RC 20724 (91825) 2/7/97
Computer Science/Mathematics 103 pages

Research Report

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

Don Coppersmith
IBM Research Division
T.J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Igor Shparlinski
School of MPCE
Macquarie University
NSW 2109, Australia

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

Don Coppersmith

IBM T. J. Watson Research Center
Yorktown Heights, NY 10598, USA
copper@watson.ibm.com

and

Igor Shparlinski

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

February 3, 1997

Contents

Acknowledgment iii

Preface v

I Preliminaries 1

1 Introduction 3

2 Auxiliary Results 11

II Approximation and Complexity of the Discrete Logarithm 21

3 Approximation of the Discrete Logarithm Modulo p 23

4 Approximation of the Discrete Logarithm Modulo $p-1$ 35

5 Approximation of the Discrete Logarithm by Boolean Functions 41

6 Approximation of the Discrete Logarithm by Real Polynomials 49

III Complexity of Breaking the Diffie–Hellman Cryptosystem and Other Applications 53

7 The Diffie–Hellman Cryptosystem 55

8 Trade-off Between the Boolean and Arithmetic Depths of Modulo p Functions 75

9 Permutation Polynomials, Powers, Zech's Logarithm, Primitive Root Testing and Symmetric Boolean Functions 85

10 Some Remarks, Generalizations and Open Questions 91

Bibliography 99

Acknowledgment

This work was essentially written during a visit by the second 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 a very stimulating atmosphere and numerous fruitful discussions. In particular, the idea to consider the sensitivity $\sigma(B)$ of Boolean functions of Theorem 5.3 belongs to Joachim von zur Gathen.

We would like to thank Dima Grigoriev and Helmut Meyn for several valuable pieces of advice. Theorems 3.3 and 7.3 and as well as Open Question 10.1 were motivated by a discussion with Johan Håstad (at KTH, Sweden).

Preface

Several exponential (in terms of $\log p$) lower bounds are obtained on the degrees and orders of

- polynomials;
- algebraic functions;
- Boolean functions;
- linear recurring sequences

coinciding with values of the discrete logarithm modulo a prime p at sufficiently many points (the number of points can be as little as $p^{1/2+\epsilon}$). These functions are considered over the residue ring modulo p and over the residue ring modulo an arbitrary divisor d of $p-1$. The case of $d=2$ is of special interest since it corresponds to the representation of the rightmost bit of the discrete logarithm and defines whether the argument is a quadratic residue. These results are used to obtain lower bounds on the parallel complexity of computing the discrete logarithm.

The method is based on bounds of character sums and numbers of solutions of some polynomial equations.

Similar results are obtained for breaking the Diffie–Hellman cryptosystem. Several other applications of the method are indicated as well.

Part I

Preliminaries

Chapter 1

Introduction

In the first part of this work 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 'easily 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 [12, 37]. So, the principal motivation of this work 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 $\{1, \ldots, p-1\}$ essentially, onto the set $\{0, 1, \ldots, p-2\}$. 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

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

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 work.

It has been shown in [30] 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, it 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 $x = 1, \ldots, p-1$ 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;

- approximation on random 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 (to which the argument of $\operatorname{ind} x$ belongs);
- 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);
- over fields of real and complex numbers (if we consider the argument x and the value $\operatorname{ind} x$ as real numbers).

In particular, our results provide a non-trivial lower bound of the form $\Omega(p^{1/2}\log^{-1} p)$ for the linear complexity [32] of the discrete logarithm modulo any divisor $d > 1$ of $p-1$. The question on the non-linear complexity is dealt with as well.

In fact for a small divisor d of $p-1$, the residue of $\operatorname{ind} x$ modulo d can be found in $d^{1/2}\log^{O(1)} p$ Boolean operations. Thus the sequential complexity of this question is known to be polynomial. The results of this work provide some insight on its parallel complexity.

The case $d = 2$ corresponds to the studying the rightmost bit of $\operatorname{ind} x$. This bit is of special interest of course since its parity determines

whether 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 rightmost bit of $\operatorname{ind} x$. We apply it to obtain the lower bound $\Omega(\log\log p)$ on the depth of Boolean circuits deciding whether x is quadratic residue or not. This automatically implies the same lower bound on the parallel complexity of computing the discrete logarithm as well as on the complexity of irreducibility testing of polynomials over $\mathbb{F}_p$.

Our result supplements some of the results of [9, 11] 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 rightmost 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, that is, the complexity on a parallel random access machine with unlimited number of all-powerful processors. More precisely, we consider the modification which is known as CREW (concurrent read, exclusive write) PRAM. Such a machine has an infinite shared memory and each cell of which an hold an integer number and such that simultaneous reads of a single cell by several processors are permitted, but simultaneous writes are not [33, 45].

We remark that several results about complexity of bits of the discrete logarithm have been already obtained but all of them are based on some unproven assumptions. Also they mainly concern the discrete logarithm modulo a product of two primes rather than the classical discrete logarithm modulo a prime. A good outline of such results can be found in [16].

Then, we show that the same considerations are applicable to some questions related to the Diffie–Hellman cryptosystem [6] 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 randomized 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 whether 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.

Nevertheless, using a new and very general approach developed in Chapter 8 to estimate the complexity of functions over $\mathbb{F}_p$, we obtain the lower bound $(0.25 + o(1))\log\log p$ on the CREW PRAM complexity of breaking the Diffie–Hellman cryptosystem modulo a prime p. This lower bound (as well as several others) is doubly 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.

Several lower bounds are also known on the complexity of deterministic [31] and probabilistic [36] sequential algorithms to compute discrete logarithms. However the results and approach of those papers are quite different from those of the present work.

It could also be relevant to mention the papers [3, 4] where complexity of finding of some small portion bits of the Diffie–Hellman transformation (over a prime field $\mathbb{F}_p$) is considered and is shown to be expected polynomial time equivalent to the whole problem of breaking the Diffie–Hellman cryptosystem.

In the papers [2, 27] it is demonstrated that under certain conditions,

breaking the Diffie–Hellman cryptosystem is polynomial time equivalent (in the Boolean model of computation) to computing the discrete logarithm.

Several more interesting result about parallel complexity of computing discrete logarithms modulo p, can be found in [42]. It should be mentioned that in that paper more general Boolean circuits are used (with unlimited fan-in), thus the obtained there upper bounds cannot unfortunately be compared with our lower bounds.

We apply our method to derive quite a general estimate showing that for any non-linear and non-constant function modulo sufficiently large prime p its arithmetic and Boolean depths cannot be smaller than $0.124 \log\log p$ simultaneously. Although many results showing that if one of those depths is small then the other one is not too large are readily available [11], estimates of the type which we obtain here seem to be unknown before.

These results provide the background for the aforementioned lower bound on the complexity of breaking the Diffie–Hellman cryptosystem modulo p.

Finally we show that several other related questions about permutation polynomials, powers, Zech's logarithm, primitive root testing and some special 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.

Estimates of exponential sums are also used in [13] in a similar way.

We also use some standard facts and notions of the theory of finite fields which one can easily find in [25].

In obtaining the lower bounds on the depth of circuits in Theorem 5.2 our arguments are quite close to those of [9, 10, 11] (see also given there references to other works). However, it seems that in the proof

of Theorem 7.7 some new arguments appear. We also use several other notions and results of the complexity theory [33, 45].

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

We also use the notation

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

and use $\log z$ to denote the logarithm in base 2.

Chapter 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

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

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

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

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 $n+1$

$$f(x+n+1) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n+1}{k} f(x+k) \quad (2.3)$$

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 $x = 1, \ldots, H$ with $u(x) \neq 0$.*

Proof. It is obvious that if n consecutive values

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

then all further values $u(x+n), u(x+n+1), \ldots$ are zeros as well.

Moreover, using the fact that $c_0 \neq 0$ one easily derives that all previous values $u(x-1), u(x-2), \ldots$ 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. □

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

The next four statements are slightly more general forms 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 [46] and the standard method of estimating of incomplete sums via complete ones [5, 17, 44].

The method is based on the identity (see Exercise 11.b to Chapter 3 of [44])

$$\sum_{c=0}^{M-1} \mathbf{e}(2\pi icu/M) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod{M}; \\ M, & \text{if } u \equiv 0 \pmod{M}. \end{cases} \tag{2.4}$$

and the inequality (see Exercise 11.c to Chapter 3 of [44])

$$\sum_{c=0}^{M-1} \left| \sum_{y=H+1}^{H+N} \mathbf{e}(2\pi icy/M) \right| \le M(\ln M + 1) \tag{2.5}$$

which hold for any integers $M > 1$ and u.

