On Polynomial Approximation and the Parallel Complexity of the Discrete Logarithm and Breaking the Diffie-Hellman Cryptosystem

Igor Shparlinski

School of MPCE, Macquarie University
NSW 2109, Australia
igor@mpce.mq.edu.au

July 3, 1996

1 Introduction

In the first part of this paper we consider various representations and approximations of the discrete logarithm via some other functions over finite fields such as polynomials and their combinations with exponential functions (linear recurring sequences, basically) and algebraic functions (i.e. via functions $f(X)$ satisfying a polynomial equation $F(X, f(X)) = 0$ over a finite field).

The aforementioned functions form a basic set of "easy computable" functions, at least when they are of small degree or order. For polynomials this is obvious. For linear recurring sequences one can use a kind of repeated squaring like for computing a single exponential function. For algebraic functions it is justified by recent progress in solving polynomial equations over finite fields and finding points on algebraic curves [8, 24]. So, the principal motivation of this paper is to show that none of such simple representations of the discrete logarithm holds. In some cases we also show that the polynomials involved contain sufficiently many monomials. Moreover, here we deal with partial representations, those are representations which hold only for some subsets of the set of all possible values of the argument of the discrete logarithm.

Such results lead to lower bounds on the parallel complexity of computing the discrete logarithm in several different computational models.

Here we consider the case of prime fields. Respectively, we use the language of congruences modulo a prime p rather than finite fields.

Let us fix a primitive root g modulo a prime number $p \geq 3$ and denote by $\operatorname{ind} x$ the *discrete logarithm* (or *index*) of x with $\gcd(x,p) = 1$, that is the smallest non-negative integer u with $g^u \equiv x \pmod p$. Thus the discrete logarithm defines a bijective mapping from the group of units of the residue ring modulo p, from the set $\{1,\dots,p-1\}$ essentially, onto the set $\{0,1,\dots,p-2\}$. Hence one can ask about polynomial representation of this mapping that is a polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most $p-1$ such that

$$\operatorname{ind} x \equiv f(x) \pmod p, \qquad x = 1,\dots,p-1.$$

Our argument x "lives" in the residue ring modulo p, this is why we consider congruences modulo p. On the other hand, the function $\operatorname{ind} x$ resembles the logarithmic function in the residue ring modulo $p-1$. Thus studying polynomial and other approximations modulo $p-1$ is another natural question which we also address in this paper.

It has been shown in [21] that the polynomial

$$f(x) \equiv -1 + \sum_{k=1}^{p-2} (g^{-k} - 1)^{-1} x^k \pmod p \tag{1.1}$$

is the unique interpolation polynomial of the discrete logarithm modulo p. We note that this polynomial is of very large degree and is dense (that is contains $p-2$ monomials).

Here we show that these two properties are preserved even for partial representations and approximations of the discrete logarithm. More precisely, for many practical purposes it would be enough to have a simple polynomial representation of the discrete logarithm for almost all $x = 1,\dots,p-1$ rather than for all of them. We show that even such a polynomial must be of high degree and contain many non-zero coefficients. That result is quite simple and completely elementary. Then using more involved arguments we consider

- approximation on small intervals $[N+1, N+H]$;
- approximation on very sparse sets;
- piecewise approximation

The approximating function can be

- a polynomial;
- a Boolean function;
- an algebraic function;
- a linear recurring sequence.

Respectively, the aforementioned approximations are studied

- over the residue ring modulo p (where the argument of $\operatorname{ind} x$ belongs to);
- over the residue ring modulo $p-1$ (where the behaviour of $\operatorname{ind} x$ resembles the behaviour of $\log x$);
- over the r-dimensional Boolean cube where r is the bit length of p (if we consider the argument x and the value $\operatorname{ind} x$ as sequences of bits).

In particular, our results provide a non-trivial lower bound $\Omega(p^{1/2} \log^{-1} p)$ for the linear complexity [22] of the discrete logarithm modulo any divisor $d > 1$ of $p-1$. The case $d = 2$ corresponds to the linear complexity of the rightmost bit of $\operatorname{ind} x$.

This bit is of special interest of course since its parity determines wether x is a quadratic residue. Using estimates of character sums we obtain a lower bound of order $p^{1/4}$ on the number of monomials of a Boolean function on bits of x computing the last bit of $\operatorname{ind} x$. We apply it to obtain an $\Omega(\log \log p)$ lower bound on the depth of Boolean circuits deciding wether x is quadratic residue or not. This supplements some results of [5, 7] about arithmetic circuits (over $\mathbb{F}_q$) deciding whether $x \in \mathbb{F}_q$ is a quadratic residue or not. Those papers are based on the observation that this question is equivalent to computation of values of the polynomial $x^{(q-1)/2}$. Here, in the same fashion, we use our bound on the degree of Boolean functions giving the values of the last bit of $\operatorname{ind} x$. We also estimate from below some other characteristic of such functions which in turn gives a lower bound on their PRAM complexity, i.e. the complexity on a parallel random access machine with unlimited number of processors [28].

Then, we show that the same considerations are applicable to some questions related to the Diffie-Hellman cryptosystem [3] based on the discrete logarithm. This question is studied over arbitrary finite fields.

We apply our results to obtain a linear lower bound for the depth of randomised arithmetic circuits over $\mathbb{F}_q$ breaking this cryptosystem. We show that the depth of such circuit is of order $\log q$ at least. Thus it cannot be done in parallel logarithmic time $(\log\log q)^{O(1)}$. This holds for probabilistic circuits giving the correct answers for very sparse sets of values of the argument. Moreover, we show that even probabilistic verification wether given $u, v \in \mathbb{F}_q$ satisfy $u = g^x$, $v = g^{x^2}$ cannot be done in parallel logarithmic time.

The aforementioned result concerns arithmetic model of computation when each element of $\mathbb{F}_q$ is considered as a whole without access to its bits. Then, over $\mathbb{F}_{2^n}$ we also deal with the Boolean model of computation. We assume that each element $u \in \mathbb{F}_{2^n}$ is given by a binary vector $u = (u_1, \ldots, u_n)$ containing the "coordinates" of u in some fixed basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then we give a lower bound of the degree of Boolean functions expressing the coordinates of g^{x^2} via the coordinates of g^x. The bound is rather weak but still provides some non-trivial results about parallel Boolean complexity of breaking the Diffie-Hellman cryptosystem. For example it cannot be done by a Boolean circuit of constant depth. Unfortunately, this method does not work for other finite fields.

Finally we show that some other related questions about permutation polynomials, powers and Boolean functions can be dealt with along the same lines.

Our method is based on such classical tools of the theory of finite fields as:

- bounds for the number of solutions of equations and congruences;
- bounds for various character sums.

We also use some standard facts and notions of the theory of finite fields which one can easily find in [16].

In obtaining the lower bounds on the depth of circuits in Theorem 5.2 our arguments are quite close to those of [5, 6, 7] (see also given there references to other works). However, it looks like that in the proof of Theorem 6.5 some new arguments appears.

Throughout the paper, for a polynomial f over a ring $\mathcal{R}$, $\mathrm{wt}\, f$ denotes its *weight* which is defined as the total number of its non-zero coefficients.

We also use the notation

$$\mathbf{e}(z) = \exp(2\pi i z),$$

$\log z$ means the logarithm in base 2.

2 Auxiliary Results

Here we collect some lemmas we will need afterwards.

Let $(u(x))$ be a linear recurring sequence of order n over a field $\mathbb{K}$, that is

$$u(x+n) = c_{n-1}u(x+n-1) + \ldots + c_0 u(x), \qquad x = 1, 2, \ldots, \tag{2.1}$$

where $\psi(T) = T^n - c_{n-1}T^{n-1} - \ldots - c_0 \in \mathbb{K}[T]$ with $c_0 \neq 0$ is called the *characteristic polynomial*.

It is useful to recall that such a sequence can be uniquely represented in the form

$$u(x) = \sum_{i=1}^{m} \lambda_i^x f_i(x) \tag{2.2}$$

where $\lambda_1, \ldots, \lambda_m$ are the roots of $\psi(T)$ with multiplicities $k_1, \ldots, k_m$, respectively, and $f_1(X), \ldots, f_m(X)$ are polynomials (over an algebraic extension of $\mathbb{K}$) of degrees at most $k_1 - 1, \ldots, k_m - 1$, respectively. The inverse statement is also true: any sequence having a representation of the form (2.2) is a linear recurring sequence of order $n = m + \deg f_1 + \ldots + \deg f_m$.

In particular a polynomial $f(X) \in \mathbb{Z}[X]$ of degree n satisfies a linear recurrent equation of order $n+1$

$$f(x+n+1) = \sum_{k=0}^{n} \binom{n+1}{k} (-1)^{k+1} f(x+k)$$

with characteristic polynomial $\psi(T) = (T-1)^{n+1}$.

Lemma 2.1. *Let $(u(x))$ be a linear recurring sequence of order n satisfying an equation of the form (2.1) over a field $\mathbb{K}$ with $c_0 \neq 0$ and let $u(x) \neq 0$ for at least one integer $x \geq 1$ then for any integer $H \geq 1$ there are at least $\lfloor H/n \rfloor$ values of $x = 1, \dots, H$ with $u(x) \neq 0$.*

Proof. It is obvious that if n consecutive values

$$u(x) = \dots = u(x+n-1) = 0$$

then all further values $u(x+n), u(x+n+1), \dots$ are zeros too. Moreover, using the fact that $c_0 \neq 0$ one sees that all previous values $u(x-1), u(x-2), \dots$ are zeros as well. So among every n consecutive terms of the sequence there is at least one non-zero term and the bound follows. $\square$

The following lemma is based on very similar elementary considerations.

Lemma 2.2. *Let $f(X) \in \mathbb{F}_q[X]$ be a non-zero polynomial with* $\deg f \leq q-2$ *and* $\operatorname{wt} f = t \geq 1$. *Then there are at least $(q-1)/t$ values of $x \in \mathbb{F}_q$ with $f(x) \neq 0$.*

Proof. Noticing that $f(g^x) \neq f(g^{x+q-1})$, we see that the number N of $x = 0, \dots, q-2$ with $f(g^x) = 0$ is t times less than the number T of pairs (y, i), $y = 0, \dots q-2$, $i = 0, \dots, t-1$, with $f(g^{y+i}) \neq 0$. Using properties of Vandermonde matrices one can easily see that for any $y = 0, \dots, q-2$, $f(g^{y+i}) \neq 0$ for at least one $i = 0, \dots, t-1$. Thus $tN = T \geq q-1$ and the estimate follows. $\square$

The next two statements are slightly more general form of the Weil bound than it is usually known. They are combinations of a partial case of the result of Example 12 of Appendix 5 of [29] and the standard method of estimating of incomplete sums via complete ones [9].

