ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Applied Mathematics 128 (2003) 193–206

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

Interpolation of the discrete logarithm in $\mathbf{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$

Tanja Lange[a], Arne Winterhof[b,*]

[a] *Institute of Experimental Mathematics, University of Essen, Ellernstr. 29, 5326 Essen, Germany*
[b] *Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19/2, 1010 Wien, Austria*

Received 8 February 2001; received in revised form 29 May 2001; accepted 8 April 2002

Abstract

Recently, Shparlinski proved several results on the interpolation of the discrete logarithm in finite prime fields by Boolean functions. In the first part of the paper, these results are extended to arbitrary finite fields of odd characteristic. More precisely, we prove some complexity lower bounds for Boolean functions representing the least significant bit of the discrete logarithm in a finite field.

In the second part of the paper we obtain lower bounds on the sparsity and the degree of polynomials over $\mathbf{F}_q$ in several variables computing the discrete logarithm modulo a prime divisor of $q-1$. These results are valid for even characteristic, as well.

Keywords: Discrete logarithm; Finite fields; Boolean functions; Exponential sums; Complexity lower bounds

1. Introduction

This paper deals with one of the hard problems in cryptography: finding complexity lower bounds on the discrete logarithm. It continues the work of several authors [1,7,13,14,20], in particular of Igor Shparlinski [17].

* Corresponding author.
E-mail addresses: lange@exp-math.uni-essen.de (T. Lange), arne.winterhof@oeaw.ac.at (A. Winterhof).

0166-218X/03/$ - see front matter
PII: S0166-218X(02)00445-6

Let G be a (multiplicatively written) finite cyclic group of order g with generator γ and $\xi \in G$. The *discrete logarithm* (or *index*) of ξ to the base γ, denoted $\mathrm{ind}_\gamma \xi$, is the unique integer l with $0 \leqslant l < g$ such that $\xi = \gamma^l$.

In public-key cryptography the discrete logarithm has gained increasing interest as a one-way function. The Diffie–Hellman key exchange, the El Gamal cryptosystem, and their derivatives (see e.g. [5,6,12]) depend on the intractability of the discrete logarithm. Two interesting choices of G used in practice are the multiplicative group of a finite field and a cyclic subgroup of the group of points of an elliptic curve defined over a finite field. Menezes et al. [11] reduced the elliptic curve discrete logarithm problem to the discrete logarithm problem in a finite extension field. In this article we consider the discrete logarithm problem in arbitrary finite fields.

Let $\mathbf{F}_q$ denote the finite field of order $q = p^r$ with a prime p and an integer $r \geqslant 1$. Except for the last section we assume $p > 2$. For many practical purposes it would be sufficient to have an easily computable function which represents the discrete logarithm for almost all nonzero elements of $\mathbf{F}_q$. For several kinds of polynomials it was shown that the complexity of the discrete logarithm is high in several measures as degree and sparsity [1,7,13,14,17,20]. In the first part of the present paper we investigate *Boolean functions*, i.e. multilinear polynomials over $\mathbf{F}_2$, and in the second part we consider *multivariate polynomials* modulo a prime divisor of $q-1$. We prove bounds which show how hard the discrete logarithm problem is at least, choosing these kinds of attack.

In the sequel we make use of a special ordering of the elements of $\mathbf{F}_q$. Let $\{\beta_1, \ldots, \beta_r\}$ be a basis of $\mathbf{F}_q$ over $\mathbf{F}_p$ and define ξ_k for $0 \leqslant k < q$ by

$$\xi_k = k_1\beta_1 + k_2\beta_2 + \cdots + k_r\beta_r$$

if

$$k = k_1 + k_2 p + \cdots + k_r p^{r-1}, \quad \text{with } 0 \leqslant k_i < p \text{ for } 1 \leqslant i \leqslant r. \tag{1}$$

For $1 \leqslant K \leqslant p$ put

$$\mathscr{K}_K = \{k = k_1 + k_2 p + \cdots + k_r p^{r-1} \mid 0 \leqslant k_i < K \text{ for } 1 \leqslant i \leqslant r\}.$$

Recently, in [7] we considered Boolean functions B of rs, $s = \lfloor \log_2(p) \rfloor$, $p > 2$, variables producing the *least significant bit* of $\mathrm{ind}_\gamma \xi_k$ from the bit representation of k for any ξ_k with $k \in \mathscr{K}_{2^s}$, i.e.

$$B(u_{11}, \ldots, u_{1s}, \ldots, u_{r1}, \ldots, u_{rs}) = \begin{cases} 0 & \text{if } \xi_k \text{ is a square in } \mathbf{F}_q, \\ 1 & \text{if } \xi_k \text{ is a nonsquare in } \mathbf{F}_q, \end{cases} \tag{2}$$

where

$$k_i = u_{i1} + u_{i2}2 + \cdots + u_{is}2^{s-1} \quad \text{with } u_{ij} \in \{0,1\} \tag{3}$$

for $1 \leqslant j \leqslant s$, $1 \leqslant i \leqslant r$, and $k \in \mathscr{K}_{2^s} \setminus \{0\}$.