We present a proof only the last Lemma; the other three can be obtained similarly (and apparently can be found in the literature as well).

Lemma 2.3. *For any non-trivial multiplicative 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 linear forms $a_ix + b_i$ with $a_i, b_i \not\equiv 0$ and $b_i/a_i \not\equiv b_j/a_j \pmod{p}$, $i, j = 1 \ldots, n$, $i \ne j$.

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 $H \le p$.

Lemma 2.5. *For any polynomials $f(X), g(X) \in \mathbb{Z}[X]$ with*

$$\deg f + \deg g = n$$

and such that the rational function $h(X) = f(X)/g(X)$ is neither a constant nor a linear function modulo p, the bound

$$\left| \sum_{\substack{x=N+1 \\ g(x) \not\equiv 0 \pmod p}}^{N+H} \mathbf{e}\left(\frac{h(x)}{p}\right) \right| \le np^{1/2} \log p$$

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

Lemma 2.6. *For any non-trivial multiplicative character χ of $\mathbb{F}_q$ 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*

$$\left| \sum_{x=N+1}^{N+H} \chi\left(\prod_{i=0}^{n} (a_i g^x + b_i)^{c_i}\right) \right| \le (n+1) q^{1/2} \log q$$

holds for any integers N and $H \le q-1$ and any linear forms $a_i x + b_i$ with $a_i, b_i \ne 0$ and $b_i/a_i \ne b_j/a_j \pmod p$, $i, j = 0 \ldots, n$, $i \ne j$.

Proof. From (2.4) we obtain

$$\begin{aligned}
&\sum_{x=N+1}^{N+H} \chi\left(\prod_{i=0}^{n} (a_i g^x + b_i)^{c_i}\right) \\
&\quad = \frac{1}{q-1} \sum_{x=0}^{q-2} \chi\left(\prod_{i=0}^{n} (a_i g^x + b_i)^{c_i}\right) \sum_{c=0}^{q-2} \sum_{y=N+1}^{N+H} \psi(c(x-y) \\
&\quad = \frac{1}{q-1} \sum_{c=0}^{q-2} \sum_{x=0}^{q-2} \chi\left(\prod_{i=0}^{n} (a_i g^x + b_i)^{c_i}\right) \psi(x)^c \sum_{y=N+1}^{N+H} \psi(-cy),
\end{aligned}$$

where

$$\psi(x) = \mathbf{e}\left(2\pi i \frac{x}{q-1}\right)$$

is a primitive multiplicative character of $\mathbb{F}_q$. Therefore χ is some power of ψ,

$$\chi(u) = \psi(u)^e,$$

where the exponent e satisfies

$$1 \le e \le q-2, \qquad \gcd(e, q-1) = (q-1)/d.$$

Applying the Weil bound in the form of Theorem 5.41 of [25] we obtain

$$\begin{aligned}\left|\sum_{x=0}^{q-2}\chi\left(\prod_{i=0}^{n}(a_ig^x+b_i)^{c_i}\right)\psi(g^{cx})\right| &= \left|\sum_{x=0}^{q-2}\psi\left(g^{xc}\prod_{i=0}^{n}(a_ig^x+b_i)^{ec_i}\right)\right| \\ &= \left|\sum_{x\in\mathbb{F}_q}\psi\left(x^c\prod_{i=0}^{n}(a_ix+b_i)^{ec_i}\right)\right| \\ &\le (n+1)q^{1/2}\end{aligned}$$

(one easily verifies that the condition of that theorem is satisfied). Taking into account that

$$\ln(q-1)+1 \le \log q$$

for $q \ge 2$, from (2.5) we derive the desired bound. □

For a sequence of H points

$$\Gamma = (\gamma_{0,x},\dots\gamma_{N-1,x})_{x=1}^{H}$$

of the N-dimensional unit cube denote by Δ_Γ its discrepancy. That is

$$\Delta_\Gamma = \sup_{B\in[0,1]^N}\left|\frac{T_\Gamma(B)}{H}-|B|\right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\beta_0,\alpha_0]\times\dots\times[\beta_{N-1},\alpha_{N-1}] \subseteq [0,1]^N.$$

and the supremum is taken over all such boxes.

For an integer vector $\mathbf{a} = (a_0,\dots,a_{N-1}) \in \mathbb{Z}^N$ we denote

$$\|\mathbf{a}\| = \max_{i=0,\dots,N-1}|a_i|, \qquad r(\mathbf{a}) = \prod_{i=0}^{N-1}\max\{|a_i|,1\}^{-1}.$$

We need the Koksma-Szüsz inequality which we present in the following form [20, 43].

Lemma 2.7. *There exist an absolute constant $C > 0$ such that for any integer $L > 1$ the bound*

$$\Delta_\Gamma < C^N \left(\frac{1}{L} + \frac{1}{H} \sum_{0<\|\mathbf{a}\|\le L} \frac{1}{r(\mathbf{a})} \left| \sum_{x=1}^{H} \mathbf{e}\left(2\pi i \sum_{j=0}^{N-1} a_j \gamma_{j,x} \right) \right| \right),$$

where the sum is taken over all integer vectors

$$\mathbf{a} = (a_0, \ldots, a_{N-1}) \in \mathbb{Z}^N$$

with $\|\mathbf{a}\| \le L$, holds.

We remark that the sequence Γ hits any box

$$B = [\beta_0, \alpha_0] \times \ldots \times [\beta_{N-1}, \alpha_{N-1}] \subseteq [0,1]^N$$

of size $|B| > \Delta_\Gamma$.

To apply this lemma we will also need the following statement.

Lemma 2.8. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial whose degree satisfies $p > \deg f \ge 3$, and whose leading coefficient does not vanish modulo p. Suppose that integers s and m satisfy the inequality*

$$s(m+1) < \log p.$$

Let $L = 2^s - 1$ and $e_0 = 0$, $e_i = 2^{si}$, $i = 1, \ldots, m$. Then for any vector $\mathbf{a} \in \mathbb{Z}^{m+1}$, with $0 < \|\mathbf{a}\| \le L$ the linear combination

$$F(X) = \sum_{i=0}^{m} a_i f(X + e_i)$$

is neither a constant nor a linear function modulo p.

Proof. Without loss of generality we may assume that $a_m \ne 0$. Let $n = \deg f$ and $f(X) = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_0$. Then the leading coefficient of F equals

$$C_n = c_n \sum_{i=0}^{m} a_i,$$

and the second leading coefficient of $F(X)$ equals

$$C_{n-1} = nc_n \sum_{i=0}^{m} a_i e_i + c_{n-1} \sum_{i=0}^{m} a_i.$$

By the condition of the theorem we have $c_n \not\equiv 0 \pmod{p}$. Hence if $C_n = 0$ then

$$\sum_{i=0}^{m} a_i = 0 \pmod{p}$$

and

$$C_{n-1} \equiv nc_n \sum_{i=0}^{m} a_i e_i \pmod{p}.$$

One easily verifies that

$$\left| \sum_{i=0}^{m} a_i e_i \right| \le L \sum_{i=1}^{m} e_i < p,$$

and that

$$\left| \sum_{i=0}^{m} a_i e_i \right| \ge e_m - L \sum_{i=1}^{m-1} e_i > 0.$$

Therefore $A_{n-1} \not\equiv 0 \pmod{p}$, thus F is of degree at least $n - 1 \ge 2$ modulo p. □

Finally we need a similar result for rational functions.

Lemma 2.9. *Let $f(X), g(X) \in \mathbb{Z}[X]$ be polynomials such that the rational function $h(X) = f(X)/g(X)$ is not a polynomial modulo p. Then for any integer $k < \log p$ there exist at least*

$$M \ge k - \frac{\deg g(\deg g - 1)}{2}$$

integers

$$0 \le s_i \le k, \qquad i = 1, \ldots, M,$$

such that any non-trivial modulo p linear combination

$$H(X) = \sum_{i=0}^{M} a_i h\left(X + e_i\right),$$

where $e_0 = 0$, $e_i = 2^{s_i}$, $i = 1, \ldots, M$, is neither a constant nor a linear function modulo p.