Lemma 2.3. *For any non-trivial character χ modulo p of order d and any $n \ge 1$ integers $c_0, c_1, \ldots, c_n$ which are not all divisible by d the bound*

$$\left| \sum_{x=N+1}^{N+H} \chi\left(x^{c_0}(a_1x+b_1)^{c_1} \ldots (a_nx+b_n)^{c_n}\right) \right| \le (n+1)p^{1/2} \log p$$

holds for any integers N and $H \le p$ and any pairwise distinct linear forms $a_ix + b_i$ with $a_i \ne 0$, $i = 1 \ldots, n$.

Lemma 2.4. *For any non-trivial multiplicative character χ modulo p and any polynomial $f(X) \in \mathbb{Z}[X]$ of degree $n = \deg f \ge 1$, the bound*

$$\left| \sum_{x=N+1}^{N+H} \chi(x) \mathbf{e}\left(\frac{f(x)}{p}\right) \right| \le np^{1/2} \log p$$

holds for any integers N and $H \le p$.

3 Approximation of the Discrete Logarithm Modulo p

Here we show that polynomials and algebraic functions approximating the discrete logarithm modulo p on sufficiently large sets must be of sufficiently large degree, in fact exponentially (in terms of $\log p$) large.

We start with a rather simple statement.

Theorem 3.1. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n = \deg f$ and of weight $t = \mathrm{wt}\, f$ such that*

$$\mathrm{ind}\, x \equiv f(x) \pmod p, \qquad x \in S, \tag{3.1}$$

for a set $S \subseteq \{1, \ldots, p-1\}$ of cardinality $|S| = p - 1 - s$. Then

$$n \ge p - 2 - 2s, \qquad t \ge (p-1)/(2s+1) - 1.$$

Proof. Let R be the set of $x \in \{1, \ldots, p-1\}$ for which both

$$\operatorname{ind} x \equiv f(x) \pmod p \quad \text{and} \quad \operatorname{ind} gx \equiv f(gx) \pmod p.$$

Then $|R| \geq p - 1 - 2(p - 1 - |S|) = p - 1 - 2s$. We have, $\operatorname{ind} gx = 1 + \operatorname{ind} x$ if $x \not\equiv g^{p-2} \pmod p$. Hence

$$f(gx) \equiv \operatorname{ind} gx = 1 + \operatorname{ind} x \equiv 1 + f(x) \pmod p$$

for $x \in R$ with $x \not\equiv g^{p-2} \pmod p$. Therefore the polynomial $h(X) = f(gX) - f(X) - 1$ has at least $|R| - 1$ zeros modulo p and is not identical to zero modulo p (because $h(0) = -1$). Thus $n \geq \deg h \geq |R| - 1$.

Also, if f contains $t = \operatorname{wt} f$ monomials then h contains $\operatorname{wt} h \leq t + 1$ monomials. Because we are dealing with $x \not\equiv 0 \pmod p$, we may assume that $\deg f \leq p-2$. Applying Lemma 2.2 we see that $p-1-(|R|-1) \geq (p-1)/(t+1)$ and the desired result follows. $\square$

In particular, if $s = o(p)$ then $\deg f \sim p$ and $\operatorname{wt} f \to \infty$.

Certainly, for any S one can satisfy (3.1) with a polynomial f of degree $\deg f \leq |S| - 1 = p - 2 - s$.

Theorem 3.1 is non-trivial if the set S is dense enough, $|S| > p/2$. The next result is applicable to quite sparse sets S beginning with $|S| \sim (2p)^{1/2}$.

Theorem 3.2. *Let $p \geq 3$ and let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n = \deg f$ such that*

$$\operatorname{ind} x \equiv f(x) \pmod p, \qquad x \in S$$

for a set $S \subseteq \{1, \ldots, p-1\}$. Then

$$n \geq \frac{|S|(|S| - 1)}{2(p-2)}.$$

Proof. Let us consider the following set

$$D = \{a \equiv xy^{-1} \pmod p, \ 2 \leq a \leq p-1, \ x, y \in S\}.$$

Trivially $|D| \leq p - 2$.

On the other hand, obviously there is $a \in D$ such that there are at least $|S|(|S|-1)/|D|$ representations $a \equiv xy^{-1} \pmod p$, $x, y \in S$. Select this a and let R be the set of $x \in \{1, \dots, p-1\}$ for which both

$$\operatorname{ind} x \equiv f(x) \pmod p \quad \text{and} \quad \operatorname{ind} ax \equiv f(ax) \pmod p.$$

We see that $|R| \geq |S|(|S|-1)/(p-2)$

Also, we have, $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x$ or $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x - p + 1$. Hence either

$$f(ax) \equiv \operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} a + f(x) \pmod p$$

or

$$f(ax) \equiv \operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x - p + 1 \equiv 1 + \operatorname{ind} a + f(x) \pmod p$$

for $x \in R$. Therefore at least one of the polynomials $h_1(X) = f(aX) - f(X) - \operatorname{ind} a$ and $h_2(X) = f(aX) - f(X) - \operatorname{ind} a - 1$ has at least $|R|/2$ zeros modulo p. Because of our choice of D neither of these polynomials is identical to zero modulo p. Indeed, $h_1(0) \equiv -\operatorname{ind} a \not\equiv 0 \pmod p$ since $a \neq 1$, and $h_2(0) \equiv -\operatorname{ind} a - 1 \not\equiv 0 \pmod p$ since $0 \leq \operatorname{ind} a \leq p-2$. Thus $n \geq |R|/2$ and the desired result follows. □

Now we show that over intervals of length $H \geq p^{1/2+\varepsilon}$ polynomial approximation of the discrete logarithm requires polynomials of large degree.

Theorem 3.3. *Let $0 \leq N < N + H \leq p - 1$ and let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n = \deg f \geq 1$ such that*

$$\operatorname{ind} x \equiv f(x) + \delta_x \pmod p, \qquad N + 1 \leq x \leq N + H$$

where the "error" vector $(\delta_x)_{x=N+1}^{N+H}$ is of L_1-norm at most

$$\sum_{x=N+1}^{N+H} |\delta_x| \leq \Delta H p.$$

with $0 \leq \Delta < 0.5\pi^{-1}$. Then

$$n \geq \left(1 - 2\pi(\Delta + p^{-1})\right) \frac{H}{p^{1/2} \log p}.$$

Proof. For any real α we have

$$|\mathbf{e}(\alpha) - 1| = 2|\sin \pi\alpha| \le 2\pi|\alpha|.$$

Therefore

$$\left|\sum_{x=N+1}^{N+H} \mathbf{e}\left(\frac{\operatorname{ind} x - f(x)}{p}\right)\right| = \left|\sum_{x=N+1}^{N+H} \mathbf{e}\left(\frac{\delta_x}{p}\right)\right| \ge H - 2\pi\Delta H. \qquad (3.2)$$

We also have

$$0 \le \frac{\operatorname{ind} x}{p-1} - \frac{\operatorname{ind} x}{p} = \frac{\operatorname{ind} x}{p(p-1)} < \frac{1}{p}$$

thus

$$\left|\mathbf{e}\left(\frac{\operatorname{ind} x}{p}\right) - \mathbf{e}\left(\frac{\operatorname{ind} x}{p-1}\right)\right| < \frac{2\pi}{p}.$$

Recalling that

$$\chi(x) = \mathbf{e}\left(\frac{\operatorname{ind} x}{p-1}\right)$$

is a non-trivial multiplicative character modulo p, from Lemma 2.4 we derive

$$\begin{aligned}\left|\sum_{x=N+1}^{N+H} \mathbf{e}\left(\frac{\operatorname{ind} x - f(x)}{p}\right)\right| &\le \left|\sum_{x=N+1}^{N+H} \chi(x)\mathbf{e}\left(-\frac{f(x)}{p}\right)\right| + \frac{2\pi H}{p} \\ &\le np^{1/2}\log p + \frac{2\pi H}{p}.\end{aligned}$$

Therefore $H - 2\pi\Delta H \le np^{1/2}\log p + 2\pi H/p$ and the bound follows. □

In particular, if $\operatorname{ind} x \equiv f(x) \pmod p$ for a set $S \subseteq \{N+1, \ldots, N+H\}$ of cardinality $|S| = H - s$ then we can put $\Delta = s/H$. However in this particular case some improvement is possible.

Theorem 3.4. *Let $0 \le N < N + H \le p - 1$ and let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n = \deg f \ge 1$ such that*

$$\operatorname{ind} x \equiv f(x) \pmod p, \qquad x \in S,$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ of cardinality $|S| = H - s$. Then

$$n \ge \frac{H - 2s - 2\pi H/p}{p^{1/2}\log p}.$$

Proof. We follow the same arguments as in the proof of Theorem 3.3 but instead of (3.2) we use that

$$\left|\sum_{x=N+1}^{N+H} \mathbf{e}\left(\frac{\operatorname{ind} x - f(x)}{p}\right)\right| = \left| |S| + \sum_{x \notin S} \mathbf{e}\left(\frac{\operatorname{ind} x - f(x)}{p}\right)\right| \geq H - 2s$$

and the bound follows. □

For example, if $f(x)$ gives the correct value of $\operatorname{ind} x$ for the portion $\alpha > 0.5$ of points of an interval of length $H \geq p^{1/2+\varepsilon}$ then the degree of f is exponentially large (in terms of $\log p$), $\deg f \geq Cp^{\varepsilon} \log^{-1} p$ with some constant $C > 0$.

Now, assume that we are given a piecewise polynomial approximation of the discrete logarithm. Thus we are given $m+1$ integers $0 = N_1 < N_2 < \ldots < N_{m+1} = p-1$ and m polynomials $f_1(X), \ldots, f_m(X) \in \mathbb{Z}[x]$, of degrees $n_1 \geq 1, \ldots, n_m \geq 1$ respectively such that

$$\operatorname{ind} x \equiv f_i(x) \pmod p, \qquad x \in S \cap [N_i + 1, N_{i+1}], \quad i = 1, \ldots, m,$$

for a set $S \in \{1, \ldots, p-1\}$ of cardinality $p - 1 - s$.