The *sparsity* $\mathrm{spr}(B)$ (or *weight*) of B is the number of nonzero coefficients of B. In [7] we extended and improved slightly results of Coppersmith and Shparlinski

[1, Section 3] and Shparlinski [17, Chapter 6] showing that (2) implies

$$\mathrm{spr}(B) \geqslant (2^{-3/2}(3^{1/r}+r)^{-1/2}p^{1/4})^r - 1.$$

Thereby we obtained estimates on the degree of B and the complexity of bounded fan-in circuits representing B.

Another important characteristic value of a Boolean function B is the *average sensitivity* $\sigma_{\mathrm{av}}(B)$, a measure on how the value of B changes on average if the nth bit of the argument is flipped, i.e.

$$\sigma_{\mathrm{av}}(B) = 2^{-rs}\sum_{u\in\mathscr{B}_{rs}}\sum_{n=1}^{rs}|B(u)-B(u^{(n)})|,$$

where $\mathscr{B}_{rs}=\{u=(u_{11},\ldots,u_{1s},\ldots,u_{r1},\ldots,u_{rs})\in\{0,1\}^{rs}\}$ and $u^{(n)}$ is the vector obtained from u by flipping the nth coordinate. In Section 2 we show

$$\sigma_{\mathrm{av}}(B) \geqslant 0.5rs + \mathrm{o}(rs), \quad s\to\infty$$

if B satisfies (2).

For a Boolean function B its *Fourier coefficients* $\hat{B}(a)$, where $a\in\mathscr{B}_{rs}$, are defined as

$$\hat{B}(a) = \sum_{u\in\mathscr{B}_{rs}}(-1)^{B(u)+\langle a,u\rangle},$$

where $\langle a,u\rangle = a_{11}u_{11}+\cdots+a_{rs}u_{rs}$ for $a=(a_{11},\ldots,a_{rs})$ and $u=(u_{11},\ldots,u_{rs})$. In Section 3 we show that (2) yields

$$\max_{a\in\mathscr{B}_{rs}}|\hat{B}(a)| \leqslant 2^{(2r+3)/4}q^{7/8}(\ln(p)+1)^{r/4}+1.$$

Now we introduce a further characteristic value concerning Boolean functions. A Boolean function B of rs variables is said to belong to the class $\mathscr{P}^{rs}_{x,y}$, if for any choice of x bits there are at least y distinct functions obtainable by making all 2^x possible assignments to these fixed bits. Thus, it is a measure on how many of the variables are independent in some sense. Since $y\leqslant 2^x$, the following result obtained in Section 4 shows for which positive integer x this maximal value is attained. Let B be defined as in (2). Then

$$B\in\mathscr{P}^{rs}_{x,2^x} \quad \text{for } 1\leqslant x\leqslant \lfloor 0.25r\log_2(p)-r-1\rfloor.$$

The methods producing the above results and the results in [7] do not work for even characteristic. Since, in practice, this is the most important occurrence of nonprime fields, we need a compensation: we consider multivariate polynomials F computing the discrete logarithm modulo a prime divisor d of $q-1$, i.e. $F\in\mathbf{Z}[X_1,\ldots,X_r]$ such that

$$F(k_1,\ldots,k_r)\equiv \mathrm{ind}_\gamma(\xi_k)\bmod d \quad \text{for } 1\leqslant k<q, \tag{4}$$

where k is of the form (1). We investigate characteristic values of these polynomials in Section 5. In detail we derive lower bounds on the sparsity

$$\mathrm{spr}(F) > 0.3\,\frac{q^{1/4}}{p^{1/2}} - 1$$

and the degree of F. These results hold true for any characteristic but are of major importance for even characteristic.

2. A bound on the average sensitivity

We recall that $q = p^r$ with an odd prime p, $s = \lfloor \log_2(p) \rfloor$, and the Boolean function B computes the least significant bit of the discrete logarithm in $\mathbf{F}_q$. By definition the average sensitivity does not exceed the number of variables rs of B. Now, we prove the following lower bound.

Theorem 1. *Let B be defined as in (2). Then we have*

$$\sigma_{\mathrm{av}}(B) \geqslant 0.5rs + \mathrm{o}(rs), \quad s \to \infty.$$

Proof. Put $M = \lfloor s^{1/2} \rfloor$, $H = 2M + 1$, $J = \lfloor s - s^{1/2} \rfloor$, and $K = 2^s - H2^J$. We fix the notation

$$B'(k) = B(u_{11}, \ldots, u_{1s}, \ldots, u_{r1}, \ldots, u_{rs})$$

if $k \in \mathscr{K}_{2^s}$ is of the form (1) and (3). (Note that k runs through $\mathscr{K}_{2^s}$ as $(u_{11}, \ldots, u_{rs})$ runs through $\mathscr{B}_{rs}$.) For any fixed $0 \leqslant j \leqslant J$ and any $k \in \mathscr{K}_K$ we consider the following rH-array:

$$((B'(k + h2^j p^{i-1}))_{h=1}^{H})_{i=1}^{r}.$$

Now we are interested in the number $N(T)$ of times we obtain any possible binary rH-array $T = ((t_{i,h})_{h=1}^{H})_{i=1}^{r}$ by varying k. Since $(-1)^{B'(k)} = \chi(\xi_k)$ we have

$$N(T) = 2^{-rH} \sum_{k \in \mathscr{K}_K} \prod_{i=1}^{r} \prod_{h=1}^{H} (\chi(\xi_k + h2^j \beta_i)(-1)^{t_{i,h}} + 1),$$

