \in F_q} f(\beta)(1 - x - \beta)^{-1}. \]

It is easy to check that if $q = p^r$ then the binomial coefficient
\[ \binom{q-1}{i} \equiv (-1)^i (\text{mod } p) \quad \text{for} \quad i = 0, 1, \ldots, q-1 \]

so that we may rewrite $P(x)$ as
\[ P(x) = \sum_{i=0}^{q-1} b_i x^i \]
where
\[ b_i = \int_{\beta \in F_q} f(\beta)(\beta - 1)^{-1} \quad \text{if} \quad i = 0, \]
\[ b_i = -\sum_{\beta \in F_q} f(\beta)(\beta)^{i-1} \quad \text{if} \quad 1 \leq i \leq q-1. \]

Let $c \in F_p^*$ be a primitive element so that if $\beta \in F_p^*$ then $\beta = c^k$ for some $0 \leq k \leq q - 2$ and $\log_c \beta = k$. We wish to construct a polynomial
\[ P_c(x) \in F_q[x] \]
with the property that if $P_c(\beta) = \sum_{i=0}^{q-1} a_i \beta^i$ for some
Theorem 4. Suppose \( c \in F_q \) is a primitive element, \( \beta \in F_p^* \), and

\[
P_\epsilon(\beta) = \sum_{j=0}^{n-1} a_j \beta^j \quad \text{for some } (a_0, \ldots, a_{n-1}) \in F_p^n
\]

where the coefficients of \( P_\epsilon(x) \) are given by (6). Then

\[
\log_{\epsilon} \beta = \sum_{j=0}^{n-1} a_j \beta^j.
\]

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

\[
\log_{\epsilon} \beta = -1 + \sum_{i=1}^{p-2} (\epsilon^{p-1-i} - 1)^{-1} \beta^i.
\]

The next corollary illustrates several interesting properties of the coefficients of the polynomial representing \( \log_\epsilon x \) 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) \( b_0 + b_{p-1-i} = p-1 \) for \( 0 \leq i \leq p-1 \),

(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 \( \%/c, m \) denote the set of coefficients in \( P_\epsilon(x) \) corresponding to those exponents that are divisible by \( m \). If \( c_1 \) is another primitive element of \( F_p \), then \( \%/c_1, m \) equals \( \%/c, m \).

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 \( 0 \leq i \leq p-2 \). If \( c_1 \) is another primitive element so that \( c_1 = c^k \) with \( (k, p-1) = 1 \), then the set of elements \( c^{p-1-i} \) for \( 0 \leq j \leq p-2 \) runs through \( F_p^* \). Hence for each \( i \) there is a unique \( j \) such that \( c^{j-i} = c^{p-1-i} \). 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 \( c^{(p-1)/2} = (p-1)/2 \) so that \( i-kj \equiv 0 \) (mod \( p-1 \)) and hence \( i-kj \equiv 0 \) (mod \( m \)). Thus \( i = kj + ms \) for some integer \( s \) so that since \( k, m = 1 \), we have that \( m \) divides \( j \) if and only if \( m \) divides \( j \). Hence we have shown that

\[
a = (c^{p-1-1})^{-1} \in \%/c, m \) if and only if \( a \in \%/c_1, m \) \).

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)

\[
b_i = -\sum_{j=0}^{n-1} a_j c^{i-j} \quad \text{if } 1 \leq i \leq q-2,
\]

so that we may state

\[
\log_{\epsilon} \beta = \sum_{j=0}^{n-1} a_j \beta^j.
\]
If \( c = \alpha \) then \( b_1 = 0 \) and \( b_2 = \alpha + 1 \) so that
\[
P_\alpha(x) = (x+1)x^2+(x+1).
\]
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
\[
\log_3 x = 4x^3 + x^4 + 3x^3 + 5x^2 + 2x + 6.
\]
Similarly if \( c = 5 \) we obtain
\[
\log_5 x = 2x^5 + 5x^4 + 3x^3 + x^2 + 4x + 6
\]
so that
\[
\varphi(3, 1) = F_3 \neq \varphi(5, 1),
\]
\[
\varphi(3, 2) = \{0, 1, 5, 6\} = \varphi(5; 2),
\]
\[
\varphi(3, 3) = \{0, 3, 6\} = \varphi(5, 3),
\]
\[
\varphi(3, 6) = \{0, 6\} = \varphi(5, 6).
\]

**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**


**Received on 21.1.1985**

and in revised form on 8.7.1985