We put $s_i = N_{i+1} - N_i - |S \cap [N_i + 1, N_{i+1}]|$. Then

$$\begin{aligned} \sum_{i=1}^{m} n_i &\geq \frac{1}{p^{1/2} \log p} \sum_{i=1}^{m} (N_{i+1} - N_i - 2s_i - 2\pi(N_{i+1} - N_i)/p) \\ &= \frac{(p-1)(1 - 2\pi/p) - 2s}{p^{1/2} \log p} \geq \frac{p - 2s - 2\pi - 1}{p^{1/2} \log p}. \end{aligned}$$

In particular, is $|S| \geq \alpha p$ with some $\alpha > 0.5$ then

$$\sum_{i=1}^{m} n_i \geq Cp^{1/2} \log^{-1} p$$

where $C > 0$ is a constant.

In the following theorem we consider a possibility of representation of the discrete logarithm via algebraic functions.

Theorem 3.5. *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a bi-variate polynomial of the form*

$$F(X,Y) = \sum_{i=1}^{t} X^{n_i} f_i(Y)$$

where $0 \le n_1 < \ldots < n_t < p-1$ *and polynomials* $f_i(Y) \in \mathbb{Z}[Y]$, $i = 1, \ldots, t$, *are of degree at most* n *not all identical to zero modulo* p. *Assume that*

$$F(x, \operatorname{ind} x) \equiv 0 \pmod p, \qquad x \in S,$$

for a set $S \subseteq \{1, \ldots, p-1\}$ *of cardinality* $|S| = p - 1 - s$. *Then*

$$t(n+1) \ge (p-1)/(s+1).$$

Proof. From the condition of the theorem one sees that

$$F(g^y, y) \equiv 0 \pmod p, \qquad y \in R,$$

for a set $R \in \{0, \ldots, p-2\}$ of cardinality $|R| = |S| = p-1-s$. On the other hand, from (2.2) one finds that $u(y) = F(g^y, y)$ is a linear recurring sequence of order at most $t(n+1)$. Its characteristic polynomial has the constant term $c_0 = g^{n_1} \ldots g^{n_t} \not\equiv 0 \pmod p$. Moreover, because $0 \le n_i < n_j < p-1$, then $g^{n_i} \not\equiv g^{n_j} \pmod p$ for $1 \le i < j \le t$. Taking into account that the polynomials $f_i(Y)$, $i = 1, \ldots, t$, are not identical to zero modulo p, we conclude that the sequence $(u(y))$ is not identical to zero modulo p, either. It follows from Lemma 2.1 that

$$s \ge \left\lfloor \frac{p-1}{t(n+1)} \right\rfloor \ge \frac{p-1}{t(n+1)} - 1$$

and the desired estimate follows. □

In particular, let D_p denote the smallest degree $d = \max\{\deg_X F, \deg_Y F\}$ of all non-zero modulo p polynomials $F(X, Y) \in \mathbb{Z}[X, Y]$ such that the congruence $F(x, \operatorname{ind} x) \equiv 0 \pmod p$ holds for all $x = 1, \ldots, p-1$. Thus, D_p is the degree of the discrete logarithm as an algebraic function over $\mathbb{F}_p$. For $(d+1)^2$ coefficients of such a polynomial we obtain a system of $p-1$ homogeneous equations which has a non-zero solution whenever $(d+1)^2 \ge p$. Hence together with Theorem 3.5 (setting $t = d+1$, $n = d$, $s = 0$) we obtain a very tight bound; namely

$$p^{1/2} \ge D_p \ge (p-1)^{1/2} - 1.$$

Theorem 3.5 is non-trivial if the set $|S| \sim p$. The next result is applicable to quite sparse sets S beginning with $|S| \sim p^{1/2+\varepsilon}$.

Theorem 3.6. *Let $p \geq 3$ and let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a polynomial of degree $n = \deg F$ such that*

$$F(x, \operatorname{ind} x) \equiv 0 \pmod p, \qquad x \in S$$

for a set $S \subseteq \{1, \dots, p-1\}$. Then

$$n \geq |S|^{1/2} p^{-1/4}$$

Proof. In the proof it will be more convenient to use the language of finite fields rather than congruences. Let us consider the complete factorization of $F(X,Y)$ over the algebraic closure of $\mathbb{F}_p$ (thus all factors are absolutely irreducible polynomials). Let $H(X,Y)$ be an irreducible factor of $F(X,Y)$ for which $H(x, \operatorname{ind} x) = 0$ for more than $|S|/n$ values of $x \in S$. Denote this set of x by T, $|T| \geq |S|/n$.

As in the proof of Theorem 3.2 we select $a \neq 1$ such that there are at least $|T|(|T|-1)/(p-2)$. representations $a = xy^{-1}$, $x, y \in T$. Let R be the set of $x \in \{1, \dots, p-1\}$ for which both

$$H(x, \operatorname{ind} x) = 0 \quad \text{and} \quad H(ax, \operatorname{ind} ax) = 0. \tag{3.3}$$

We see that

$$|R| \geq \frac{|S|(|S|-n)}{n^2(p-2)}$$

We have, $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x$ or $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x - p + 1$. Hence either

$$H(ax, \operatorname{ind} x + \operatorname{ind} a) = 0$$

or

$$H(ax, \operatorname{ind} x + \operatorname{ind} a + 1) = 0$$

for $x \in R$. Therefore at least one of the polynomials $H(aX, X + \operatorname{ind} a)$ and $H(aX, X + \operatorname{ind} a + 1)$ has at least $|R|/2$ zeros. We see, that $\operatorname{ind} a \neq 0$ since $a \neq 1$ and $\operatorname{ind} a \neq -1$ since $0 \leq \operatorname{ind} a \leq p-2$. Therefore, there is $b \neq 0$ such that the system of equations

$$H(X,Y) = H(aX, Y+b) = 0$$

has at least $|R|/2$ solutions.

If the polynomials $H(X,Y)$ and $H(aX,Y+b)$ are relatively prime then this system has at most n^2 solution and we obtain

$$n^2 \geq \frac{|S|(|S|-n)}{2n^2(p-2)}$$

We may assume that $n \leq |S|/3$ otherwise the bound is trivial. Then $|S|-n \geq 2|S|/3$, also $3(p-2) \geq p$ and the desired inequality follows.

If $H(X,Y)$ and $H(aX,Y+b)$ are not relatively prime, then recalling that $H(X,Y)$ is absolutely irreducible (thus so is $H(aX,Y+b)$) we see that $H(aX,Y+b) = \mu H(X,Y)$ for some constant $\mu \neq 0$. If

$$H(X,Y) = \sum_{i=0}^{n} X^i f_i(Y)$$

then for each $i = 0,\ldots,n$, $f_i(Y)$ divides $f_i(Y+b)$. Thus, if $f_i(Y) = f_i(Y+b)$. If $n < p$ (otherwise there is nothing to prove) then this is possible only if $f_i(Y)$ is a constant polynomial. Thus $H(X,Y) = H(X)$ is a polynomial in one variable. Therefore, the system 3.3 has at most n solutions. Hence

$$n \geq \frac{|S|(|S|-n)}{2n^2(p-2)}$$

and the desired result follows. □

4 Approximation of the Discrete Logarithm Modulo $p-1$

In this section we consider various approximations and representation of the discrete logarithmmodulo a divisor d of $p-1$. Certainly the case of $d=2$ is of special interest because corresponds to representation of the last bit of $\operatorname{ind} x$.

Moreover, instead of polynomials we consider a much wider class of representations via linear recurring sequences.

Theorem 4.1. *Let $0 \le N < N + H \le p - 1$ and let $d > 1$ be a divisor of $p-1$. Let $(u(x))$ be an integer linear recurring sequence of order n such that*

$$\operatorname{ind} x \equiv u(x) \pmod d, \qquad x \in S,$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ of cardinality $|S| = H - s$. Then

$$n \ge \frac{H}{2s + p^{1/2}\log p} - 2.$$

Proof. We see that for at least $H - n - (n+1)(H - |S|) \ge H - (n+2)s$ values of $x = N+1, \ldots, N+H$,

$$\operatorname{ind}(x+i) \equiv u(x+i) \pmod p, \qquad i = 0, \ldots, n.$$

Put $c_n = -1$. From (2.1) we see that

$$\sum_{i=0}^{n} c_i \operatorname{ind}(x+i) \equiv 0 \pmod d. \tag{4.1}$$

for at least $H-(n+2)s$ values of $x = N+1, \ldots, N+H$. The congruence (4.1) is equivalent to the statement that the product $x^{c_0}(x+1)^{c_1}\ldots(x+n)^{c_n}$ is d-th power residue modulo p. Thus, for a non-trivial character χ of $\mathbb{F}_p^*$ of order d, we have

$$\left| \sum_{x=N+1}^{N+H} \chi\left(x^{c_0}(x+1)^{c_1}\ldots(x+n)^{c_n}\right) \right| \ge H - 2(n+2)s.$$

On the other hand, because $c_n = -1$ Lemma 2.3 can be applied. Therefore,

$$H - 2(n+2)s \le (n+1)p^{1/2}\log p$$

and the result follows. $\square$

In particular, if $H \ge \max\{sp^{\delta}, p^{1/2+\delta}\log p\}$ with some fixed $\delta > 0$ then the order of the sequence must be exponentially large, $n \gg p^{\delta}$.

It is interesting to note that the lower bound does not depend on the divisor d. In particular, selecting $d = 2$ we see that even the last bit of $\operatorname{ind} x$ cannot be given by a linear recurring sequence of small order.

In particular, using $s = 0$ one obtains a lower bound $\Omega(p^{1/2}\log^{-1} p)$ on the *linear complexity* of the discrete logarithm modulo a divisor d of $p-1$. We recall that the linear complexity of a sequence $a_1, \ldots, a_m$ over a ring $\mathcal{R}$ is defined as the smallest order L of a linear recurrent relation

$$a_{x+L} = c_{L-1}a_{x+L-1} + \ldots + c_0 a_x, \qquad x = 1, \ldots, m-L,$$

among elements of this sequence [22].