where χ denotes the quadratic character of $\mathbf{F}_q$. Expanding the products we get one term of value $K^r 2^{-rH}$ and $2^{rH} - 1$ terms of the form

$$\pm 2^{-rH} \sum_{k \in \mathscr{K}_K} \chi((\xi_k + h_1 2^j \beta_{i_1}) \cdots (\xi_k + h_v 2^j \beta_{i_v})),$$

where $v \leqslant rH$ and the pairs $(h_{v'}, i_{v'})$ are distinct. (For fixed v there are $\binom{rh}{v}$ such sums.) Applying an extension of the Polya-Vinogradov bound [19, Theorem 2] we get

$$\begin{aligned} N(T) &= K^r 2^{-rH} + \mathrm{O}\left(2^{-rH} \sum_{v=1}^{rH} \binom{rH}{v} v q^{1/2} (\ln(p) + 1)^r\right) \\ &= K^r 2^{-rH} + \mathrm{O}(2^{-rH} 2^{rH} rH q^{1/2} (\ln(p) + 1)^r) \\ &= K^r 2^{-rH} + \mathrm{O}(rH 2^{rs/2} s^r) = K^r 2^{-rH} + \mathrm{o}(K^r 2^{-rH}). \end{aligned}$$

Among the 2^{rH} possible binary rH-arrays there are $2^{rH}+o(2^{rH})$ ones satisfying both of the following statements:

$$t_{i,2h} \neq t_{i,2h+1} \quad \text{for } 0.5rM+o(rM) \text{ values of } 1 \leqslant h \leqslant M \text{ and } 1 \leqslant i \leqslant r, \tag{5}$$

$$t_{i,2h} \neq t_{i,2h-1} \quad \text{for } 0.5rM+o(rM) \text{ values of } 1 \leqslant h \leqslant M \text{ and } 1 \leqslant i \leqslant r. \tag{6}$$

In short, let us denote by $k^{(ij)}$ the integer obtained from k by flipping the jth bit of k_i, i.e. u_{ij}. If $((B'(k+h2^j p^{i-1}))_{h=1}^{H})_{i=1}^{r}$ equals an array T satisfying (5) and (6) then since

$$B'((k+h2^j p^{i-1})^{(ij)}) = B'(k+(2h\pm 1)2^{j-1}p^{i-1})$$

about half of the rM values $B'(k+h2^j p^{i-1})$ for $1 \leqslant h \leqslant M$, $1 \leqslant i \leqslant r$, differ from $B'((k+h2^j p^{i-1})^{(ij)})$. This leads to the following estimate:

$$\sum_{j=1}^{J}\sum_{k\in\mathscr{K}_K}\sum_{i=1}^{r}\sum_{\substack{h=1\\ B'(k+h2^j p^{i-1})\neq B'((k+h2^j p^{i-1})^{(ij)})}}^{M} 1$$

$$\geqslant J(K^r 2^{-rH}+o(K^r 2^{-rH}))(2^{rH}+o(2^{rH}))(0.5rM+o(rM))$$

$$= 0.5JK^r rM + o(JK^r rM).$$

For every $1 \leqslant i \leqslant r$, every $1 \leqslant j \leqslant J$, and every $1 \leqslant h \leqslant M$ we find

$$\left| \sum_{\substack{k\in\mathscr{K}_K\\ B'(k+h2^j p^{i-1})\neq B'((k+h2^j p^{i-1})^{(ij)})}} 1 - \sum_{\substack{k\in\mathscr{K}_{2^s}\\ B'(k)\neq B'(k^{(ij)})}} 1 \right| \leqslant r2^{(r-1)s}H2^J = o(2^{rs}).$$

Therefore,

$$\sigma_{\mathrm{av}}(B) = 2^{-rs}\sum_{i=1}^{r}\sum_{j=1}^{s}\sum_{\substack{k\in\mathscr{K}_{2^s}\\ B'(k)\neq B'(k^{(ij)})}} 1$$

$$\geqslant 2^{-rs}\sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{\substack{k\in\mathscr{K}_{2^s}\\ B'(k)\neq B'(k^{(ij)})}} 1$$

$$= 2^{-rs}M^{-1}\left(\sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{h=1}^{M}\left|\sum_{\substack{k\in\mathscr{K}_K\\ B'(k+h2^j p^{i-1})\neq B'((k+h2^j p^{i-1})^{(ij)})}} 1\right.\right.$$

$$\left. - \sum_{\substack{k\in\mathscr{K}_{2^s} \\ B'(k)\neq B'(k^{(ij)})}} 1 \right| + \sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{k\in\mathscr{K}_K} \sum_{\substack{h=1 \\ B'(k+h2^j p^{i-1})\neq B'((k+h2^j p^{i-1})^{(ij)})}}^{M} 1 \Bigg)$$

$$= 0.5rs + o(rs). \qquad \square$$

Remark. Theorem 1 and Parberry and Yan [15, Theorem 4.7] yield a lower bound on the CREW PRAM (concurrent read exclusive write parallel random access machine) complexity of B (for a complete definition see e.g. [18, Chapter 13]).