Proof. From the condition of the theorem we conclude that $g(X)$ is not constant modulo p. Obviously it is enough to show that there exist at least M integers $0 \le s_1 \le \ldots \le s_M \le k$ such that the polynomials $g(x+e_i)$, $i = 0, \ldots, M$ are pairwise relatively prime in the residue ring modulo p.

Let $\lambda_1, \ldots, \lambda_N$ be the $N \le \deg g$ distinct roots of g in the algebraic closure of $\mathbb{Q}$.

Let D be the set of integers δ, $0 \le \delta \le p-1$, such that

$$\lambda_l - \lambda_r \equiv \delta \pmod{p}.$$

for some pair (l, r), with $1 \le l < r \le N$.

We define the 2-adic order $\operatorname{ord}_2 \delta$ of integer δ as the largest power of 2 which divides δ, i.e., $\operatorname{ord}_2 = \nu$ if and only if

$$\mu \equiv 0 \pmod{2^\nu}, \qquad \mu \not\equiv 0 \pmod{2^{\nu+1}}$$

and put

$$T = \{\operatorname{ord}_2 \delta \ : \ \delta \in D\}$$

We define the sequence $s_1, \ldots, s_M$ by the relation

$$\{s_1, \ldots, s_M\} = \{1, \ldots, k\} \setminus T$$

It is obvious that if

$$\lambda_l - \lambda_r \equiv 2^{s_i} - 2^{s_j} \pmod{p}$$

or

$$\lambda_l - \lambda_r \equiv 2^{s_i} \pmod{p}$$

for some pair (l, r), with $1 \le l < r \le N$, and some pair (i, j) with $0 \le i, j \le M$, $i \ne j$, then

$$\delta \equiv 2^{s_i} - 2^{s_j} \pmod{p}$$

or

$$\delta \equiv 2^{s_i} \pmod{p}$$

for some $\delta \in D$. Because $k < \log p$ these congruences imply that

$$\delta = 2^{s_i} - 2^{s_j}$$

or

$$\mu = 2^{s_i}$$

which is impossible because of the choice of the sequence $s_1, \ldots, s_M$.

Thus the corresponding polynomials $g(x + e_i)$, $i = 0, \ldots, M$, are pairwise relatively prime in the residue ring modulo p. It is easy to see that $M \geq k - |T| \geq k - N(N-1)/2$. □

Following [45], for a Boolean function $B(U_1, \ldots, U_r)$ we define the *critical complexity* which is also known as *sensitivity* $\sigma(B)$ as the largest integer $s \leq r$ such that there is a binary vector $x = (x_1, \ldots, x_r)$ for which $B(x) \neq B(x^{(i)})$ for s values of i, $1 \leq i \leq r$, where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate. In other words, $\sigma(B)$ is the maximum, over all binary vectors $x = (x_1, \ldots, x_r)$, of the number of points y on the unit Hamming sphere around x with $B(y) \neq B(x)$.

This function gives a lower bound for several other complexity characteristics of B, see [33] or Chapter 13 of [45]. In particular, the relation between the sensitivity and the CREW PRAM complexity of a Boolean function is given by the following inequality which is essentially Theorem 4.7 of [33].

Lemma 2.10. *For the CREW PRAM complexity of any Boolean function B the inequality*

$$CREW\ PRAM(B) \geq 0.5 \log \sigma(B) + O(1)$$

holds.

Part II

Approximation and Complexity of the Discrete Logarithm

Chapter 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 large (in terms of $\log p$).

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

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

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

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

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

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

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 $n \ge \deg h \ge |R| - 1$.

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

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 $\deg f \le |S| - 1 = p - 2 - s$.

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 $p \ge 3$ 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

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

Proof. Let us consider the following set

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

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

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 $x \in \{1, \ldots, p - 1\}$ 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 $|R| \ge |S|(|S| - 1)/(p - 2)$.

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. □

Certainly, for any S one can satisfy (3.1) with a unique polynomial f of degree $\deg f \leq |S| - 1$. Now we show that for a randomly selected set S that degree cannot be smaller. In particular, with probability $1 - o(1)$ we have $\deg f = |S| - 1$ for that polynomial.

Theorem 3.3. *Let S be a set of m random elements picked uniformly from $\{1, \dots, p-1\}$. Then the probability $P_k(p, m)$ that there exists a polynomial $f(X) \in \mathbb{Z}[X]$ of degree*

$$\deg f < m - k$$

and such that

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

satisfies the bound

$$P_k(p, m) \leq \left(\frac{2m}{p-1}\right)^{k/2}.$$

Proof. We say that a set T is satisfied by a polynomial $f(X) \in \mathbb{Z}[X]$ if the condition of the theorem is fulfilled for this pair (T, f). Accordingly

we say that a set T is maximally satisfied by a polynomial $f(X) \in \mathbb{Z}[X]$ if it is satisfied by this polynomial but any superset of T is not.

Suppose there are N various sets $S_i \subseteq \{1, \ldots, p-1\}$, $i = 1, \ldots, N$, that are maximally satisfied by polynomials f_i of degree at most $n = m - k - 1$. In particular, polynomials f_i, $i = 1, \ldots, N$ are pairwise distinct.

Therefore, $|S_i \cap S_j| \le n$, $1 \le i < j \le N$, otherwise we would have $f_i = f_j$ being the unique polynomial on the intersection $S_i \cap S_j$. Thus,

$$\sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T| = n+1}} 1 \le \sum_{\substack{T \subseteq \{1, \ldots, p-1\} \\ |T| = n+1}} 1 \le \binom{p-1}{n+1}. \tag{3.2}$$

From Theorem 3.2 we see that $|S_i| \le (2n(p-1))^{1/2}$.

For an $(n+1)$-element set $T \subseteq \{1, \ldots, p-1\}$, denote by f_T the unique polynomial of degree at most n such that T is satisfied by this polynomial. Also, denote by R_T the set which is maximally satisfied by f_T. Then,

$$\begin{aligned} P_k(p,m) &= \sum_{|T| = n+1} \binom{p-1}{n+1}^{-1} \sum_{\substack{T \subseteq S \subseteq R_T \\ |S| = m}} \binom{p-n-2}{k}^{-1} \\ &\le \binom{p-1}{n+1}^{-1} \binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T| = n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S| = m}} 1 \\ &= \binom{p-1}{n+1}^{-1} \binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{n+1} \binom{|S_i| - n - 1}{k} \end{aligned}$$

We have,

$$\begin{aligned} \binom{p-n-2}{k}^{-1} \binom{|S_i| - n - 1}{k} &\le \left(\frac{|S_i| - n - 1}{p-n-2} \right)^k \\ &\le \left(\frac{|S_i|}{p-1} \right)^k \le \left(\frac{2n}{p-1} \right)^{k/2}. \end{aligned}$$

Substituting this in the the previous inequality and using (3.2) we derive the results. □

Selecting $k = 1$ we obtain that if $m = o(p)$, for almost all sets of size m the smallest degree of the polynomial which they satisfy is of degree $m - 1$.

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 3.4. *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

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

Therefore

$$\left| \sum_{x=N+1}^{N+H} \mathrm{e}\left(\frac{\operatorname{ind} x - f(x)}{p}\right) \right| = \left| \sum_{x=N+1}^{N+H} \mathrm{e}\left(\frac{\delta_x}{p}\right) \right| \geq H - 2\pi\Delta H. \qquad (3.3)$$

We also have

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

thus

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

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 3.5. *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 3.4 but instead of (3.3) we use that

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

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 $H \ge p^{1/2+\epsilon}$ then the degree of f is exponentially large (in terms of $\log p$), $\deg f \ge Cp^{\epsilon}\log^{-1} p$ 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 $n_1 \ge 1, \ldots, n_m \ge 1$ 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

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

In particular, if $|S| \ge \alpha p$ with some $\alpha > 0.5$ then

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

where $C > 0$ is an absolute constant.