Also, assume that we are given a piecewise representation of the discrete logarithm via linear recurring sequences, thus we are given $m+1$ integers $0 = N_1 \le N_2 \le \ldots \le N_{m+1} = p-1$, m divisors $d_1, \ldots, d_m$ of $p-1$ and m linear recurring sequences $(u_1(x)), \ldots, (u_m(x))$, of orders $n_1, \ldots, n_m$ respectively such that

$$\operatorname{ind} x \equiv u_i(x) \pmod{d_i}, \qquad x \in [N_i + 1, N_{i+1}], \quad i = 1, \ldots, m.$$

Then

$$\sum_{i=1}^{m} n_i \ge \frac{1}{p^{1/2}\log p}\sum_{i=1}^{m}(N_{i+1} - N_i) - m = (p-1)p^{-1/2}\log^{-1} p - m$$

On the other hand, obviously

$$\sum_{i=1}^{m} n_i \ge m$$

thus

$$\sum_{i=1}^{m} n_i \ge 0.5(p-1)^{1/2}\log^{-1} p.$$

Obviously one can apply the result above to the special case of polynomials.

5 Approximation of the Discrete Logarithm by Boolean Functions

In [5] (see also [7]) the identity

$$x^{(q-1)/2} = \begin{cases} 1, & \text{if } x \text{ is a quadratic residue in } \mathbb{F}_q, \\ -1, & \text{if } x \text{ is a quadratic non-residue in } \mathbb{F}_q, \end{cases}$$

has been used to obtain the lower bound $\Omega(\log q)$ on the depth of arithmetic circuits over $\mathbb{F}_q$ deciding wether $x \in \mathbb{F}_q^*$ is a quadratic residue (the most important thing is that the degree $(q-1)/2$ is large). Here we consider Boolean circuits. It should be noted that our bound $\Omega(\log\log p)$ (which we prove for prime fields $\mathbb{F}_p$ only) on their depth is weaker. This actually agrees with the expectation that for this particular question Boolean circuits are exponentially more powerful than arithmetic ones, see [7] for a discussion of this phenomena and a survey of relevant results.

Each Boolean function $B(X_1, \dots, X_r)$ we consider as a multilinear polynomial of degree n over $\mathbb{F}_2$ of the form

$$B(U_1, \dots, U_r) = \sum_{k=0}^{n} \sum_{1 \le i_1 < \dots < i_k \le r} A_{i_1 \dots i_k} U_{i_1} \dots U_{i_r} \in \mathbb{F}_2[U_1, \dots, U_r]. \quad (5.1)$$

We consider Boolean functions producing the last bit of $\operatorname{ind} x$ from the bit representation of x. We also assume that all numbers contain the same number r of bits (adding several leading zeros if necessary) where $r = \lfloor \log p \rfloor$. Thus each such function is defined on a portion $1 \le x \le 2^r - 1 \le p - 1$ of the complete residue system modulo p.

Theorem 5.1. *Let a Boolean function $B(U_1, \dots, U_r)$ be such that for any x, $1 \le x \le 2^r - 1$,*

$$B(u_1, \dots, u_r) = \begin{cases} 0, & \text{if } x \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } x \text{ is a quadratic non-residue modulo } p, \end{cases}$$

where $x = u_1 \dots u_r$ is the bit representation of x , $r = \lfloor \log p \rfloor$. Then

$$\operatorname{wt} B \ge 2^{-3/2} p^{1/4} \log^{-1/2} p - 1$$

Proof. Put $t = \operatorname{wt} B$ and define k by the inequalities

$$2^k > t + 1 \ge 2^{k-1}.$$

For each $m = 1, \dots, 2^k - 1$ we consider the function

$$B_m(V_1, \dots, V_{r-k-1}) = B(V_1, \dots, V_{r-k}, e_1, \dots, e_k)$$

where $m = e_1 \dots e_k$ is the bit representation of m. Obviously the total number of distinct monomials in $V_1, \dots, V_{r-k}$ occurred in all these functions does not exceed t. Therefore, because of the choice of k, one can find a non-trivial linear combination

$$\sum_{m=1}^{2^k-1} c_m B_m(V_1, \dots, V_{r-k}), \qquad c_1, \dots, c_{2^k-1} \in \mathbb{F}_2,$$

which vanishes identically.

Let $\chi(z)$ be the quadratic character modulo p. From the condition of the theorem we see,

$$\chi(x) = (-1)^{B(x_1, \dots, x_r)}.$$

Therefore, for $0 \le y \le 2^{r-k} - 1$ we have

$$\prod_{m=1}^{2^k-1} \chi(2^k y + m)^{c_m} = (-1)^{\sum_{m=1}^{2^k-1} c_m B_m(v_1, \dots, v_{r-k})} = 1$$

where $y = v_1 \dots v_{r-k}$ is the binary expansion of y.

Combining this result with Lemma 2.3 we get

$$2^{r-k} = \sum_{y=0}^{2^{r-k}-1} \chi\left(\prod_{m=1}^{2^k-1} (2^k y + m)^{c_m}\right) \le 2^k p^{1/2} \log p.$$

Hence, $2^{2k} \ge 2^r p^{-1/2} \log^{-1} p \ge 0.5 p^{1/2} \log^{-1} p$. And finally we derive that $t + 1 \ge 2^{k-1} \ge 2^{-3/2} p^{1/4} \log^{-1/2} p$. □

To estimate the degree of $n = \deg B$ from below we recall the asymptotic

$$\log \binom{N}{\gamma N} \sim H(\gamma) N$$

where $H(\gamma) = -\gamma \log \gamma - (1-\gamma) \log(1-\gamma)$ which holds for any fix γ, $0 < \gamma < 1/2$ and $N \to \infty$, see [17], Section 10.11. Then from the inequality

$$t \le \binom{r}{n}$$

one can easily derive that under the condition of Theorem 5.1

$$n \geq \vartheta \log p + o(\log p) \tag{5.2}$$

where $\vartheta = 0.041\ldots$ is the root of the equation $H(\vartheta) = 1/4$, $0 < \vartheta < 1/2$.

Now we obtain a lower bound for the parallel complexity of computing the last bit of $\operatorname{ind} x$ by Boolean circuits.

We deal with circuits which use addition and multiplication modulo 2 as their basic operations. Certainly the circuits using more common logical **AND, OR, NOT** can be simulated by such a circuit with only a constant factor increase of the depth.

We consider Boolean circuits of depth d over $\mathbb{F}_q$ of the following class $\mathrm{BC}_q(d)$.

Given a sequence of bits $u_1, \ldots, u_r$, such a circuit $C \in \mathrm{BC}_q(d)$ computes the values of some Boolean function $B(u_1, \ldots, u_r)$ in the following way.

Each circuit $C \in \mathrm{BC}_q(d)$ has one special *starting* level and d levels of Boolean processors which are called *gates*. Levels are numbered from 0 for the starting level to d for the last level. Each level may have an unlimited number of gates, with only one gate on the last level.

Each gate of the starting level, accept either some constant or the value of one the input variables $u_1, \ldots, u_r$ for which we want to compute the function B.

Each gate of level $k \geq 1$ accepts 2 values from some gates of previous levels, ϕ_1, ϕ_2, and then computes and outputs the value of $\phi_1 \# \phi_2$ where $\#$ stays for one of the arithmetic operations over $\mathbb{F}_2$, that is $\# \in \{+, \times\}$.

The gate of the last level outputs the result of the computation $C(u_1, \ldots, u_r)$.

Theorem 5.2. *Assume that there is a circuit $C \in BC_q(d)$ such that given the bit representation $u_1 \ldots u_r$ of x it computes*

$$C(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } x \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } x \text{ is a quadratic non-residue modulo } p, \end{cases}$$

where $1 \leq x \leq 2^r - 1$, $r = \lfloor \log p \rfloor$. Then

$$d \geq \log \log p + O(1)$$

Proof. We can assume that the kth level has no more than 2^{d-k} gates. Indeed the last dth level may utilize no more than 2 gates of the $(d-1)$th level, those may utilize no more than 4 gates of the $(d-2)$th level and so on.

Now it is easy to see that the output values $C(u_1, \dots, u_r)$ coincide with values of some Boolean function of degree at most 2^d. Applying (5.2), we obtain the result. $\square$

Now we show that the same method which is used in the proof of Theorem 5.1 can be used in studying one more characteristic of those functions. Following [28], for a Boolean function $B(U_1, \dots, U_r)$ we define the *critical complexity* $c(B)$ as the largest integer $s \le r$ such that there is a binary vector $x = (x_1, \dots, x_r)$ for which $B(x) \ne B(x^{(i)})$ for s values of i, $1 \le i \le r$, where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate. In other words, $c(B)$ is the largest over all binary vector $x = (x_1, \dots, x_r)$ number of points y on the unit Hamming sphere around x with $B(y) \ne B(x)$. This function gives a lower bound for several other complexity characteristics of B, see Chapter 13 of [28].

Theorem 5.3. *Let a Boolean function $B(U_1, \dots, U_r)$ be such that for any x, $1 \le x \le 2^r - 1$,*

$$B(u_1, \dots, u_r) = \begin{cases} 0, & \text{if } x \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } x \text{ is a quadratic non-residue modulo } p, \end{cases}$$

where $x = u_1 \dots u_r$ is the bit representation of x , $r = \lfloor \log p \rfloor \ge 3$. Then

$$c(B) \ge 0.25r - \log r - 1$$

Proof. Put $k = \lfloor 0.25r - \log r \rfloor$. In order to show that $c(B) \ge k$ we prove that there is $1 \le x \le 2^{r-k} - 1$ such that $2^k x$ is a quadratic non-residue but its k flips $2^k x + 2^i$, $i = 0, \dots, k-1$, are quadratic residues modulo p. Indeed, assume that such x does not exist. Then

$$\Big(\chi(2^k x) - 1\Big) \prod_{i=0}^{k-1} \Big(\chi(2^k x + 2^i) + 1\Big) = 0$$

for $x = 1, \dots, 2^{r-k} - 1$, where $\chi(z)$ is the quadratic character modulo p. Therefore,

$$\sum_{x=1}^{2^{r-k}-1} \Big(\chi(2^k x) - 1\Big) \prod_{i=0}^{k-1} \Big(\chi(2^k x + 2^i) + 1\Big) = 0. \tag{5.3}$$

After simple evaluation one sees that the right hand side contains one "main" term $-2^{r-k}+1$ and $2^{k+1}-1$ terms of the form

$$\pm \sum_{x=1}^{2^{r-k}-1} \chi\left((2^k x + j_1)\dots(2^k x + j_m)\right)$$

where $m \le k+1$ and $0 \le j_1 < \dots < j_m \le 2^{k-1}$. Applying Lemma 2.3 we see that each such term does not exceed $mp^{1/2}\log p$. Thus from (5.3) we derive

$$-2^{r-k} + 1 + \sum_{m=1}^{k+1} \binom{k+1}{m} mp^{1/2} \log p \ge 0.$$

Therefore

$$2^{r-k} - 1 \le \sum_{m=1}^{k+1} \binom{k+1}{m} mp^{1/2} \log p = 2^k(k+1)p^{1/2} \log p$$

From our choice of k we see that $\log r \ge \log 3 \ge 5/4$, thus $k+1 \le (r-1)/4$. Also, $\log p \le r+1$ and $p^{1/2} \le 2^{r/2+1/2}$, hence

$$2^{r-k} - 1 \le 2^k(k+1)p^{1/2}\log p \le 2^{r/2+k-3/2}(r-1)(r+1) < 2^{r/2+k-1}r^2 - 1$$

or $2^{2k-1} > 2^{r/2}r^{-2}$, $k > 0.25r - \log r + 0.5$ which contradicts to our selection of k. □

Combining this result with Theorem 4.3 of Chapter 13 of [28] one gets the lower bound $C \log\log p + O(1)$ where

$$C = \frac{1}{\log\left(5 + (21)^{1/2}\right) - 1} = 0.442\dots$$

on the PRAM complexity of B (the complexity on a parallel random access machine with an unlimited number of processors of unlimited power). The bound is weaker than that of Theorem 5.2 but it concerns a more powerful (but maybe less realistic) computational model.