3. A bound for the maximum Fourier coefficient

In this section we prove an upper bound for $\max_{a\in\mathscr{B}_{rs}} |\hat{B}(a)|$. Moreover, from the bound on the maximum Fourier coefficient we get information on the complexities of unbounded fan-in circuits and the size of a decision tree computing B.

Theorem 2. *Let B be defined as in (2). Then we have*

$$\max_{a\in\mathscr{B}_{rs}} |\hat{B}(a)| \leqslant 2^{(2r+3)/4} q^{7/8} (\ln(p)+1)^{r/4} + 1.$$

Proof. As $(-1)^{B(u_{11},\ldots,u_{rs})} = \chi(\xi_k)$, where χ is the quadratic character of $\mathbf{F}_q$, we have for any $a\in\mathscr{B}_{rs}$,

$$\hat{B}(a) = \sum_{k\in\mathscr{K}_{2^s}\setminus\{0\}} \chi(\xi_k)(-1)^{\langle k,a\rangle} + (-1)^{B(0,\ldots,0)},$$

where $\langle k,a\rangle = \langle (u_{11},\ldots,u_{1s},\ldots,u_{r1},\ldots,u_{rs}),a\rangle$ and $k_i = u_{i1}+\cdots+u_{is}2^{s-1}$. Put

$$S(a) = \sum_{k\in\mathscr{K}_{2^s}} \chi(\xi_k)(-1)^{\langle k,a\rangle}$$

using the convention $\chi(0)=0$. Then,

$$|\hat{B}(a)| \leqslant |S(a)| + 1.$$

Put

$$x = \lceil 0.5\log_2 (2^{1/r} p^{3/2}(\ln(p)+1))\rceil.$$

We obtain

$$S(a) = \sum_{y\in\mathscr{K}_{2^x}} \sum_{z\in\mathscr{K}_{2^{s-x}}} \chi(\xi_y + \xi_{2^x z})(-1)^{\langle y,b\rangle+\langle z,c\rangle},$$

where

$$\langle y,b\rangle = \langle (y_{11},\dots,y_{1x},\dots,y_{r1},\dots,y_{rx}),(a_{11},\dots,a_{1x},\dots,a_{r1},\dots,a_{rx})\rangle,$$

$$\langle z,c\rangle = \langle (z_{11},\dots,z_{1(s-x)},\dots,z_{r1},\dots,z_{r(s-x)}),(a_{1(x+1)},\dots,a_{1s},\dots,a_{r(x+1)},\dots,a_{rs})\rangle,$$

and the obvious meaning of the bit representations. Therefore,

$$|S(a)| \leqslant \sum_{y\in\mathscr{K}_{2^x}} \left| \sum_{z\in\mathscr{K}_{2^{s-x}}} \chi(\xi_y + \xi_{2^x z})(-1)^{\langle z,c\rangle} \right|.$$

By the Cauchy–Schwarz inequality we get

$$\begin{aligned} |S(a)|^2 &\leqslant 2^{rx} \sum_{y\in\mathscr{K}_{2^x}} \left| \sum_{z\in\mathscr{K}_{2^{s-x}}} \chi(\xi_y + \xi_{2^x z})(-1)^{\langle z,c\rangle} \right|^2 \\ &= 2^{rx} \sum_{y\in\mathscr{K}_{2^x}} \sum_{z_1,z_2\in\mathscr{K}_{2^{s-x}}} \chi((\xi_y + \xi_{2^x z_1})(\xi_y + \xi_{2^x z_2}))(-1)^{\langle z_1,c\rangle+\langle z_2,c\rangle} \\ &\leqslant 2^{rx} \sum_{z_1,z_2\in\mathscr{K}_{2^{s-x}}} \left| \sum_{y\in\mathscr{K}_{2^x}} \chi((\xi_y + \xi_{2^x z_1})(\xi_y + \xi_{2^x z_2})) \right|. \end{aligned}$$

There are $2^{r(s-x)}$ pairs (z_1,z_2) with $z_1 = z_2$. For the remaining

$$2^{r(s-x)}(2^{r(s-x)} - 1)$$

pairs we make use of [19, Theorem 2],

$$\left| \sum_{y\in\mathscr{K}_{2^x}} \chi((\xi_y + \xi_{2^x z_1})(\xi_y + \xi_{2^x z_2})) \right| \leqslant 2q^{1/2}(\ln(p)+1)^r.$$

Using

$$(2^{1/r}p^{3/2}(\ln(p)+1))^{1/2} \leqslant 2^x < 2(2^{1/r}p^{3/2}(\ln(p)+1))^{1/2},$$

we get

$$\begin{aligned} |S(a)|^2 &\leqslant 2^{rx}(2\times 2^{2r(s-x)}q^{1/2}(\ln(p)+1)^r + 2^{r(s-x)}\times 2^{rx}) \\ &\leqslant (2^{1/r}\times 2^{-x}p^2 p^{1/2}(\ln(p)+1))^r + (2^x p)^r \\ &\leqslant p^r \left(\frac{2^{1/r}p^{3/2}(\ln(p)+1)}{(2^{1/r}p^{3/2}(\ln(p)+1))^{1/2}} \right)^r + (2p(2^{1/r}p^{3/2}(\ln(p)+1))^{1/2})^r \\ &< 2^{r+3/2}q^{7/4}(\ln(p)+1)^{r/2}, \end{aligned}$$

hence the claim of the theorem. □

The theorem can be used to obtain a bound on the class $\mathrm{UBC}(d,S)$ of unbounded Boolean circuits of B. An unbounded Boolean circuit of class $\mathrm{UBC}(d,S)$ consists of a special starting level and d levels each of which contains at most S unbounded fan-in gates. That means that each gate accepts any number of inputs obtained in the previous levels and produces one bit of output. The final level contains only one gate and produces the value of $B(u_{11},\dots,u_{rs})$.