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

Theorem 3.6. *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*

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

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 $0 \leq n_i < n_j < p-1$, then $g^{n_i} \not\equiv g^{n_j} \pmod{p}$ for $1 \leq i < j \leq t$. 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

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

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 $(d+1)^2 \geq p$. Hence together with Theorem 3.6 (setting $t = d+1$, $n = d$, $s = 0$) we obtain a very tight bound; namely

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

Theorem 3.6 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 3.7. *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a non-zero modulo $p \geq 3$ polynomial of total 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

$$n \geq |S|(3p)^{-1/2}.$$

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 $\Psi(X,Y)$ be an irreducible factor of $F(X,Y)$, of total degree $d = \deg \Psi$, for which $\Psi(x, \operatorname{ind} x) = 0$ for at least $|S|d/n$ values of $x \in S$. Denote this set of x by T, $|T| \geq |S|d/n$.

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

$$\Psi(x, \operatorname{ind} x) = 0 \quad \text{and} \quad \Psi(ax, \operatorname{ind} ax) = 0. \tag{3.4}$$

We see that

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

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

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

or

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

for $x \in R$. Therefore at least one of the polynomials $\Psi(aX, X + \operatorname{ind} a)$ and $\Psi(aX, X + \operatorname{ind} a + 1)$ 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

$$\Psi(X,Y) = \Psi(aX, Y+b) = 0$$

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

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

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

We may assume that $n \leq |S|/3$ otherwise the bound is trivial. Then

$$|S|d - n \geq 2|S|d/3,$$

so that $d^2 \geq S^2d^2/(3n^2p)$, and the desired inequality follows.

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

$$\Psi(X, Y) = \sum_{i=0}^{d} X^i f_i(Y)$$

then for each $i = 0, \ldots, n$, $f_i(Y)$ divides $f_i(Y + b)$. That implies $f_i(Y) = \mu_i f_i(Y + b)$ for some constant $\mu_i \neq 0$. If $n < p$ (otherwise there is nothing to prove) then this is possible only if $f_i(Y)$ is a constant polynomial and $\mu_i = 1$. Thus $\Psi(X, Y) = \Psi(X)$ is a polynomial in one variable. Therefore, the system (3.4) has at most d solutions. Hence

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

and the desired result follows. □

It is obvious that for any $S \subseteq \{1, \ldots, p-1\}$ there is a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ of degree at most $(2|S|)^{1/2} + 1$ which satisfies the condition of Theorem 3.7. Now we show that for almost all sets S this bound is the best possible.

Theorem 3.8. *Let p be sufficiently large, $0 < \varepsilon < \delta < 1$ and $m \leq p^{1-\delta}$. Let S be a set of m random elements picked uniformly from $\{1, \ldots, p-1\}$. Then the probability $P_{\varepsilon,\delta}(p, m)$ that there exists a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ of degree*

$$\deg F < \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 1$$

and such that

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

satisfies the bound

$$P_{\varepsilon,\delta}(p, m) \le 2^m p^{-(\delta-\varepsilon)m/2}.$$

Proof. We say that a set T is satisfied by a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ if the condition of the theorem is fulfilled for this pair (T, F). Accordingly we say that T is maximally satisfied by a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ if it is satisfied by this polynomial but any superset of T is not.

Suppose there are N various sets $S_i \subseteq \{1, \dots, p-1\}$, $i = 1, \dots, N$, that are maximally satisfied by polynomials $F_i(X, Y) \in \mathbb{Z}[X, Y]$ of degree at most $n = \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 2$. In particular, polynomials F_i, $i = 1, \dots, N$ are pairwise distinct modulo p, thus

$$N \le p^{(n+2)(n+1)/2}.$$

From Theorem 3.7 we derive $|S_i| \le n(3p)^{1/2}$. Therefore

$$\begin{aligned} P_k(p, m) &= \binom{p-1}{m}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{m} \le \sum_{i=1}^{N} \left(\frac{|S_i|}{p-1} \right)^m \\ &\le p^{(n+2)(n+1)/2} \left(\frac{n(3p)^{1/2}}{p-1} \right)^m \le 2^m n^m p^{(n+2)(n+1)/2 - m/2} \\ &\le 2^m m^{m/2} p^{(\varepsilon-1)m/2} \le 2^m p^{-(\delta-\varepsilon)m/2}. \end{aligned}$$

and the result follows. □

Chapter 4

Approximation of the Discrete Logarithm Modulo $p-1$

In this chapter we consider various approximations and representation of the discrete logarithm modulo a divisor d of $p-1$. Certainly the case of $d=2$ is of special interest because it corresponds to representation of the rightmost 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

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

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

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

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

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

for at least $H - (n+1)(s+1)$ 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 a d-th power residue modulo p. Thus, for a non-trivial character χ of $\mathbb{F}_p^*$ of order d, we have

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

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

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

and the result follows. □

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 rightmost bit of $\mathrm{ind}\, x$ 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 [32].

Also, assume that we are given a piecewise representation of the discrete logarithm via linear recurring sequences, thus we are given $m+1$ integers $0 = N_1 < N_2 < \ldots < N_{m+1} = p-1$, 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

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

On the other hand, obviously

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

thus

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

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

Finally we obtain a lower bound on the length of non-linear recurrent relation which the rightmost bit of the discrete logarithm (therefore the discrete logarithm itself) may satisfy. Moreover, we allow the coefficients to be polynomials in x rather than constants.

Theorem 4.2. *Let* $0 \leq N < N + H \leq p - 1$ *and*

$$\operatorname{ind}(x + m_n) \equiv F(x, \operatorname{ind}(x + m_0), \ldots, \operatorname{ind}(x + m_{n-1})) \pmod{2},$$

for all elements $x \in S$ *of a set* $S \subseteq \{N+1, \ldots, N+H\}$ *of cardinality* $|S| = H - s$ *and a polynomial* $F(X_0, X_1, \ldots, X_n) \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ *and* $n+1$ *pairwise distinct modulo* p *integers* $m_0, \ldots, m_n$. *Then*

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

Proof. From the condition of the theorem we see that there does not exist $x \in S$ such that simultaneously

$$x \equiv \mathrm{ind}\,(x+m_0) \equiv \ldots \equiv \mathrm{ind}\,(x+m_{n-1}) \equiv 0 \pmod 2$$

and

$$\mathrm{ind}\,(x+m_n) \not\equiv F_0 \pmod 2,$$

where $F_0 = F(0,\ldots,0)$. Therefore for any even $x \in S$ we have

$$\left(\chi(x+m_n) - (-1)^{F_0}\right) \prod_{i=0}^{n-1} (\chi(x+m_i)+1) = 0,$$

where $\chi(z)$ is the quadratic character modulo p. Therefore

$$\sum_{\substack{x \in S \\ x \equiv 0 \pmod 2}} \left(\chi(x+m_n) - (-1)^{F_0}\right) \prod_{i=0}^{n-1} (\chi(x+m_i)+1) = 0. \qquad (4.2)$$

After simple evaluation one sees that the right hand side contains one 'main' term with absolute value at least $H/2 - s - 1$ and $2^{n+1} - 1$ terms of the form

$$\pm \sum_{\substack{x \in S \\ x \equiv 0 \pmod 2}} \chi\left((x+j_1)\ldots(x+j_k)\right),$$

where $0 \le j_1 < \ldots < j_k \le p-1$, $k \le n+1$. Applying Lemma 2.3 we see that the absolute value of each such term does not exceed

$$\begin{aligned}
&\left| \sum_{\substack{x \in S \\ x \equiv 0 \pmod 2}} \chi\left((x+j_1)\ldots(x+j_k)\right) \right| \\
&\quad \le \left| \sum_{\substack{x=N+1 \\ x \equiv 0 \pmod 2}}^{N+H} \chi\left((x+j_1)\ldots(x+j_k)\right) \right| + s \\
&\quad = \left| \sum_{(N+1)/2 \le x \le (N+H)/2}^{N+H} \chi\left((2x+j_1)\ldots(2x+j_k)\right) \right| + s \\
&\quad \le s + kp^{1/2}\log p.
\end{aligned}$$

Thus from (4.2) we derive

$$\begin{aligned} H/2 - s - 1 &\le \sum_{k=1}^{n+1} \binom{n+1}{k} (s + kp^{1/2} \log p) \\ &\le 2^{n+1} \left(s + (n+1)p^{1/2} \log p\right), \end{aligned}$$

which implies the desired result. □

The case when the polynomial F does not depend on the first coordinate, $s = 0$, and $m_i = i$, $i = 0, \ldots, n$, corresponds to the non-linear complexity of the discrete logarithm (on the interval $x = N+1, \ldots, N+H$). Thus if $H \ge p^{1/2+\epsilon}$ then it is $\Omega(\log p)$.