6 The Diffie-Hellman Cryptosystem

Let g be a primitive root of a finite field $\mathbb{F}_q$ of q elements. One of the most popular public-key cryptosystems, the Diffie-Hellman cryptosystem is based on the assumption that recovering the value of g^{xy} from the known values of g^x and g^y is essentially equivalent to the discrete logarithm problem and therefore is hard. Here we show that even computation g^{x^2} from g^x is cannot be realized by a polynomial of low degree. We remark (although it is not essential for the rest) that indeed the general case can be reduced to this one via the identity

$$g^{(x+y)^2} g^{-x^2} g^{-y^2} = g^{2xy}$$

We note that square root extracting which can be done in deterministic polynomial time because a primitive root g of $\mathbb{F}_q$ is known [24]. It is demonstrated in [18] that the correct square root can easily be determined (and the entire reduction can be done $O(\log^2 q)$ arithmetic operations in $\mathbb{F}_q$.

Theorem 6.1. *Let $f(X) \in \mathbb{F}_q[X]$ be such that*

$$g^{x^2} = f(g^x), \qquad x \in S \tag{6.1}$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ of cardinality $|S| = H - s$ with $H \le q-1$. Then

$$\deg f \ge H - 2s - 3.$$

Proof. Let R be the set of $x \in \{N+1, \ldots, N+H\}$ for which both $g^{x^2} = f(g^x)$ and $g^{(x+1)^2} = f(g^{x+1})$. We see that, $|R| \ge H - 1 - 2(H - |S|) = H - 1 - 2s$. Now, for $u = g^x$ with $x \in R$ we have

$$f(gu) = f(g^{x+1}) = g^{x^2+2x+1} = g^{2x+1} f(g^x) = gu^2 f(u).$$

So the polynomial $h(X) = gX^2 f(X) - f(gX)$ has at least $|R|$ zeros in $\mathbb{F}_q$ and is obviously not identical to zero. Therefore $|R| \le \deg h = \deg f + 2$ thus $\deg f \ge |R| - 2 \ge H - 2s - 3$. $\square$

Thus, as in the case of the discrete logarithm, if $s = o(H)$ then $\deg f \sim H$. Also, if $N = 0$, $H = q-1$, one can show that $\mathrm{wt}\, f \ge (q-1)/4s$.

Certainly, for any S one can satisfy (6.1) with a polynomial f of degree $\deg f \leq |S| - 1 = H - s - 1$.

Theorem 6.1 is non-trivial if the set S is dense enough on some interval, $|S| > H/2$. The next result is applicable to arbitrary quite sparse sets S beginning with $|S| \sim 2H^{2/3}$.

The proof of the following result was shown to the author by Don Coppersmith, it improves, simplifies and generalises the original version of the author.

Theorem 6.2. *Let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree $n = \deg f$ such that*

$$g^{x^2} = f(g^x), \qquad x \in S$$

for a set $S \subseteq \{N+1, \dots, N+H\}$ with $H \leq q-1$. Then

$$n \geq |S|^2/2H - 4H/|S| - 1$$

Proof. Let us define $K = \lfloor 2H/|S| \rfloor$ and consider the $K+1$ shift-sets $S_i = S - i$, $i = 0, \dots, K$. They all belong to the interval of length of $H + K$, thus denoting $R_{i,j} = S_i \cap S_j$ we obtain

$$(K+1)|S| - \sum_{0 \leq i < j \leq K} |R_{i,j}| = \sum_{i=0}^{K} |S_i| - \sum_{0 \leq i < j \leq K} |R_{i,j}| \leq | \cup_{i=0}^{K} S_i| \leq H + K.$$

Therefore, there is a pair $0 \leq i < j \leq k$ such that

$$|R_{0,j-i}| = |R_{i,j}| \geq 2|S|/K - 2(H+K)/K(K+1) \geq |S|/K - 1 \geq |S|^2/2H - 1$$

For this pair we put $k = j - i$ and let $R = R_{0,k}$. Then for any $x \in R$ we have both

$$g^{x^2} = f(g^x) \quad \text{and} \quad g^{(x+k)^2} = f(g^{x+k}).$$

Therefore,

$$f(g^{x+k}) = g^{(x+k)^2} = g^{x^2} g^{2kx} g^{k^2} = g^{2kx} g^{k^2} f(g^x).$$

Thus the equation $f(g^k u) = g^{k^2} u^{2k} f(u)$ is satisfied for each $u = g^x$ with $x \in R$. On the other hand, it can be reduced to the form

$$g^{k^2} u^{2k} f(u) - f(g^k u) = 0$$

and therefore has at most $2k + n$ solutions (because $k > 0$ the polynomial on the left hand side is not identical to zero). Hence $n \geq |R| - 2K$. $\square$

Now we consider representation via algebraic functions.

Theorem 6.3. *Let $F(U,V) \in \mathbb{F}_q[U,V]$ be a not identical to zero polynomial with*

$$\deg_U F = n, \qquad \deg_V F = m.$$

Assume that

$$F(g^x, g^{x^2}) = 0, \qquad x \in S,$$

for a set $S \subseteq \{N+1,\dots,N+H\}$ of cardinality $|S| = H - s$ with $H \le q-1$. Then

$$(m+1)(n+s+1) + \frac{2}{3}m(m+1)(m+2) \ge H+1.$$

Proof. First of all we write down the polynomial $F(U,V)$ in the form

$$F(U,V) = \sum_{i=1}^{t} V^{k_i} f_i(U)$$

where $f_i(U) \in \mathbb{F}_q[U]$, $i = 1,\dots,t$, are non-zero polynomials, $0 \le k_1 < \ldots < k_t \le m$, $t \le m+1$.

We see that there is a set R of cardinality at least

$$|R| \ge H - t + 1 - t(H - |S|) = H - t(s+1) + 1 \ge H - (m+1)(s+1) + 1$$

such that for any $x \in R$

$$F(g^{x+j}, g^{(x+j)^2}) = 0, \qquad j = 0,\dots,t-1.$$

Therefore, for any $x \in R$, the homogeneous system of equations

$$\sum_{i=1}^{t} Z_i g^{2jk_ix + j^2k_i} f_i(g^{x+j}) = 0, \qquad j = 0,\dots,t-1.$$

has a non-zero solution $Z_i = g^{k_ix^2}$, $i = 1,\dots,t$. Hence its determinant equals zero. Thus we see that the polynomial

$$\Delta(U) = \det\left(g^{(j-1)^2k_i} U^{2k_i(j-1)} f_i(g^{j-1}U)\right)_{i,j=1}^{t}$$

has at least $|R|$ zeros $u = g^x$, $x \in R$. Now we show that $\Delta(U)$ is not identical to zero. Indeed, let $\pi \in S_t$ be a permutation of the set $\{0, \ldots, t-1\}$. The term of Δ corresponding to the permutation π is of degree

$$\sum_{i=1}^{t} (\deg f_i + 2k_i \pi(i)) = \sum_{i=1}^{t} \deg f_i + 2 \sum_{i=1}^{t} k_i \pi(i).$$

It is know that for any two sequences of non-negative numbers $0 \le a_1 < \ldots < a_t$ and $0 \le b_1 < \ldots < b_t$ the sum $a_1 b_{\pi(1)} + \ldots + a_t b_{\pi(t)}$ attains it maximal value for the identical permutation and that value is strictly greater than values corresponding to other permutations. So $\Delta(U)$ is a non-zero polynomial of degree

$$\begin{aligned} \deg \Delta &= \sum_{i=1}^{t} \deg f_i + 2 \sum_{i=1}^{t} k_i (i-1) \le (m+1)n + 2 \sum_{i=1}^{m+1} i(i-1) \\ &= (m+1)n + \frac{2}{3} m(m+1)(m+2), \end{aligned}$$

and the result follows. $\square$

In particular, if $d = \max\{n, m\}$ then

$$d \ge \min\{H/2(s+1), (H/2)^{1/3}\} - 1.$$

Once again, one can see that Theorem 6.3 is quite precise. Indeed, it is easy to see that for any m and n with $(m+1)(n+1) > |S| = H - s$ there is a polynomial F satisfying the conditions of the theorem.

The following result is non-trivial for sparse sets with at least $H^{2/3+\varepsilon}$ elements.

Theorem 6.4. *Let $F(U, V) \in \mathbb{F}_q[U, V]$ be a not identical to zero polynomial of degree $n = \deg F$ such that*

$$F(g^x, g^{x^2}) = 0, \qquad x \in S$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$. Then

$$n \ge 0.5 |S|^{3/5} H^{-2/5}$$

Proof. Let us consider the complete factorization of $F(U,V)$ over the algebraic closure of $\mathbb{F}_q$ (thus all factors are absolutely irreducible polynomials). Let $H(U,V)$ be an irreducible factor of $F(U,V)$ for which $H(g^x, g^{x^2}) = 0$ for more than $|S|/n$ values of $x \in S$. Denote this set of x by T, $|T| \geq |S|/n$.

As in the proof of Theorem 6.2 we select $k \leq 2H/|T|$ for which both

$$H(g^x, g^{x^2}) = 0 \quad \text{and} \quad H(g^{(x+k)}, g^{(x+k)^2}) = 0. \tag{6.2}$$

hold at least $|T|^2/2H - 1$ values of x. Then we see that the system of equations

$$H(U,V) = H(bU, aVU^m) = 0.,$$

where $a = g^{k^2}$, $b = g^k$, $m = 2k$, has at least $|S|^2/2n^2H - 1$ solutions.