Theorem 3. *Assume that there is an unbounded fan-in circuit $C \in \mathrm{UBC}(d,S)$ such that it computes the least significant bit of the discrete logarithm of ξ_k given the bit representation of $k \in \mathscr{K}_{2^s}$. Then we have*

$$d \log_2(\log_2(S)) \geqslant (1+\mathrm{o}(1)) \log_2(rs).$$

Proof. The proof is a direct generalization of [17, Theorem 6.5] based on an inequality of Linial et al. [9] (see also [10, Theorem 11.7]), the Parseval identity, and Theorem 2, respectively. □

A further model used in the theory of Boolean functions is the decision tree, i.e. a branching program based on a tree. This means that the value of $B(u_{11},\dots,u_{rs})$ is computed following the unique path in a binary tree determined by choosing at the node labeled ij the edge denoted by u_{ij}. The value is the label of the final node, i.e. the leaf, which is $\in\{0,1\}$. By its size $\mathrm{DT}(B)$ we mean the minimal number of leaves needed to compute B.

Corollary 1. *Let B be defined as in (2). Then we have*

$$\mathrm{DT}(B) \geqslant 2^{rs/8+\mathrm{o}(s)}.$$

Proof. The proof is a direct generalization of [17, Theorem 6.7] based on Jukna et al. [3,4, Lemma 2.2], the Parseval identity, and Theorem 2, respectively. □

4. A bound on the combinatorial complexity

In this section we consider the number of distinct functions obtained by fixing x bits of the input. This knowledge is used to give a bound on the combinatorial complexity.

Theorem 4. *Let B be defined as in (2). Then*

$$B \in \mathscr{P}^{rs}_{x,2^x} \quad \text{for } 1 \leqslant x \leqslant \lfloor 0.25r \log_2(p) - r - 1 \rfloor.$$

Proof. Fix x positions at

$$1 \leqslant i_{l,1} < \cdots < i_{l,x_l} \leqslant s, \quad 1 \leqslant l \leqslant r$$

for any partition $x = \sum_{l=1}^{r} x_l$ of x. In addition put $i_{l,0} = 0$ and $i_{l,x_l+1} = s + 1$ for $1 \leqslant l \leqslant r$. Let

$$\mathscr{U} = \left\{ u_1 + \cdots + u_r p^{r-1} \,\middle|\, u_l = \sum_{j=0}^{x_l} y_j 2^{i_{l,j}} \text{ with } 0 \leqslant y_j < 2^{i_{l,j+1}-i_{l,j}-1} \right.$$
$$\left. \text{for } 0 \leqslant j \leqslant x_l, 1 \leqslant l \leqslant r \right\}$$

be the set of integers u with $0 \leqslant u < 2^{rs}$ and zero bits at the fixed positions i_{l,x_l}. Put

$$h_{l,j} = \lfloor 2^{i_{l,j+1}-i_{l,j}-2} \rfloor \quad \text{for } 0 \leqslant j \leqslant x_l,\ 1 \leqslant l \leqslant r,$$

$$b = b_1 + \cdots + b_r p^{r-1} \quad \text{where } b_l = \sum_{j=0}^{x_l} h_{l,j} 2^{i_{l,j}}$$

and

$$\mathscr{V} = \left\{ v_1 + \cdots + v_r p^{r-1} \,\middle|\, v_l = \sum_{j=0}^{x_l} y_j 2^{i_{l,j}} \text{ where } 0 \leqslant y_j < \lceil 2^{i_{l,j+1}-i_{l,j}-2} \rceil \right.$$
$$\left. \text{for } 0 \leqslant j \leqslant x_l, 1 \leqslant l \leqslant r \right\}.$$

Then we have $b + v - w \in \mathscr{U}$ and $\xi_{b+v-w} = \xi_b + \xi_v - \xi_w$ for all $v, w \in \mathscr{V}$. Let a_1 and a_2 be two distinct integers with prescribed bits at the x fixed positions and zero bits at all other positions, i.e.

$$a_n = a_{n,1} + \cdots + a_{n,r} p^{r-1}, \quad a_{n,l} = \sum_{j=1}^{x_l} a_{n,l,j} 2^{i_{l,j}-1}$$

for $a_{n,l,j} \in \{0, 1\}$, $1 \leqslant j \leqslant x_l$, $1 \leqslant l \leqslant r$, and $1 \leqslant n \leqslant 2$. Then put $b_1 := a_1 + b$ and $b_2 := a_2 + b$. We have $\xi_{b_n - v + w} = \xi_{b_n} - \xi_v + \xi_w$ for $1 \leqslant n \leqslant 2$. Now the claim follows once we have shown that

$$\left| \sum_{v,w \in \mathscr{V}} \chi((\xi_{b_1} - \xi_v + \xi_w)(\xi_{b_2} - \xi_v + \xi_w)) \right| < |\mathscr{V}|^2 - 2|\mathscr{V}|.$$

