ARCHIVUM MATHEMATICUM (BRNO)
Tomus 29 (1993), 25 – 28

EXPLICIT FORM FOR THE DISCRETE LOGARITHM OVER THE FIELD $GP(p,k)$

Gerasimos C. Meletiou

Abstract. For a generator of the multiplicative group of the field $GF(p,k)$, the discrete logarithm of an element b of the field to the base a, $b \neq 0$ is that integer $z : 1 \leq z \leq p^k - 1$, $b = a^z$. The p-ary digits which represent z can be described with extremely simple polynomial forms.

1. Introduction

The present note addresses the Discrete Logarithm problem ([1], [3], [4], [6]). The problem amounts to finding a quick method (efficient algorithm) for the computation of an integer z satisfying the equation:

$$a^z = b. \tag{1}$$

for $b \in GF(p,k)$, given a generator a of the multiplicative group of the field $GF(p,k)$. The main practical interest in the problem stems from cryptography ([1], [2], [3], [4], [6]).

In the case that a and z are known the computation of b can be done rapidly (Discrete Exponential Function [4], [7, p. 399]). However, computing z from a and b, that is, computing logarithms over $GF(p,k)$, does not appear to admit a fast algorithm. ([1], [3], [4]).

The integer z in (1) is computed modulo $p^k - 1$. In the case $k = 1$, a and b can be regarded as integers from $\{1, 2, \dots, p-1\}$ and z as an integer from $\{1, \dots, p-2\}$. The following polynomial formula has been found ([6]).

$$z \equiv \sum_{i=1}^{p-2} (1 - a^i)^{-1} b^i \pmod{p}\,. \tag{2}$$

The mere existence of such a formula in terms of powers of b is due to the fact that in a finite field every function from the field to itself can be expressed as a

1991 *Mathematics Subject Classification*: 11T71, 11T99.
Key words and phrases: discrete logarithm, finite fields, cryptography.
Received December 10, 1991.

polynomial. Although (2) is of no computational use, still, it is of mathematical interest.

The generalization of (2) to the field $GF(p,k)$, $k > 1$ is the purpose of this correspondence. Integer z in (1) is going to be computed modulo $q-1$, $q = p^k$. Therefore it can be assumed $1 \leq z \leq q-1$ and

$$z = \sum_{m=0}^{k-1} d_m p^m \,, \tag{3}$$

where $0 \leq d_m \leq p-1$. We use the numeric system with p as a basis, the $d_m s$ are p-digits. In the case $p=2$ the $d_m s$ are binary digits (that is bits).
For $k=1$ one has $z = d_0$.

It remains to find explicit formulas for the $d_m s$. Since $0 \leq d_m \leq q-1$ d_m can be regarded as an element of $GF(p,k)$. The $d_m s$ are uniquely determined in (3); they are functions of b provided that a is a generator of the multiplicative group of $GF(p,k)$. Then

$$d_m = \sum_{i=1}^{q-2} b^i/(1-a^i)^{p^m}, \quad m = 0,1,\ldots,k-1\,. \tag{4}$$

Trivially, (4) is a generalization of (2).
For $p=2$ (4) becomes

$$d_m = \sum b^i/(1+a^i)^{2^m}, \quad m = 0,1,\ldots,k_1, d_i \in \{0,1\}\,. \tag{5}$$

Therefore in any finite field the discrete logarithm function can be expressed with k polynomials with $q-2$ different coefficients. Surprisingly enough, the formulas for the coefficients are very simple.

II. Main Calculations

Equation (4) has to be shown. For $m=0$ it becomes:

$$d_0 = \sum_{i=1}^{q-2} b^i(1-a^i)^{-1}\,. \tag{6}$$

For the proof Lagrangian Interpolation is going to be used. According to (3) d_0 is the rightmost p-digit of z, thus $d_0 \equiv z (\mathrm{mod}\ p)$. The characteristic of the field is p. It follows:

$$d_0 = 1 \cdot \delta(b,a) + 2 \cdot \delta(b,a^2) + \cdots + (q-1) \cdot \delta(b,a^{q-1}) \tag{7}$$

where $\delta(b,a^j)$ is defined as

$$\delta(b,a^j) = \begin{cases} 1 & b = a^j \\ 0 & b \neq a^j\,. \end{cases}$$

Further

$$\delta(b, a^j) = 1 - (b - a^j)^{q-1} = 1 - \sum_{i=0}^{q-1} b^i (-a^j)^{q-1-i} \cdot \binom{q-1}{i} . \tag{8}$$

However, since $q = p^k$ ones concludes:

$$\binom{q-1}{i} = \frac{(p^k - 1)(p^k - 2) \ldots (p^k - i)}{i!} \equiv (-1)^i (\bmod p) . \tag{9}$$

In the case $p \neq 2$ the value of $(-1)^{q-1}$ is 1.