If the polynomials $H(U,V)$ and $H(bU, aVU^m)$, of degrees at most n and $n(m+1)$, respectively, are relatively prime then this system has at most $n^2(m+1)$ solutions and we obtain

$$|S|^2/2n^2H - 1 \leq n^2(2Hn/|S| + 1) \leq 3n^3H/|S|.$$

We may assume that $n \leq |S|/2H^{-1/2}$ otherwise the bound is trivial. Then $|S|^2/2n^2H - 1 \geq |S|^2/4n^2H$ and the desired inequality follows.

If $H(U,V)$ and $H(bU, aVU^m)$ are not relatively prime, then recalling that $H(U,V)$ is absolutely irreducible and that they are of the same V-degree we see that $H(bU, aVU^m) = G(U)H(U,V)$ with some polynomial $G(U)$ (over the algebraic closure of $\mathbb{F}_q$). If

$$H(U,V) = \sum_{i=0}^{n} V^i f_i(U)$$

then for each $i = 0, \ldots, n$, $f_i(U)G(U) = f_i(U)U^{im}$. This is possible if only one of $f_0(U), \ldots, f_n(U)$ is not identical to zero. Thus $H(U,V) = V^d f(U)$. where $d \leq n$ and $f(U)$ is a non-zero polynomial of degree at most n. Thus the system (6.2) has at most n solutions. Hence

$$n \geq |S|^2/2n^2H - 1$$

and the desired result follows. $\square$

Now we obtain a lower bound on the parallel complexity of breaking the Diffie-Hellman cryptosystem by *probabilistic branching arithmetic circuits*. In fact the method above allows to obtain a lower bound for a weaker question about verifying if $\mathrm{ind}\, v = \mathrm{ind}^{\,2} u$ for a given $u, v \in \mathbb{F}_q^*$. Moreover it is enough to require that such a circuit works correctly on a very small portion of the input.

We consider the of the following class $\mathrm{PAC}_q(d)$ of circuits of depth d over $\mathbb{F}_q$.

Each circuit $C \in \mathrm{PAC}_q(d)$ has one special *starting* level and d levels of arithmetic processors which are called *gates*. Levels are numbered from 0 for the starting level to d for the last level. Each level may have an unlimited number of gates, with only one gate on the last level.

Each gate of the starting level, accept either some constant constant or the value of one of two variables $u, v \in \mathbb{F}_q$ for which we want to verify that $\mathrm{ind}\, v = \mathrm{ind}^{\,2} u$.

Each gate of level $d-1 \ge k \ge 1$ accepts 4 values from some gates of previous levels, $\phi_1, \phi_2, \phi_3, \phi_4$ and one special *branching* value ψ which is either some value computed on a previous level or the value of a random variable taking values 0 and 1 with probability 1/2.

Then it computes and outputs the value of $\phi_1 \# \phi_2$ if $\psi \neq 0$ and $\phi_3 \# \phi_4$ otherwise, where # stays for one of the arithmetic operations over $\mathbb{F}_q$, that is $\# \in \{+, -, \times, /\}$ (not necessary the same each time).

The gate of the last levels accepts only one value ψ (which is either some value computed on a previous level or the value of a random variable taking values 0 and 1 with probability 1/2) and outputs $C(u, v) = \mathbf{YES}$ if $\psi = 0$ and $C(u, v) = \mathbf{NO}$ otherwise.

Theorem 6.5. *Assume that there is a circuit $C \in PAC_q(d)$ such that given $u = g^x$, $v = g^{x^2}$, $u, v \in \mathbb{F}_q^*$ it outputs* **YES** *for all x from some set $S \subseteq \{N+1, \ldots, N+H\}$, $1 \le H \le q-1$, of cardinality $|S| \ge H^\delta$ with probability*

$$\Pr[C(g^x, g^{x^2}) = \mathbf{YES}] \ge |S|^{-\gamma}$$

where $\gamma, \delta > 0$ with are some constants such that

$$(1-\gamma)\delta > 2/3$$

and outputs **NO** *for any other inputs u, v. Then*

$$d \geq C(\gamma, \delta) \log H$$

where the constant $C(\gamma, \delta) > 0$ depends on γ and δ only.

Proof. We can assume that the kth level has no more than 5^{d-k} gates. Indeed the last dth level may utilize no more than 5 gates of the $(d-1)$th level, those may utilize no more than 25 gates of the $(d-2)$th level and so on.

Let $\vartheta = (\vartheta_1, \ldots, \vartheta_l)$ be the vector or random variables used by the circuit C. Obviously k does not exceed the total number of gates, that is $l = O(5^d)$. For each fixed vector $\vartheta = (\vartheta_1, \ldots, \vartheta_l)$ we obtain a deterministic circuit C_ϑ.

Let $R(\vartheta)$ be the set of $x \in S$ such that given $u = g^x$, and $v = g^{x^2}$, C_ϑ works correctly, $C_\vartheta(u, v) =$ **YES**. Therefore, there is $\vartheta_0 \in \{0,1\}^l$ for which C_ϑ produces the correct result for at least $|S|^{1-\gamma}$ values of $x \in S$.

We define the sequence of sets $R_1, \ldots, R_d$ recursively. We put $R_1 = R(\vartheta_0)$. Assume that the set $R_{i-1}(\vartheta)$ has been already defined, $2 \leq i \leq d$. We define R_i as the set of $x \in R_{i-1}$ for which $\psi(g^x, g^{x^2}) \neq 0$ for all non-constant functions ψ defining branching on the ith level. Obviously, for $u \in R_{i-1}$ all such functions $\psi(V, U)$ of the ith level are rational functions in V and U of degree at most 2^{i-1}. It is follows from Theorem 6.4 that the number of $x \in R_{i-1} \subseteq S$ for which such a function vanishes is at most $2^{5i} H^{2/3}$. Therefore

$$|R_{i-1}| \geq |R_i| - 5^{d-i} 2^{5i} H^{2/3}$$

Taking into account that because of our selection of ϑ_0, $|R_1| \geq |S|^{1-\gamma}$ we find that

$$|R_d| \geq |S|^{1-\gamma} + O(32^d H^{2/3}) \geq 0.5|S|^{1-\gamma}$$

if

$$d \leq \log_{33}(|S|^{1-\gamma} H^{-2/3}) \leq ((1-\gamma)\delta - 2/3) \log_{33} H$$

and H is large enough (otherwise there is nothing to prove). So, there are at least $0.5|S|^{1-\gamma}$ values of $x \in S$ for which the circuit works without branching and outputs the correct answer. We note that the function ψ of the last level cannot be a constant, thus this is a non-constant rational function of degree at most 2^{d-1} having at least $|R_d|$ zeros. From Theorem 6.4 we find

$$2^{d-1} \geq 0.5|R_d|^{3/5} H^{-2/5} \geq 0.5 H^{3(1-\gamma)\delta/5 - 2/5}$$

and the claim follows. $\square$

Certainly the constant $C(\gamma, \delta)$ can be explicitly evaluated.

Also, we see that if $H \geq \exp((\log q)^{\varepsilon})$ with some $\varepsilon > 0$ then the depth cannot be polynomial in $\log \log q$.

The bounds above are related to the arithmetic model of computation. Generally speaking, this model seems more powerful than the Boolean model (in some situations it is) there is no proof that this is really the case for our particular situation. Moreover, as a dual question computing powers in parallel (over finite fields of small characteristic) shows in some cases the Boolean model is exponentially more powerful than the arithmetic model [5, 6]. Generally, obtaining non-trivial lower bounds for the Boolean model of computation is an interesting (and probably very hard) open question.

As the very first step, below we derive a lower bounds on the degree of Boolean functions giving the binary coordinate vector of $g^{x^2} \in \mathbb{F}_{2^r}$ with respect to some fixed basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ from the binary coordinate vector of $g^x \in \mathbb{F}_{2^r}$. As before, each Boolean function $B(U_1, \ldots, U_r)$ we consider as a multilinear polynomial over $\mathbb{F}_2$ of the form (5.1).

We also fix a basis $\omega_1, \ldots, \omega_r$ of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$.

Theorem 6.6. *Let Boolean functions $B_i(U_1, \ldots, U_r)$, $j = 1, \ldots, r$, be such that*

$$g^{x^2} = \omega_1 B_1(u_1, \ldots, u_r) + \ldots + \omega_r B_n(u_1, \ldots, u_r)$$

where

$$g^x = \omega_1 u_1 + \ldots + \omega_r u_r,$$

for at least $2^r - 1 - s$ values of $x \in \mathbb{F}_{2^r}^*$. Then

$$\max_{1 \leq i \leq r} \deg B_i \geq \frac{r - \log(2s+1) - 2}{\log r}.$$

Proof. Denote by

$$\mathrm{Tr}\,(z) = z + z^2 + \ldots + z^{2^{r-1}}$$

the trace of $z \in \mathbb{F}_{2^r}$ to $\mathbb{F}_2$ and let $\vartheta_1, \ldots, \vartheta_r$ be the dual basis to $\omega_1, \ldots, \omega_r$, see [16]. That is $\mathrm{Tr}\,(\vartheta_i \omega_j) = 1$ if $i = j$ and $\mathrm{Tr}\,(\vartheta_i \omega_j) = 0$ if $i \neq j$, $1 \leq i, j \leq r$.

Therefore,
$$u = \sum_{i=1}^{r} \omega_i \mathrm{Tr}\,(\vartheta_i u).$$
Thus from the condition of the theorem we obtain
$$g^{x^2} = \sum_{i=1}^{r} \omega_i B_i \left(\mathrm{Tr}\,(\vartheta_1 g^x), \ldots, \mathrm{Tr}\,(\vartheta_r g^x)\right)$$
for at least $2^r - 1 - s$ values of $x \in \mathbb{F}_{2^r}^*$. As in the proof of Theorem 6.1 we obtain that the polynomial $gU^2 f(U) - f(gU)$, where
$$f(U) = \sum_{i=1}^{r} \omega_i B_i \left(\mathrm{Tr}\,(\vartheta_1 U), \ldots, \mathrm{Tr}\,(\vartheta_r U)\right)$$
has at least $2^r - 1 - 2s$ zeros over $\mathbb{F}_{2^r}$.