Let ψ denote the additive canonical character of $\mathbf{F}_q$. Then by Weil's theorems [16,8, Theorem 2G; Theorem 5.41] we get

$$\left| \sum_{v,w \in \mathscr{V}} \chi((\xi_{b_1} - \xi_v + \xi_w)(\xi_{b_2} - \xi_v + \xi_w)) \right|$$
$$= \frac{1}{q} \left| \sum_{\xi \in \mathbf{F}_q} \chi((\xi_{b_1} + \xi)(\xi_{b_2} + \xi)) \sum_{v,w \in \mathscr{V}} \sum_{\mu \in \mathbf{F}_q} \psi(\mu(\xi + \xi_v - \xi_w)) \right|$$

$$\leqslant \frac{1}{q}\sum_{\mu\in\mathbf{F}_q}\left(\left|\sum_{\xi\in\mathbf{F}_q}\chi((\xi_{b_1}+\xi)(\xi_{b_2}+\xi))\psi(\mu\xi)\right|\left|\sum_{v\in\mathscr{V}}\psi(\mu\xi_v)\right|^2\right)$$

$$< \frac{1}{q}\sum_{\mu\in\mathbf{F}_q}2q^{1/2}\left|\sum_{v\in\mathscr{V}}\psi(\mu\xi_v)\right|^2$$

$$\leqslant 2q^{1/2}|\mathscr{V}|.$$

Now since

$$|\mathscr{V}| \geqslant \prod_{l=1}^{r}\prod_{j=0}^{x_l}2^{i_{l,j+1}-i_{l,j}-2} = \prod_{l=1}^{r}2^{s-2x_l-1} = 2^{rs-2x-r},$$

we have

$$2q^{1/2} \leqslant |\mathscr{V}| - 2$$

for $x \leqslant 0.25r\log_2(p) - r - 1$. □

Theorem 4 can be used to obtain a result for the combinatorial complexity $\mathrm{CC}(B)$ of B, i.e. the minimal number of gates needed to compute B by a bounded fan-in Boolean circuit of fan-out 1. In [2, Theorem 6.2] (see also [17, Lemma 3.19]) it was shown that $B\in\mathscr{P}_{3,5}^{rs}$ implies $\mathrm{CC}(B)\geqslant(7rs-4)/6$.

Corollary 2. *Let B be defined as in (2). Then*

$$\mathrm{CC}(B) \geqslant \frac{7rs-4}{6} \quad \textit{for } p > 2^{(4r+16)/4}.$$

5. Interpolation of the discrete logarithm by polynomials modulo a divisor of $q-1$

In this section we derive complexity lower bounds on the discrete logarithm for arbitrary finite fields (especially $p=2$ is allowed). For polynomials F in r variables computing the discrete logarithm modulo a prime divisor d of $q-1$ we estimate the sparsity and the degree of F.

Theorem 5. *Let d be a prime divisor of $q-1$ and $F\in\mathbf{Z}[X_1,\ldots,X_r]$ satisfy (4). Then we have*

$$\mathrm{spr}(F) > 0.3\,\frac{q^{1/4}}{p^{1/2}} - 1.$$

Proof. Let $p^x > \mathrm{spr}(F)+1 \geqslant p^{x-1}$ and $Mp^{x-1} > \mathrm{spr}(F)+1 \geqslant (M-1)p^{x-1}$ with $M\geqslant 2$. For each $1\leqslant m < Mp^{x-1}$ we consider the function

$$F_m(X_1,\ldots,X_{r-x}) = F(X_1,\ldots,X_{r-x},m_1,\ldots,m_x),$$

where $m = m_1 + m_2 p + \cdots + m_x p^{x-1}$ with $0 \leqslant m_i < p$ for $1 \leqslant i < x$ and $0 \leqslant m_x < M$ is the p-adic expansion of m. The number of different monomials occurring in some F_m cannot exceed the sparsity of F. Hence, we can find a vanishing linear combination modulo d of the form

$$\sum_{m=1}^{Mp^{x-1}-1} c_m F_m(X_1, \ldots, X_{r-x}) \equiv 0 \bmod d, \quad c_m \in \mathbf{Z},$$

where $c_m \not\equiv 0 \bmod d$ for some $1 \leqslant m < Mp^{x-1}$. By the condition of the theorem we have

$$\chi(\xi_k) = \eta^{F(k_1,\ldots,k_r)} \quad \text{for } 1 \leqslant k < q$$

for a dth root of unity η and a character χ of $\mathbf{F}_q$ of order d. Hence, for $0 \leqslant y < p^{r-x}$ we have

$$\prod_{m=1}^{Mp^{x-1}-1} \chi(\xi_y + \xi_{p^{r-x}m})^{c_m} = \eta^{\sum_{m=1}^{Mp^{x-1}-1} c_m F_m(y_1,\ldots,y_{r-x})} = 1, \tag{7}$$

where

$$y = y_1 + y_2 p + \cdots + y_{r-x} p^{r-x-1} \quad \text{with } 0 \leqslant y_i < p \quad \text{for } 1 \leqslant i \leqslant r-x$$

is the p-adic expansion of y. Summing (7) over y yields

$$p^{r-x} = \sum_{y=0}^{p^{r-x}-1} \chi\left(\prod_{m=1}^{Mp^{x-1}-1} (\xi_y + \xi_{p^{r-x}m})^{c_m}\right) < 2.2\, p^{(r-x)/2} M^{1/2} p^{(x-1)/2} q^{1/4}.$$