The result can be extended to any divisor d of $p-1$ without any difficulties.

Chapter 5

Approximation of the Discrete Logarithm by Boolean Functions

Here we consider bitwise approximation of the discrete logarithm given the bit representation of the argument. Moreover, we concentrate on the rightmost bit on $\operatorname{ind} x$. This question is essentially equivalent to deciding quadratic residuosity of x.

In [9] (see also [11]) 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 whether $x \in \mathbb{F}_q^*$ 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 [11] for a discussion of this phenomenon and a survey of relevant results.

Each Boolean function $B(X_1, \ldots, X_r)$ we represent as a multilinear

polynomial of degree n over $\mathbb{F}_2$ of the form

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

We consider Boolean functions producing the rightmost 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 $B(U_1, \ldots, U_r)$ of $r = \lfloor \log p \rfloor$ Boolean variables be such that for any x, $1 \le x \le 2^r - 1$,*

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

where $x = u_1 \ldots u_r$ is the bit representation of x. 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 $m = 1, \ldots, 2^k - 1$ we consider the function

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

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

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

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 $t + 1 \ge 2^{k-1} \ge 2^{-3/2} p^{1/4} \log^{-1/2} p$. □

It easy to see that the same result holds for the monomials of the form $(a_1 U_1 + b_1) \dots (a_n U_n + b_n)$ with $a_i, b_i = 0, 1$, $i = 1, \dots, n$ as well. In other words one can consider not only positive literals but negative ones as well.

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

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

where $H(\gamma) = -\gamma \log \gamma - (1 - \gamma) \log(1 - \gamma)$, which holds for any fixed γ, $0 < \gamma < 1/2$ and $N \to \infty$; see [26], Section 10.11. Then from the inequality

$$t \le \sum_{i=0}^{n} \binom{r}{i} \le (n+1) \binom{r}{n},$$

which holds for $n \le r/2$, one can easily derive that under the condition of Theorem 5.1

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

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

In fact for a half of primes a better estimate can be obtained. Indeed, suppose $p \equiv \pm 3 \pmod 8$. Then 2 is a quadratic non-residue modulo p. Hence the polynomial

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

takes the value of 1 for all non-zero binary $(r-1)$-tuples $(x_1, \ldots, x_{r-1})$, where as before $r = \lfloor \log p \rfloor$. On the other hand, $F(0, \ldots, 0) = 0$. Therefore

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

Thus

$$\deg B \geq \deg F = r - 1 \tag{5.3}$$

and

$$\mathrm{wt}\, B \geq \lceil 0.5 \mathrm{wt}\, F \rceil = \left\lceil (2^{r-1} - 1)/2 \right\rceil = 2^{r-2}.$$

Boolean functions giving the rightmost bit of $\mathrm{ind}\, x$ for all but at most s values of $x = 1, \ldots, 2^r - 1$ can be considered as well. Indeed, one easily sees that the bound of Theorem 5.1 can be modified as

$$t \geq C \min\{p^{1/4} \log^{-1/2} p,\ ps^{-1}\}, \tag{5.4}$$

where C is an absolute constant.

If $p \equiv \pm 3 \pmod 8$ then as in the proof of the bound (5.3) we obtain that the polynomial

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

takes the value 1 for all but at most $2s+1$ binary $(r-1)$ tuples but is not identical to one. Applying the presented in [15] bound of R. Smolensky which claims that if a polynomial

$$F(Y_1, \ldots, Y_m) \in \mathbb{F}_q[Y_1, \ldots, Y_m]$$

of degree n has one zero over $\mathbb{F}_q$ that it has at least q^{m-n} zeros, we obtain

$$\deg B \geq \deg F = r - 1 - \log(2s + 1). \tag{5.5}$$

Now we obtain a lower bound for the parallel complexity of computing the rightmost 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 of the following class $\mathrm{BC}(d)$.

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

Each circuit $C \in \mathrm{BC}(d)$ 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, accepts either some constant or the value of one of 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 two values from some gates of previous levels, ϕ_1, ϕ_2, and then computes and outputs the value of $\phi_1 \# \phi_2$, where $\#$ stands for one of the arithmetic operations over $\mathbb{F}_2$, that is $\# \in \{+, \times\}$.

Finally, 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 $C \in BC(d)$ 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 $C(u_1, \ldots, u_r)$ coincide with values of some Boolean function of degree at most 2^d. Applying (5.2), we obtain the result. □

Now we show that the same method which is used in the proof of Theorem 5.1 can be used in studying the sensitivity of the Boolean functions deciding quadratic residuosity.

Theorem 5.3. *Let a Boolean function $B(U_1, \ldots, U_r)$ of $r = \lfloor \log p \rfloor$ Boolean variables be such that for any x, $1 \le x \le 2^r - 1$,*

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

where $x = u_1 \ldots u_r$ is the bit representation of x. Then

$$\sigma(B) \ge 0.5r + o(r).$$

Proof. We put $m = \left\lfloor r^{1/2} \right\rfloor$, $k = 2m + 1$, $l = \left\lfloor r - r^{1/2} \right\rfloor$, $R = 2^r - k2^l$. One sees that for any fixed i, $0 \le i \le l$, and any $x = 0, \ldots, R-1$, the vector $(B(x + j2^i))_{j=1}^{k}$ is defined. As x ranges, the vector takes on the value of each possible binary k-tuple $T = (t_1, \ldots, t_k)$ with multiplicity

$$N(T) = 2^{-k} \sum_{x=0}^{R-1} \prod_{j=1}^{k} \left(\chi(x + j2^i)(-1)^{t_j} + 1 \right).$$

After simple evaluation one finds that the sum on the left hand side contains one 'main' term $R2^{-k}$ and $2^k - 1$ terms of the form

$$\pm 2^{-k} \sum_{x=0}^{R-1} \chi\left((x + j_1 2^i) \ldots (x + j_s 2^i) \right),$$

where $s \le k$ and $1 \le j_1 < \ldots < j_s \le k$. Applying Lemma 2.3 we see that each term does not exceed $2^{-k} s p^{1/2} \log p$ in absolute value. Thus,

$$N(T) = R2^{-k} + O\left(2^{-k} \sum_{s=1}^{k} \binom{k}{s} s p^{1/2} \log p \right)$$

$$\begin{aligned} &= R2^{-k} + O\left(kp^{1/2}\log p\right) \\ &= R2^{-k} + O(mr2^{r/2}) = R2^{-k} + o(R2^{-k}). \end{aligned}$$

It follows from probabilistic arguments that for $2^k + o(2^k)$ binary k-tuples $T = (t_1, \ldots, t_k)$, both of the following statements are true: $t_{2j} \neq t_{2j+1}$ for $0.5m + o(m)$ values of $j = 1, \ldots, m$, and $t_{2j} \neq t_{2j-1}$ for $0.5m + o(m)$ values of $j = 1, \ldots, m$.

That means that, whatever the $(i+1)$th bit of x happens to be, if the vector $(B(x + j2^i))_{j=1}^k$ is such a k-tuple T, then among the m values $B(x + j2^{i+1})$, $j = 1, \ldots, m$, about half differ from their respective

$$B\left((x + j2^{i+1})^{(i)}\right) = B(x + j2^{i+1} \pm 2^i) = B\left(x + (2j \pm 1)2^i\right).$$

So,

$$\begin{aligned} &\sum_{i=0}^{l}\sum_{x=0}^{R-1} \sum_{B(x+j2^{i+1}) \neq B\left((x+j2^{i+1})^{(i)}\right)}^{m} 1 \\ &\quad \geq (l+1)\left(R2^{-k} + o(R2^{-k})\right)\left(2^k + o(2^k)\right)(0.5m + o(m)) \\ &\quad = 0.5Rlm + o(Rlm). \end{aligned}$$

For every i, $0 \leq i \leq l$ and every j, $1 \leq j \leq m$, we find

$$\left| \sum_{x=0 \atop B(x+j2^{i+1}) \neq B\left((x+j2^{i+1})^{(i)}\right)}^{R-1} 1 - \sum_{x=0 \atop B(x) \neq B\left(x^{(i)}\right)}^{2^r-1} 1 \right| \leq m2^{l+1} = o(2^r).$$

Therefore

$$\sum_{i=0}^{l} \sum_{x=0 \atop B(x) \neq B\left(x^{(i)}\right)}^{2^r-1} 1 \geq 2^{r-1}l + o(2^r l).$$

Thus there exists x_0, $0 \leq x_0 \leq 2^r - 1$, with

$$\sigma(B) \geq \sum_{i=0 \atop B(x_0) \neq B\left(x_0^{(i)}\right)}^{l} 1 \geq 0.5l + o(l) = 0.5r + o(r)$$

and we are done. □

Combining this result with Lemma 2.10 one gets the lower bound $0.5 \log \log p + O(1)$ on the CREW PRAM complexity of B. The bound is slightly weaker than that of Theorem 5.2 but it concerns a more powerful (but maybe less realistic) computational model.