Let $n = \max_{1 \le i \le n} B_i$. It is easy to see that $f(U)$ contains at most
$$\mathrm{wt}\, f \le t(r, n) = r^n + r^{n-1} + \ldots + r + 1 = \frac{r^{n+1} - 1}{r - 1}$$
monomials corresponding to the powers of U with exponents
$$2^{r_1} + \ldots + 2^{r_k}, \quad 1 \le r_1, \ldots, r_k \le r, \ 0 \le k \le n.$$
Denote by $h(U)$ the polynomial obtained from $gU^2 f(U) - f(gU)$ after the reduction of powers of all its monomials modulo $q - 1$. Obviously, $h(U)$ still has at least $2^r - 1 - 2s$ zeros over $\mathbb{F}_{2^r}$.

We remark that if $\mathrm{wt}\, f < 2^r - 1$ then $h(U)$ is a non-zero polynomial. Indeed, let E denote the set of exponents of all the monomials of $f(U)$ reduced modulo $q - 1$. Since by $f(U)$ is not a zero polynomial on $\mathbb{F}_{2^r}^*$ then $E \neq \emptyset$. Hence, if $h(U)$ is identical to zero then $E \equiv E + 2 \pmod{2^r - 1}$. However the last property mean that $E \equiv E + 2m \pmod{2^r - 1}$ for any integer m, thus $E = \{0, 1, \ldots, 2^r - 2\}$. Finally, we see that if $t(n, d) < 2^r - 1$ then $h(U)$ is a non-zero polynomial of weight $\mathrm{wt}\, h \le 2\mathrm{wt}\, f \le 2t(r, n)$ with at most $2s + 1$ non-zeros over $\mathbb{F}_{2^r}$. From Lemma 2.2 we see
$$\frac{2^r - 1}{2t(r, n)} \le 2s + 1.$$
Trivially, $2^r - 1 \ge 2^{r-1}$ hence $t(r, n) \le 2r^n$ thus $r^n \ge 2^{r-2}/(2s + 1)$ and the bound follows. $\square$

An analogue of Theorems 5.2 and 6.5 can be obtained as well (for deterministic Boolean circuits). Using Theorem 6.6 one can show that for any $\alpha < 1$ there is a constant $C > 0$ such that any deterministic branching Boolean circuit computing the coordinates of g^{x^2} from the coordinates of $g^x \in \mathbb{F}_{2^r}$ for all but at most $2^{\alpha r}$ values of $x = 0, \ldots, 2^r - 2$ must be of depth at least $C \log r$.

This lower bound is double logarithmic in terms of the field size so it does not rule out the possibility that the question belongs to the complexity class **NC** but at least shows that it cannot be done "superquickly" even with unlimited parallelism.

7 Permutation Polynomials, Powers and Symmetric Boolean Functions

Let $f(X) \in \mathbb{F}_q[X]$ be a non-linear permutation polynomial (that is the mapping $x \to f(x)$ is bijective on $\mathbb{F}_q$. One can also consider the inverse mapping $h(f(x)) = x$, which obviously is also bijective and as any mapping over $\mathbb{F}_q$ is given by some polynomial $h(X) \in \mathbb{F}_q[X]$. It is mentioned in [20], Problem 10, that apparently both of these polynomials cannot be of small degree. Here we show that this is really the case.

Theorem 7.1. *Let $f(X), h(X) \in \mathbb{F}_q[X]$ be two permutation polynomials of degrees $\deg f = n$ and $\deg h = m$ which generate relatively inverse mappings. If $\max\{n, m\} > 1$ then $nm \geq q$.*

Proof. We see that $h(f(x)) = x$ for $x \in \mathbb{F}_q[X]$. Therefore the polynomial $h(f(X)) - X$ is of degree $nm > 1$ and has at least q zeros. $\square$

A lower bound on the number of monomials can be obtained as well.

Now we consider polynomial approximations of powers x^d in finite fields.

Theorem 7.2. *Let d be an integer with $0 \leq d \leq q-1$ and let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree n such that $f(X) \neq a_n X^n$. Assume that*

$$f(x) = x^d, \qquad x \in S,$$

for a set $S \subseteq \mathbb{F}_q$. Then

$$n \geq \frac{(|S|-1)^2}{2(q-1)}$$

Proof. Let $T \geq |S|-1$ denote the number of solutions of the equation $f(x) = x^d$, $x \in \mathbb{F}_q^*$. It is enough to show that $T \leq (2n(q-1))^{1/2}$.

Obviously, T^2 is the number of solutions of the system of equations

$$f(x) = x^d, \quad f(y) = y^d, \qquad x, y \in \mathbb{F}_q^*$$

which after the substitution $y = xz$ reduces to the equivalent system

$$f(x) = x^d, \quad f(xz) = (xz)^d, \qquad x, z \in \mathbb{F}_q^*.$$

From here we derive $f(xz) = z^d f(x)$. For those values of z for which the polynomial $F_z(X) = f(Xz) - z^d f(X)$ is not identical to zero there are at most n corresponding values of x; for others z there are at most $q-1$ corresponding values of x. Thus, $T^2 \leq (q-1)n + (q-1)Q$ where Q is the number of $z \in \mathbb{F}_q^*$ such that $F_z(X)$ is identical to zero. Taking into account that $f(X)$ contains at least two non-zero monomials, say $a_n X^n$ and $a_m X^m$, $a_n a_m \neq 0$, $O \leq m < n$, we find then this is possible only if $z^m = z^d$ and $z^n = z^d$. In particular, $z^m = z^n$ therefore $Q \leq n$ and the result follows. $\square$

The polynomial $f(X) = X$ shows that the condition $f(X) \neq a_n X^n$ is necessary. Indeed, we have $x = x^{(q+1)/2}$ for any quadratic residue x.

Applications to constructing symmetric Boolean functions which cannot be approximated by polynomials of small degree, are possible too, see the paper [1], for example, which demonstrates how to use such functions for obtaining non-trivial lower bounds of the computational complexity theory.

First of all we fix a normal basis

$$\omega, \omega^2, \ldots, \omega^{2^{r-1}}$$

of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ (see [16, 24]) and identify the Boolean cube $\{0,1\}^r$ and $\mathbb{F}_{2^r}$ as follows

$$(x_1, \ldots, x_r) \in \{0,1\}^r \leftrightarrow x = x_1\omega + \ldots + x_r\omega^{2^{r-1}} \in \mathbb{F}_{2^r}$$

Taking into account the identity

$$\begin{aligned} x^2 &= \left(x_1\omega + \ldots + x_r\omega^{2^{r-1}}\right)^2 = x_1\omega^2 + \ldots + x_r\omega^{2^r} \\ &= x_r\omega + x_1\omega^2 + \ldots + x_{r-1}\omega^{2^{r-1}} \end{aligned}$$

we see that any symmetric Boolean function $B(x_1, \ldots, x_r)$ satisfies the functional equation $B(x) = B(x^2)$ over $\mathbb{F}_{2^r}$. Thus if a polynomial $f(X) \in \mathbb{F}_{2^r}[X]$ coincides with $B(x)$ for at least $q - s$ values of $x \in \mathbb{F}_q$ then $f(x) = f(x^2)$ for at least $q - 2s$ points, thus $2 \deg f \geq q - 2s$ and $\deg f \geq q/2 - s$.

8 Some Remarks, Generalizations and Open Questions

In this paper we considered the discrete logarithm over prime fields only. This is because there is the obvious bijective mapping between the residue ring $\mathbb{Z}/(p-1)$ and the multiplicative group $\mathbb{F}_p^*$. For $\mathbb{Z}/(q-1)$ and $\mathbb{F}_q^*$ where $q = p^r$ is a prime power such a map also exists [21] (via p-adic expansions and representation of elements of $\mathbb{F}_q$ with respect to some fixed basis). Another way is to consider representations of the discrete logarithm via multivariate functions (on coordinates of its argument). In both cases many details become quite messy. Nevertheless, apparently many of the results of this paper can be extended onto arbitrary finite fields $\mathbb{F}_q$.

One can see that Theorems 3.1, 3.2, 6.1 and 6.2 can easily be extended to rational functions (with somewhere stronger bounds than those following from more general Theorems 3.5, 3.6, 6.3 and 6.4).

We mention that using some standard tricks [2] one can replace $p^{1/2} \log p$ by $p^{1/2}$ in Theorems 3.3, 3.4, 4.1 and 5.1 (with slightly worse constants). Moreover, using the improvements of the Weil bound from [14, 19] (concerning the case of quadratic characters only) one can show that the linear complexity of the discrete logarithm modulo 2 is at least $2p^{1/2} + O(1)$. Certainly, other bounds of complete and incomplete character sums with polynomials can be useful as well. For instance, some new (but fairly weak) results can be extracted from [26].

Also, instead of Lemma 2.4 one could use a more general estimate of [23] of character sums with algebraic functions (including rational functions of course). That would allow to generalize Theorems 3.3 and 3.4 to the case of approximation by algebraic and rational functions.

As we have mentioned, one can obtain the upper bound $\deg f \le |S| - 1$ on the smallest possible degrees of polynomials involved in Theorems 3.1, 3.2, 3.4, 6.1 and 6.2.

Open Question 8.1. *Find examples of sets S for which the aforementioned trivial bound can be improved.*

A similar question can be asked about algebraic functions as well.

There is also one more interesting type of sets which probably can be dealt with by the method of this work, we mean random sets.

Open Question 8.2. *Obtain improved probabilistic versions of lower bounds of Theorems 3.2, 3.6, 6.2 and 6.4 for random sets S.*

Unfortunately a modulo $p-$ analogue of the explicit representation (1.1) is not known. Theorem 4.1 provides the bound $\Omega(p^{1/2}\log^{-1} p)$ on the degree of such a polynomial (in fact the logarithmic term can be omitted) while one should expect it to be of order p.

Open Question 8.3. *Obtain an explicit expression for a polynomial $f(X) \in \mathbb{Z}[X]$ of the such degree with*

$$\operatorname{ind} x \equiv f(x) \pmod{p-1}, \qquad x = 1, \ldots, p-1.$$

In this paper we have been dealing with representations of the discrete logarithm modulo p and modulo a divisor d of $p-1$. Representations of the discrete logarithm (modulo p) in the residue rind modulo another integer $M \ne p$ are of interest as well.

Open Question 8.4. *Obtain analogues of the results above for congruences of the form*

$$\operatorname{ind} x \equiv f(x) \pmod{M}, \qquad x \in S,$$

with an arbitrary integer M, some "simple" functions $f(X)$ and various sets $S \subseteq \{1, \ldots, p-1\}$.