The latter inequality follows from [14, Theorem 3.1] if $p^{r-x} \geqslant 4.84 q^{1/2}$ and it is trivial otherwise. Hence,

$$Mp^{2x-1} > 0.2 q^{1/2}$$

and thus

$$(\mathrm{spr}(F) + 1)^2 p \geqslant (M-1)^2 p^{2x-1} \geqslant 0.5 Mp^{2x-1} > 0.1 q^{1/2}. \qquad \square$$

Remark. (1) For $r \leqslant 2$ Theorem 5 is trivial.

(2) Since we consider the polynomial F modulo d, the maximum possible sparsity of F is d^r. Therefore, this result shows the nonexistence of such a function if d is small compared to p.

For $d < p$ this nonexistence is evident since otherwise the discrete logarithm has to satisfy strong linearity conditions. We had for each pair $k = k_1 + \cdots + k_r p^{r-1}$, $l = l_1 + \cdots + l_r p^{r-1}$ with $k_i + d l_i < p$ for $1 \leqslant i \leqslant r$,

$$\mathrm{ind}_\gamma(\xi_k) \equiv \mathrm{ind}_\gamma(\xi_k + d\xi_l) \bmod d.$$

Since d cannot be identified with an element of $\mathbf{F}_p$ if $d > p$ the linear properties of $F \bmod d$ do not imply linear properties of ind_γ in this case.

Using the bound of the theorem we obtain information on the degree of F. Like in the theorem we assume that r is sufficiently large, i.e. $r \geqslant 3$.

Corollary 3. *Under the conditions of Theorem 5 we can find for any $\epsilon > 0$ and any integer r a $p_0(\epsilon, r)$ such that*

$$\deg F > \left(\frac{r-2}{4} - \epsilon\right) \log_2(p)$$

holds for any $p \geqslant p_0(\epsilon, r)$.

Proof. Put $n = \deg F$. As the local degree in any X_i is also bounded by n we have

$$\mathrm{spr}(F) \leqslant \sum_{i=0}^{n} \binom{r+i-1}{i} < \sum_{i=0}^{n} \binom{r+n-1}{i} \leqslant 2^{(r+n-1)}.$$

Hence,

$$\log_2(0.3) + \frac{r-2}{4} \log_2(p) \leqslant r + n - 1$$

and

$$n \geqslant \left(\frac{r-2}{4} - \frac{r+0.74}{\log_2(p)}\right) \log_2(p).$$

Using $p_0(\epsilon, r) \geqslant 2^{(r+0.74)/\epsilon}$ the claim follows. □

For $d > p$ further improvement on Theorem 5 and Corollary 3 can be gained if we choose a polynomial basis

$$\{\beta_1, \ldots, \beta_r\} = \{1, \alpha, \ldots, \alpha^{r-1}\}. \tag{8}$$

Additionally, we assume that α is not a dth power in $\mathbf{F}_q$. Furthermore, we restrict ourselves to polynomials of local degree at most $p-1$ in each variable.

Theorem 6. *Let $d > p$ be a prime divisor of $q-1$, and let $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ be such that α is not a dth power in $\mathbf{F}_q$. Let $F \in \mathbf{Z}[X_1, \ldots, X_r]$ satisfy (4) and (8) and let F be of local degree at most $p-1$. Then we have*

$$\deg(F) \geqslant (p-1)(r-1)$$

and

$$\mathrm{spr}(F) \geqslant \begin{cases} 2^{r-2} & \text{if } p = 2, \\ \frac{3^{r-1}-1}{2} & \text{if } p > 2. \end{cases}$$

Proof. W.l.o.g. we assume $\mathrm{ind}_\gamma(\alpha) \equiv 1 \bmod d$. Define $F' \in \mathbf{Z}[X_1, \ldots, X_{r-1}]$ by

$$F'(X_1, \ldots, X_{r-1}) = -F(X_1, \ldots, X_{r-1}, 0) + F(0, X_1, \ldots, X_{r-1})$$

and consider $\xi_k \neq 0$, $k < p^{r-1}$. If $F(k_1, \ldots, k_{r-1}, 0) \equiv c \equiv \mathrm{ind}_\gamma(\xi_k) \bmod d$ then $F'(k_1, \ldots, k_{r-1}) \equiv -c + (c + \mathrm{ind}_\gamma(\alpha)) \equiv 1 \bmod d$, since $(0, k_1, \ldots, k_{r-1})$ corresponds to $\alpha\xi_k$. Thus, for any $1 \leqslant k < p^{r-1}$, the function $F' \bmod d$ evaluates to 1. Note that however we define $F(0, \ldots, 0)$, we obtain $F'(0, \ldots, 0) = 0$. Hence, we know the values

of F' on a complete $(r-1)$-dimensional grid and can thus interpolate (variable by variable) the polynomial. For $p=2$ we obtain

$$F'(X_1,\ldots,X_{r-1}) \equiv (-1)^r \prod_{i=1}^{r-1}(X_i-1)+1 \bmod d$$

and for $p>2$

$$F'(X_1,\ldots,X_{r-1}) \equiv -((p-1)!)^{1-r}\prod_{i=1}^{r-1}((X_i-1)\cdots(X_i-(p-1)))+1 \bmod d.$$