Chapter 6

Approximation of the Discrete Logarithm by Real Polynomials

Here we consider some question about approximation of the discrete logarithm by real or complex polynomials. Unfortunately our results are weaker that those in our previous settings.

For a complex $z \in \mathbb{C}$ we define its 'residue' modulo an integer m as

$$\langle z \rangle_m = z - m \lfloor \Re z/m \rfloor - m \lfloor \Im z/m \rfloor \, i.$$

Theorem 6.1. *Let $0 \le N < N + H \le p - 1$, $\delta \ge 0.5$ and let $f(X) \in \mathbb{C}(X)$ be such that*

$$|\operatorname{ind} x - \langle f(x) \rangle_{p-1}| < \delta, \qquad x \in S,$$

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

$$\deg f \ge \min\{0.5 \log(H/\delta),\, H/2(s+1)\} - 2.$$

Proof. Let $n = \deg f$. Using the recurrent equation (2.3) as in the proof of Theorem 4.1 we derive that for at least $H - (n+2)(s+1)$

values of $x = N+1, \ldots, N+H$,

$$\sum_{i=0}^{n+1} (-1)^{n+1-i} \binom{n+1}{i} \operatorname{ind}(x+i) \equiv \Delta_x \pmod{p-1},$$

where

$$|\Delta_x| \le 2^{n+1}\delta.$$

Therefore, the rational function

$$\prod_{i=0}^{n+1} (X+i)^{(-1)^{n+1-i}\binom{n+1}{i}}$$

of degree at most 2^n takes at most $2(2^{n+1}\delta + 1))$ values for at least $H - (n+2)(s+1)$ values of $x = N+1, \ldots, N+H$. Therefore

$$H - (n+2)(s+1) \le 2^{n+1}(2^{n+1}\delta + 1) \le 2^{2n+3}\delta$$

and the result follows. □

Now we consider computing the rightmost bit of the discrete logarithm by real polynomials (on bits of the argument).

Theorem 6.2. *Let $r = \lfloor \log p \rfloor$ and let a multilinear polynomial*

$$f(X_1, \ldots, X_r) \in \mathbb{R}[X_1, \ldots, X_r]$$

be such that $f(u_1, \ldots, u_r) > 0$ if x is a quadratic residue modulo p and $f(u_1, \ldots, u_r) \le 0$ otherwise, where $x = u_1 \ldots u_r$ is the bit representation of x, $1 \le x \le 2^r - 1$. Then

$$\deg f \ge \log r + o(\log r).$$

Proof. Assuming that p is large enough we put $m = \left\lfloor \log r - \log^{1/2} r \right\rfloor$. Let $n = \deg f$ and

$$M = \sum_{l=0}^{n} \binom{m}{l}.$$

We consider all possible multilinear monomials $\mu_i(y)$, $i = 1, \ldots, M$ in $y = (y_1, \ldots, y_m)$ of degree at most n, arbitrarily ordered.

For every m-dimensional binary vector $y = (y_1, \ldots, y_m) \in [0,1]^m$ we have a representation of the form

$$f(x_1, \ldots, x_{r-m}, y) = \sum_{i=1}^{M} \mu_i(y) f_i(x_1, \ldots, x_{r-s}). \tag{6.1}$$

Let $\mathrm{Par}\,(y)$ denote the parity function, that is $\mathrm{Par}\,(y) = 0$ if an even number of the bits of y are 1, and $\mathrm{Par}\,(y) = 1$ otherwise. Thus, if $n < m$ then one easily verifies that

$$\sum_{y \in [0,1]^m} (-1)^{\mathrm{Par}\,(y)} \mu_i(y) = 0, \qquad i = 1, \ldots, M. \tag{6.2}$$

On the other hand, as in the proofs of Theorems 5.1 and 5.3, we see that for $0 \le x \le 2^{r-m} - 1$ any 2^m-dimensional pattern of signs occurs

$$2^{r-m} 2^{-2^m} + O(r 2^{r/2+m})$$

times among the coordinates of the vector $(f(x_1, \ldots, x_{r-s}, y))_{y \in [0,1]^m}$, where $x_1, \ldots, x_{r-m}$ is the bit representation of x. For p large enough that amount is positive. In particular, there is $x = x_1 \ldots x_{r-m}$ with $f(x_1, \ldots, x_{r-s}, y) > 0$ if $\mathrm{Par}\,(y) = 0$ and $f(x_1, \ldots, x_{r-s}, y) \le 0$ otherwise, for all $y \in [0,1]^s$. Thus,

$$\sum_{y \in [0,1]^m} (-1)^{\mathrm{Par}\,(y)} f(x_1, \ldots, x_{r-m}, y) > 0$$

which contradicts (6.1) and (6.2). Hence $n \ge m$. □

In particular, one sees that a threshold representation (corresponding to linear polynomials) of the rightmost bit of $\mathrm{ind}\, x$ is not possible.

More generally, using the same method one can show that any exponential polynomial $\Phi(x_1, \ldots, x_r)$ of the form

$$\Phi(X_1, \ldots, X_r) = \sum_{i=1}^{k} \exp\left(L_i(X_1, \ldots, X_r)\right) f_i(X_1, \ldots, X_r)$$

with linear forms L_i and polynomials f_i, $i = 1, \ldots, k$ with complex coefficients and such that $\Phi(x_1, \ldots, x_r) > 0$ if $x = u_1 \ldots u_r$ is a quadratic residue and $\Phi(u_1, \ldots, u_r) \le 0$ otherwise (thus it takes real values at binary vectors) satisfies the inequality

$$\sum_{i=1}^{k} \sum_{l=0}^{\deg f_i} \binom{m}{l} \ge 2^m,$$

where $m = \left\lfloor \log r - \log^{1/2} r \right\rfloor$.

Part III

Complexity of Breaking the Diffie–Hellman Cryptosystem and Other Applications

Chapter 7

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 extraction can be done in deterministic polynomial time because a primitive root g of $\mathbb{F}_q$ is known [37]. It is demonstrated in [27] that the correct square root can easily be determined (and the entire reduction can be done in $O(\log^2 q)$ arithmetic operations in $\mathbb{F}_q$).

Theorem 7.1. *Let $f(X) \in \mathbb{F}_q[X]$ be such that*

$$g^{x^2} = f(g^x), \qquad x \in S, \tag{7.1}$$

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 $\deg f \ge |R| - 2 \ge H - 2s - 3$. □

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 (7.1) with a polynomial f of degree $\deg f \le |S| - 1 = H - s - 1$.

Theorem 7.1 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 $|S| \sim 2H^{2/3}$.

Theorem 7.2. *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 $S \subseteq \{N+1, \ldots, N+H\}$ *with* $H \le q-1$. *Then*

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

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

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

Therefore, there is a pair $0 \le i < j \le K$ such that

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

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 $n \ge |R| - 2K$. □

Certainly, for any S one can satisfy (7.1) with a unique polynomial f of degree $\deg f \le |S| - 1$. Now we show that for a randomly selected set S that degree cannot be smaller. In particular, with probability $1 - o(1)$ we have $\deg f = |S| - 1$ for that polynomial.

Theorem 7.3. *Let q be sufficiently large and let S be a set of m random elements picked uniformly from $\{0, \dots, q-2\}$. Then the probability $P_k(p, m)$ that there exists a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree*

$$\deg f < m - k$$

and such that

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

satisfies the bound

$$P_k(q, m) \le \left(\frac{4m}{q-1}\right)^{k/2} + \begin{cases} 0, & \text{if } m - k \ge q^{1/3}, \\ (3q^{-1/3})^m, & \text{if } m - k < q^{1/3}. \end{cases}$$

Proof. We say that a set T is satisfied by a polynomial $f(X) \in \mathbb{F}_q[X]$ if the condition of the theorem is fulfilled for this pair (T, f), and that T is maximally satisfied by a polynomial $f(X) \in \mathbb{F}_q[X]$ if it is satisfied by this polynomial but any superset of T is not.