If $M \geq p-1$ then the value of $\operatorname{ind} x$ can be recovered unambiguously. If $M < p-1$ then the complete recovering is not possible but it still can provide some useful information about $\operatorname{ind} x$ (that is what we actually want to avoid). For example, if $M = 2^k$ then such a representation gives us k rightmost bits of $\operatorname{ind} x$. The case $k = 1$ is covered by Theorem 4.1 and its improvement for $k > 1$ would be very interesting.

The case when M is prime can possibly be handled along the same lines as we use in this paper but if M is composite some additional considerations are required. Indeed, although analogues of our auxiliary results (bounds for the number of zeros [12, 13], bounds of character sum [10, 25] , etc.) are known modulo an arbitrary composite M as well, they are essentially weaker and, respectively, lead to much weaker statements. Nevertheless apparently this question can be approached at least for some interesting values of M like $M = 2^k$.

Along with Boolean functions covered by Theorem 5.1 one can also consider the Boolean function

$$B(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } \operatorname{ind} x \leq (p-3)/2, \\ 1, & \text{if } \operatorname{ind} x \geq (p-1)/2, \end{cases} \tag{8.1}$$

where $x = u_1 \ldots u_r$ is the bit representation of x , $r = \lceil \log p \rceil$. This function has to do with first bits of $\operatorname{ind} x$. The method of the proof of Theorem 5.1 can be applied to this function but produces a rather weak result (the lower bound $\Omega(\log p)$ for the number of terms and no non-trivial bound on the degree).

Open Question 8.5. *Obtain non-trivial lower bound on the degree of the Boolean function (8.1).*

Approximations by polynomials over reals are of interest as well.

Open Question 8.6. *Obtain analogues of the results above for polynomials $f(X) \in \mathbb{R}[X]$ over reals satisfying the inequality of the form*

$$|\operatorname{ind} x - f(x)| < 1/2, \qquad x \in S,$$

for various sets $S \subseteq \{1, \ldots, p-1\}$.

One can also consider threshold function representations of separate bits of the discrete logarithm.

Open Question 8.7. *Does there exist a threshold representation of the last bit of the discrete logarithm, in other words do they exist real $w_0, w_1, \dots w_r$ such that $w_1 u_1 + \dots w_r u_r > w_0$, where $x = u_1 \dots u_r$ is the bit representation of x, if and only if $x = 1, \dots, p-1$ is a quadratic residue modulo p.*

The author believes that the answer on that question is negative but probably is hard to obtain. Thus, one can assume that such a representation exists (with integer weights $w_0, w_1, \dots w_r$ without loss of generality) and try to obtain lower bounds on $w_0, w_1, \dots w_r$.

Theorem 5.2 provides a lower bound $\Omega(\log \log p)$ on the depth of a straight-line deterministic Boolean circuit solving the discrete logarithm problem modulo p.

Open Question 8.8. *Obtain analogues of Theorem 5.2 for branching and randomised Boolean circuits.*

Note that in [27], probabilistic Boolean circuits of depth $(\log \log p)^{O(1)}$ and subexponential size are constructed.

It can also be relevant to mention the paper [18] which demonstrates that under certain conditions, breaking the Diffie-Hellman cryptosystem is polynomial time equivalent (in the Boolean model of computation) to computing the discrete logarithm.

Here we have considered representations and approximations via polynomials and algebraic functions of a given degree n or containing a given number t of monomials and show that for n or t small enough such representations and approximations are impossible. The motivating idea was to show that the discrete logarithm cannot be represented or even approximated by such easily computable functions. On the other hand, there is one more very interesting class of functions which are also easy to compute thus extensions of our "impossibility" results on these functions would be very important. We mean functions of low additive complexity. Those are functions which can be represented using a given number of the $\pm$-symbols (and any number of multiplications). We do not give a precise definition of additive complexity but just mention that a polynomial is of additive complexity t if there is it can be written down with at most t signs $\pm$. Say, the polynomials $f(X) = (X+1)^k - (X+2)^m$ and $F(X,Y) = (Y+1)^k(X-1)^m + (Y-1)^m(X+1)^k$ are of additive complexity 3 and 5 respectively but neither of low degree nor sparse (for k and m large enough). It is easy to see that using repeated squaring their values can be computed very quickly at any point.

To fulfil this program one needs to answer the following question.

Open Question 8.9. *Obtain a non-trivial upper bound for the number of zeros of polynomials of additive complexity t over $\mathbb{F}_q$.*

As the very first step to such a general bound one can try to estimate the number of zeros of functions of the shape

$$f(X) = \sum_{i=1}^{t} a_i(X+b_i)^{n_i} \in \mathbb{F}_q[X].$$

We note that over fields of zero characteristic such bounds are known [11], [15] and have already produced a large number of results on computational complexity of various classes of functions [4]. Over finite field the situation is more complicated, for example the polynomial $x^{(p-1)/2} - 1$ has $(p-1)/2$ zeros thus some extra conditions should be imposed.

Acknowledgment. This paper was essentially written during a visit by the author to the University of Paderborn, whose hospitality and providing excellent working conditions are gratefully acknowledged. Special thanks go to Joachim von zur Gathen and to the members of his research group for creating very stimulating atmosphere and numerous fruitful discussions. In particular, the idea to consider the critical complexity $c(B)$ of Boolean functions of Theorem 5.3 belongs to Joachim von zur Gathen.

Also, the author would like to thank Dima Grigoriev and Helmut Meyn for several valuable advises.

During his sabbatical in February – July of 1996 the author gave a series of talks on the subject of this paper in several European Universities and Research Centers including the University of Erlangen (Germany), University of

Frankfurt am Main (Germany), Technical University of Munchen (Germany), University of Paderborn (Germany), University of Saarbrucken (Germany), INRIA (France), ETH (Switzerland), CWI (The Netherlands), KTH (Sweden). Critical remarks and advises obtained during those talks were of great help. For example, the current version of Theorem 6.2 was communicated to the author by Don Coppersmith after one of such talks (at CWI). The proof of Theorem 6.4 uses the same idea as well. Accordingly, Open Questions 8.1 and 8.2 were motivated by a discussion with Johan Håstad (at KTH).

References

[1] D.A.M. Barrington and H. Straubing, 'Lower bounds for modular counting by circuit with modular gates', *Lect. Notes in Comp. Sci.*, **911** (1995), 60–71.

[2] J. H. H. Chalk, 'Polynomials congruences over incomplete residue systems modulo k', *Proc. Kon. Ned. Acad. Wetensch.*, **A92** (1989), 49–62.

[3] W. Diffie and M. Hellman, 'New directions in cryptography', *IEEE Trans. Inform. Theory*, **22** (1976), 644–654.

[4] D. Grigoriev, 'Lower bounds in the algebraic computational complexity', *Zapiski Nauchn. Semin. Leningr. Otdel. Matem. Inst. Acad. Sci. USSR*, **118** (1982), 25–82 (in Russian).

[5] J. von zur Gathen, 'Computing powers in parallel', *SIAM J. Comp.*, **16** (1987), 930–945.

[6] J. von zur Gathen, 'Algebraic complexity theory', *Annual Review of Comp. Sci.*, **3** (1988), 317–347.

[7] J. von zur Gathen and G. Seroussi, 'Boolean circuits versus arithmetic circuits', *Inform. and Comp.*, **91** (1991), 142–154.

[8] J. von zur Gathen and I. E. Shparlinski 'Finding points on curves over finite fields', *Proc. 36 IEEE Symposium on Foundations of Computer Science*, 1995, 284-292.

[9] L.-K. Hua, *Abschatzungen von exponentialsummen und ihre anwendung in der zahlentheorie*, Teubner-Verlag, Leipzig, 1959.

[10] D. Ismailov, 'Estimates of complete character sums of polynomials', *Proc. Steklov Math. Inst.*, Moscow, **200** (1992), 171–184 (in Russian).

[11] A. G. Khovanski, *Fewnomials*, Amer. Math. Soc., Providence, 1991.

[12] S. V. Konyagin, 'On the number of solutions of an univariate congruence of n-th degree', *Matem. Sbornik*, **102** (1979), 171–187 (in Russian).

[13] S. V. Konyagin and T. Steger, 'On the number of solutions of polynomial congruences ', *Matem. Zametki*, **55** (1994), no.1, 73–79 (in Russian).

[14] N. M. Korobov, 'An estimate of the sum of the Legendre symbols', *Doklady Acad. Sci. USSR*, **196** (1971), 764–767 (in Russian).

[15] L. Lipshits, 'P-adic zeros of polynomials', *J. Reine Angew. Math.*, **390** (1988), 208–214.

[16] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, MA, 1983.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Comp., 1977.

[18] U. M. Maurer and S. Wolf, 'On the complexity of breaking the Diffie–Hellman protocol', *Preprint* , 1996, 1–30.

[19] D. A. Mit'kin, 'An estimate of the sum of the Legendre symbols on polynomials of an even degree', *Matem. Zametki*, **14** (1973), 73–81 (in Russian).

[20] G. L. Mullen, 'Permutation polynomials over finite fields', *Finite Fields: Coding Theory and Advances in Communications and Computing*, Marcel Dekker, NY, 1993, 131–151.

[21] G. L. Mullen and R. M. White, 'A polynomial representation for logarithms in $GF(q)$', *Acta Arithm.*, **47** (1986), 255–261.

[22] H. Niederreiter, 'The linear complexity profile and the jump complexity profile of keystream sequences', *Lect. Notes in Comp. Sci.*, **473** (1991), 174–188.

[23] G. I. Perel'muter, 'A bound of the sum along a curve', *Matem. Zametki*, **5** (1969), 373–380 (in Russian)

[24] I. E. Shparlinski, *Computational and algorithmic problems in finite fields*, Kluwer Acad. Publ., Dordrecht, The Netherlands, 1992.

[25] I. E. Shparlinski and S. A. Stepanov, 'Estimates of an incomplete sum of multiplicative characters of polynomials', *Diskretnaja Matem.*, **2** (1990), no.3, 115-119 (in Russian).

[26] N. M. Stephens, 'Dirichlet characters and polynomials', *Bull. Lond. Math. Soc.*, **11** (1979), 52–54.

[27] J. Sorenson, 'Polylog depth circuits for integer factoring and discrete logarithms', *Inform. and Comp.*, **110** (1994), 1–18.

[28] I. Wegener, *The complexity of Boolean functions*, Wiley Intersci. Publ., 1987.

[29] A. Weil, *Basic number theory*, Springer-Verlag, NY, 1974.