From the corresponding product and by the construction of F' we obtain

$$\deg(F) \geqslant \deg(F') = (p-1)(r-1)$$

and

$$\operatorname{spr}(F) \geqslant \lceil 0.5 \operatorname{spr}(F') \rceil.$$

Since the coefficients of the monomials $X_1^{n_1}\cdots X_{r-1}^{n_{r-1}}$ with $n_i \in \{0, p-1\}$ in F' are products of integers incongruent to zero modulo d (and thus nonzero modulo d) we have

$$\operatorname{spr}(F') \geqslant 2^{(r-1)}-1.$$

For $p>2$ the coefficients of the monomials $X_1^{n_1}\cdots X_{r-1}^{n_r-1}$ with $n_i \in \{0, p-2, p-1\}$ are nonzero modulo d since the coefficient of X_i^{p-2} in $(X_i-1)\cdots(X_i-(p-1))$ is $(p-1)p/2 \not\equiv 0 \bmod d$. Hence, $\operatorname{spr}(F') \geqslant 3^{r-1}-1$ if $p>2$ which yields the lower bound on $\operatorname{spr}(F)$. □

Remark. (1) In the most interesting case $p=2$ the restriction on the local degree of F is unnecessary since each polynomial F^* of higher local degree satisfying the remaining conditions of Theorem 6 defines a unique multilinear polynomial F by substituting $X_i^{n_i}$ by X_i if $n_i>0$. Obviously, we have $\operatorname{spr}(F^*) \geqslant \operatorname{spr}(F)$, $F^*(k_1,\ldots,k_r)=F(k_1,\ldots,k_r)$ for any binary vector $(k_1,\ldots,k_r)$, and F satisfies the conditions of Theorem 6.

Moreover, $d>p$ is no restriction for $p=2$.

(2) For a different approach to represent the discrete logarithm by polynomials in several variables modulo d see [17, Chapter 5; 20, Section 4].

Acknowledgements

We would like to thank Igor Shparlinski for valuable comments that helped in particular to improve Theorem 5.

References

[1] D. Coppersmith, I.E. Shparlinski, On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping, J. Cryptol. 13 (2000) 339–360.

[2] L.H. Harper, W.N. Hsieh, J.E. Savage, A class of Boolean functions with linear combinational complexity, Theoret. Comput. Sci. 1 (1975) 161–183.
[3] S. Jukna, A. Razborov, P. Savický, I. Wegener, On P versus NP $\cap$ co-NP for decision trees and read-once branching programs, Mathematical Foundations of Computer Science (Bratislava), Lecture Notes in Computer Science, Vol. 1295, Springer, Berlin, 1997, pp. 319–326.
[4] S. Jukna, A. Razborov, P. Savický, I. Wegener, On P versus NP $\cap$ CO-NP for decision trees and read-once branching programs, Comput. Complexity 8 (1999) 357–370.
[5] N. Koblitz, A Course in Number Theory and Cryptography, in: Graduate Texts in Mathematics, Vol. 114, Springer, New York, 1994.
[6] N. Koblitz, Algebraic aspects of cryptography, in: Algorithms and Computation in Mathematics, Vol. 3, Springer, Berlin, 1998.
[7] T. Lange, A. Winterhof, Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions, Acta Arith. 101 (2002) 223–229.
[8] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[9] N. Linial, Y. Mansour, N. Nisan, Constant depth circuits, Fourier transform, and learnability, J. Assoc. Comput. Mach. 40 (1993) 607–620.
[10] Y. Mansour, Learning Boolean functions via the Fourier transform, in: V. Roychowdhury, et al., (Eds.), Theoretical Advances in Neural Computation and Learning, Kluwer, Boston, 1994, pp. 391–424.
[11] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inform. Theory 39 (1993) 1639–1646.
[12] A. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, 1997.
[13] G.L. Mullen, D. White, A polynomial representation for logarithms in GF(q), Acta Arith. 47 (1986) 255–261.
[14] H. Niederreiter, A. Winterhof, Incomplete character sums and polynomial interpolation of the discrete logarithm, Finite Fields Appl. 8 (2002) 184–192.
[15] I. Parberry, P.Y. Yan, Improved upper and lower time bounds for parallel random access machines without simultaneous writes, SIAM J. Comput. 20 (1991) 88–99.
[16] W.M. Schmidt, Equations Over Finite Fields, in: Lecture Notes in Mathematics, Vol. 536, Springer, Berlin, New York, 1976.
[17] I.E. Shparlinski, Number Theoretic Methods in Cryptography, Birkhäuser, Basel, 1999.
[18] I. Wegener, The Complexity of Boolean Functions, Teubner, Stuttgart, 1987.
[19] A. Winterhof, Some estimates for character sums and applications, Des. Codes Cryptogr. 22 (2001) 123–131.
[20] A. Winterhof, Polynomial interpolation of the discrete logarithm, Des. Codes Cryptogr. 25 (2002) 63–72.