Suppose there are N various sets $S_i \subseteq \{0, \ldots, q-2\}$, $i = 1, \ldots, N$, that are maximally satisfied by polynomials f_i of degree at most $n = m - k$. In particular, polynomials f_i, $i = 1, \ldots, N$ are pairwise distinct.

Therefore, $|S_i \cap S_j| \le n$, $1 \le i < j \le N$, otherwise we would have $f_i = f_j$ being the unique polynomial satisfying the intersection $S_i \cap S_j$. In particular

$$\sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} 1 \le \sum_{\substack{T \subseteq \{0,\ldots,q-2\} \\ |T|=n+1}} 1 = \binom{q-1}{n+1}. \tag{7.2}$$

Also assume that only the first M of them are of size $|S_i| \ge 2n^{1/2}(q-1)^{1/2}$.

First of all we remark that $M = 0$ if $n \ge q^{1/3}$.

Indeed, from Theorem 7.2 (with $H = q-1$) we see that if $M \ne 0$ then

$$n \ge \frac{4n(q-1)}{2(q-1)} - \frac{4(q-1)}{2n^{1/2}(q-1)^{1/2}} - 1 = 2n - 2n^{-1/2}(q-1)^{1/2} - 1.$$

It is easy to verify that the last inequality fails for $n \ge q^{1/3}$.

Now we consider the case $n < q^{1/3}$. Again from Theorem 7.2 we see that in this case $|S_i| \le (2 + o(1))\, q^{2/3}$, $i = 1, \ldots, N$. We also claim that

$$\sum_{i=1}^{M} |S_i| < 2q. \tag{7.3}$$

Indeed, assuming the inverse inequality, we select $L \le M$ with

$$2q \le \sigma = \sum_{i=1}^{L} |S_i| \le 2q + 2q^{2/3}$$

We know that the number of S_i is at most

$$L \le \sum_{i=1}^{L} \frac{|S_i|}{2(qn)^{1/2}} \le \frac{2q + 2q^{2/3}}{2(qn)^{1/2}}.$$

By the inclusion-exclusion principle we know that

$$q \geq \sum_{i=1}^{L} |S_i| - \sum_{1 \leq i < j \leq L} |S_i \cap S_j| \geq \sigma - nL(L-1)/2 \geq (3/2 + o(1))\, q,$$

which is not possible for q large enough. Therefore (7.3) holds.

Now we estimate the sum

$$W = \sum_{i=1}^{M} \left(\frac{|S_i|}{q-1} \right)^{m+1}.$$

Obviously, $W = 0$ for $n \geq q^{1/3}$. For $n \leq q^{1/3}$, from (7.3) we derive

$$\begin{aligned} W &= \sum_{i=1}^{M} \left(\frac{|S_i|}{q-1} \right) \left(\frac{|S_i|}{q-1} \right)^{m} \leq (2 + o(1))^m\, q^{-m/3} \sum_{i=1}^{M} \frac{|S_i|}{q-1} \\ &\leq 3\,(2 + o(1))^m\, q^{-m/3} \leq (3q^{-1/3})^m \end{aligned}$$

for $n < q^{1/3}$ (and q large enough).

For $(n+1)$-element set $T \subseteq \{0, \ldots, q-2\}$ denote by f_T the unique polynomial of degree at most n such that T is satisfied by this polynomial. Also, denote by R_T the set which is maximally satisfied by f_T. Now we see

$$\begin{aligned} 1 - P_k(q,m) &= \sum_{|T|=n+1} \binom{q-1}{n+1}^{-1} \sum_{\substack{T \subseteq S \subseteq R_T \\ |S|=m}} \binom{q-n-2}{k}^{-1} \\ &\leq \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\ &= P_1 + P_2, \end{aligned}$$

where P_1 is the part of the sum over $i = 1, \ldots, M$ and P_2 is the part over $i = M+1, \ldots, N$. Thus

$$\begin{aligned} P_1 &= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{M} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\ &= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{M} \binom{|S_i|}{n+1} \binom{|S_i|-n-1}{k}. \end{aligned}$$

We have,

$$\binom{q-1}{n+1}^{-1}\binom{|S_i|}{n+1} \le \left(\frac{|S_i|}{q-1}\right)^{n+1}$$

and

$$\binom{q-n-2}{k}^{-1}\binom{|S_i|-n-1}{k} \le \left(\frac{|S_i|-n-1}{q-n-2}\right)^{k} \le \left(\frac{|S_i|}{q-1}\right)^{k},$$

therefore,

$$P_1 \le W \le \begin{cases} 0, & \text{if } n \ge q^{1/3}, \\ (3q^{-1/3})^m, & \text{if } n < q^{1/3}. \end{cases} \tag{7.4}$$

For P_2 we obtain

$$\begin{aligned} P_2 &= \binom{q-1}{n+1}^{-1}\binom{q-n-2}{k}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\ &= \binom{q-1}{n+1}^{-1}\binom{q-n-2}{k}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \binom{|S_i|-n-1}{k} \\ &\le \binom{q-1}{n+1}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \left(\frac{|S_i|}{q-1}\right)^{k} \\ &\le \binom{q-1}{n+1}^{-1} \left(\frac{2n^{1/2}(q-1)^{1/2}}{q-1}\right)^{k} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} 1. \end{aligned}$$

From (7.2) we derive

$$P_2 \le \left(\frac{4n}{q-1}\right)^{k/2} \le \left(\frac{4m}{q-1}\right)^{k/2}. \tag{7.5}$$

Combining (7.4) and (7.5) we obtain the results. □

We remark that the first term dominates if $k \le 2m/3$. Selecting $k = 1$ we obtain that if $m = o(q)$, for almost all sets of size m the smallest degree of the polynomial which they satisfy is $m - 1$.

Now we consider representation via algebraic functions.

Theorem 7.4. *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 $S \subseteq \{N+1, \ldots, N+H\}$ 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 $f_i(U) \in \mathbb{F}_q[U]$, $i = 1, \ldots, t$, are non-zero polynomials, $0 \le k_1 < \ldots < k_t = m$, $t \le m+1$.

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 $x \in R$

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

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

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

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

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

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 known 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 its maximal value for the identity 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. □

Once again, one can see that Theorem 7.4 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 7.5. *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 there is an absolute effectively computable constant $C > 0$ such that

$$n \ge C|S|^{3/2}/H.$$

Proof. For a polynomial $G(U, V) \in \mathbb{F}_q[U, V]$ and integer k (not necessarily positive) let us introduce the shift transformation

$$\sigma_k(G(U, V)) = U^{-l} G(g^k U, g^{k^2} U^{2k} V),$$

where l is chosen so that $\sigma_k(F)$ is a polynomial not divisible by U. One easily verifies that

$$\sigma_k\left(\sigma_m(G)\right) = \sigma_{k+m}(G).$$

and that

$$\sigma_k(G_1G_2) = \sigma_k(G_1)\sigma_k(G_2).$$

In particular, if $\Psi(U,V)$ is an absolutely irreducible polynomial which is not a univariate polynomial (either in U or in V) then $\Phi = \sigma_k(\Psi)$ is absolutely irreducible as well. We also note that for an absolutely irreducible Ψ and for $k \neq 0$, we have $\sigma_k(\Psi) \neq c\Psi$ for any non-zero $c \in \mathbb{F}_q$. Indeed, assuming that

$$\Psi(U,V) = \sum_{i=0}^{v} V^i f_i(U)$$

we would have $f_i(U) = cg^{ik^2}U^{2ik+l}f_i(g^kU)$, for each $i = 0,\ldots,v$. This is only possible if there is only one nonzero polynomial among the polynomials $f_0(U),\ldots,f_v(U)$. Thus $\Psi(U,V) = V^h f(U)$, where $h \leq v$ and $f(U)$ is a non-zero polynomial of degree at most v, which is not possible because of our assumptions.

First of all we denote by $\phi(U)$ and $\psi(V)$ two possible univariate factors of $F(U,V)$.