In the case $p = 2$, $(-1)^{q-1} = -1 \equiv 1 (\bmod 2)$. Thus (8) implies:

$$\delta(b, a^j) = -\sum_{i=1}^{q-1} b^i a^{-ij} .$$

Therefore

$$d_0 = \sum_{j=1}^{q-1} j \left(-\sum_{i=1}^{q-1} b^i a^{-ij} \right) = \sum_{i=1}^{q-1} b^i \left(-\sum_{j=1}^{q-1} j \cdot a^{-ij} \right) . \tag{10}$$

The sum $-\sum_{j=1}^{q-1} j \cdot a^{-ij}$ becomes 0 for $i = q-1$, since $a^{q-1} = 1$, and it becomes $-\dfrac{a^{-i}}{1 - a^{-i}} = (1 - a^i)^{-1}$ in the case $i \neq q-1$. Equality (6) is therefore true.

The above proof for (6) is similar to the proof given by Well's in [6, p. 846] generalized to the field $GF(p, k)$. It becomes clear because of the observation at the end of [6] which states that in the field with $q = p^k$ elements the matrix $M(a) = (a^{ij})$, $0 \leq i, j \leq q-2$ satisfies $M(a)^{-1} = -M(a^{-1})$. Also it is a good idea to be mentioned that $M(a)$ is a discrete Fourier transform over $GF(p, k)$ ([5]).

It suffices formulas for the $d_s s$ to be derived, $1 \leq s \leq k-1$. Since $z \cdot p^k \equiv z (\bmod q-1)$ it is true:

$$a^{zp^k} = b \qquad \text{or} \quad (a^{p^s})^{p^{k-s} \cdot z} = b . \tag{11}$$

The transformation $x \mapsto x^{p^s}$ is an automorphism of the field. Therefore a^{p^s} is a generator of the multiplicative group.

According to (3) $p^{k-s} \cdot z$ equals to

$$\sum_{m=0}^{s-1} d_m p^{k+m-s} + \sum_{m=s}^{k-1} d_m p^{k+m-s} .$$

The powers of p are for $m \geq s$

$$p^{k+m-s} = p^k \cdot p^{m-s} \equiv p^{m-s} (\bmod \ q-1) . \tag{12}$$

Therefore

$$p^{k-s}z \equiv v(\text{mod } q-1)\,, \tag{13}$$

where

$$v = \sum_{m=s}^{k-1} d_m p^{m-s} + \sum_{m=0}^{s-1} d_m p^{k+m-s}\,. \tag{14}$$

It follows from (14) that $0 \leq v \leq q-1$. Equation (14) is just the representation of v with p-ary digits. The rightmost p-digit is the coefficient of p^0 that is d_s.

Equation (11) can be written as:

$$(a^{p^s})^v = b\,. \tag{15}$$

The integer v is the discrete logarithm of b to the basis a^{p^s}. From (6) it is concluded

$$d_s = \sum b^i(1-a^{p^s i})^{-1} = \sum b^i(1-a^i)^{-p^s}\,. \tag{16}$$

The last equation in (16) is true since $x \mapsto x^{p^s}$ is a field automorphism. The proof is complete.

References

[1] Adleman, L. M., *A subexponential algorithm for the discrete logarithm problem, with applications to cryptography*, Proc. 20th IEEE Found. Comp. Sci. Symp. (1979), 55-60.

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

[3] Odlyzko, A. M., *Discrete logarithms in finite fields and their cryptographic significance*, Proc. of the Eurocrypt '84.

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

[5] Pollard, S. M., *The fast Fourier transform in a finite field*, Mathematics of computation **25** (1971), 365-374.

[6] Wells, A. L., *A polynomial form for logarithms modulo a prime*, IEEE Trans.Inform. Theory, IT-30 (1984), 845-846.

[7] Knuth, D. E., *The art of computer programming*, Reading MA **III** (1969), Addison Wesley.

Gerasimos C. Meletiou
TEI/M. at Arta
P.O. Box 110
ARTA, 47100, GREECE