Let us consider the complete factorization of the fraction

$$\frac{F(U,V)}{\phi(U)\psi(V)}$$

over the algebraic closure of $\mathbb{F}_q$ (thus all factors are absolutely irreducible polynomials). Index the absolutely irreducible factors in this fraction as $\Psi_{ij}(U,V)$, that is,

$$F(U,V) = \phi(U)\psi(V)\prod \Psi_{ij}(U,V),$$

in the following way. Two factors share the same first index if and only if one is essentially a shift of the other:

$$\Psi_{ij}(U,V) = c\sigma_k(\Psi_{im})$$

for some integer k and some non-zero $c \in \mathbb{F}_q$. It follows from the two aforementioned properties of the transformation σ_k that this breakup is legitimate.

Among each family Ψ_{ij} of factors sharing a first index i, assign the index $j = 0$ to that factor having minimal degree in U, and for the other members of the family, let j denote the amount of shift, that is,

$$\Psi_{ij} = c\sigma_j(\Psi_{i0})$$

with some non-zero $c \in \mathbb{F}_q$.

Collect all factors $\Psi_{ij}(U, V)$ sharing the same second index j into a factor $F_j(U, V)$. So we have

$$F(U, V) = \prod_{j \in J} F_j(U, V),$$

where J is the set of possible shifts among absolutely irreducible factors of F and for each $F_j(U, V)$, $j \in J$, we have that $\sigma_{-j}F_j$ is a factor of F_0.

For each $j \in J$ we define the set $T_j \subset S$ such that

$$F_j(g^x, g^{x^2}) = 0, \qquad x \in T_j.$$

As in the proof of Theorem 7.2 we select $1 \le k_j \le 2H/|T_j|$ for which both

$$F_j(g^x, g^{x^2}) = 0 \quad \text{and} \quad F_j(g^{(x+k)}, g^{(x+k)^2}) = 0. \tag{7.6}$$

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

$$F_j(U, V) = \sigma_{k_j}\left(F_j(U, V)\right) = 0,$$

has at least $|T_j|^2/2H - 1$ solutions.

Let $F_j(U, V)$, $j \in J$, have degrees u_j and v_j in U and V, respectively. Then the U-degree of $\sigma_{k_j}F_j$ is at most $u_j + 2k_jv_j$ (its V-degree is still v_j). Now we claim that F_j is relatively prime to $\sigma_k(F_j)$ for any integer k and $j \in J$. Indeed, otherwise F_j would have two distinct absolutely irreducible factors Ψ and Φ satisfying $\Phi = c\sigma_k(\Psi)$ with some non-zero $c \in \mathbb{F}_q$, but then Φ is a divisor of F_{j+k} rather than of F_j. Therefore, from the Bézout's Theorem we derive the inequality

$$|T_j|^2/2H - 1 \le u_jv_j + (u_j + 2k_jv_j)v_j \le 2u_jv_j + 2k_jv_j^2. \tag{7.7}$$

Let J_1 be the set of $j \in J$ with $u_j \geq k_j v_j$ and J_2 be the set of $j \in J$ with $u_j < k_j v_j$.

For $j \in J_1$ we have

$$|T_j|^2/2H \leq 4u_j v_j + 1 \leq 5u_j v_j \leq 5(\deg F_j)^2.$$

Therefore

$$n \geq \sum_{j \in J_1} \deg F_j \geq (10H)^{-1/2} \sum_{j \in J_1} |T_j|. \tag{7.8}$$

Let us turn to J_2. We notice that

$$u_j \geq |j| v_j. \tag{7.9}$$

Indeed, assume that $\Psi_{i0}(U, V)$ is an absolutely irreducible divisor of $F_0(U, V)$ such that $\Psi_{ij}(U, V)$ is a divisor of $F_j(U, V)$. Assume that

$$v = \deg_V \Psi_{i0} = \deg_V \Psi_{ij}, \quad w = \deg_U \Psi_{i0}(U, V), \quad u = \deg_U \Psi_{ij}(U, V).$$

One remarks that the coefficient of V^0 in $\Psi_{i0}(U, V)$ is a polynomial in U of some degree $0 \leq r \leq w$, and the coefficient of V^v is a polynomial in U of some degree $0 \leq s \leq w$. The first polynomial is not 0 because otherwise Ψ_{i0} would be divisible by V; the second one is not zero because the V-degree of $F_j(U, V)$ is v. Let l be the power of U in the definition of σ_j. We have

$$l \leq \min\{r,\ s + 2jv\}.$$

On the other hand,

$$u \geq \max\{r - l,\ s + 2jv - l\}.$$

If $j > 0$ than we see that

$$u \geq s + 2jv - l \geq s + 2jv - r \geq 2jv - r \geq 2jv - w.$$

If $j < 0$ than

$$u \geq r - l \geq r - 2jv - s \geq -2jv - s \geq -2jv - w.$$

From our selection of Ψ_{i0} we also see $u \ge w$. Combining these inequalities we derive $u \ge |j|v$ and (7.9) follows.

Then, for $j \in J_2$ we have

$$|T_j|^2/2H \le 4k_j v_j^2 + 1 \le 5k_v v_j^2 \le 10Hv_j^2/|T_j|.$$

Hence

$$v_j \ge 20^{-1/2}|T_j|^{3/2}H^{-1}, \qquad j \in J_2.$$

From this and (7.9) we derive

$$n \ge \sum_{j \in J_2} \deg F_j \ge \sum_{j \in J_2} u_j \ge \sum_{j \in J_2} |j| v_j \ge 20^{-1/2}H^{-1} \sum_{j \in J_2} |j||T_j|^{3/2}.$$

If $0 \in J_2$ we can include T_0 into the sum by:

$$\deg F_0 \ge v_0 \ge 20^{-1/2}H^{-1}|T_0|^{3/2},$$

thus obtaining

$$n \ge 20^{-1/2}H^{-1} \sum_{j \in J_2} \max\{|j|, 1\}|T_j|^{3/2}.$$

One verifies that

$$\sum_{j \in J_2} |T_j| \le \left(\sum_{j \in J_2} \max\{|j|, 1\}^{-2} \right)^{1/3} \left(\sum_{j \in J_2} \max\{|j|, 1\}|T_j|^{3/2} \right)^{2/3}$$

and

$$\sum_{j \in J_2} \max\{|j|, 1\}^{-2} < 1 + 2\sum_{j=1}^{\infty} j^{-2} = 1 + 2\frac{\pi^2}{6} < 5.$$

Therefore

$$n \ge (10H)^{-1} \left(\sum_{j \in J_2} |T_j| \right)^{3/2}. \tag{7.10}$$

The univariate factors ϕ and ψ are easier to treat. The set T_u of $x \in S$ for which $\phi(g^x) = 0$ is of cardinality

$$|T_u| \le \deg \phi \le n. \tag{7.11}$$

The set T_v of $x \in S$ for which $\psi(g^{x^2}) = 0$ satisfies the inequality

$$|T_v| = O(Hq^{-1/2} \deg \psi) = O(nHq^{-1/2}), \tag{7.12}$$

which follows from the general bound of [22] on the number of solutions of polynomial congruences over an incomplete residue system.Indeed in our case we have up to $\deg \psi$ congruences of the form $x^2 \equiv \operatorname{ind} v \pmod{q-1}$ for each solution v of the equation $\psi(v) = 0$. Taking into account that

$$\max\left\{|T_u|, |T_v|, \sum_{j \in J_1} |T_j|, \sum_{j \in J_2} |T_j|\right\} \geq |S|/4$$

from (7.8), (7.10), (7.11), and (7.12) we derive the result. □

It is obvious that for any $S \subseteq \{0, \ldots, q-2\}$ there is a polynomial $F(U, V) \in \mathbb{F}_q[U, V]$ of degree at most $(2|S|)^{1/2}$ which satisfies the condition of Theorem 7.5. Now we show that for almost all sets S this bound is the best possible, to within a multiplicative constant.

Theorem 7.6. *Let q be sufficiently large, $0 < \varepsilon < 2\delta/3$, $\delta < 1$ and $m \leq q^{1-\delta}$. Let S be a set of m random elements picked uniformly from $\{0, \ldots, q-2\}$. Then the probability $P_{\varepsilon,\delta}(p, m)$ that there exists a polynomial $F(U, V) \in \mathbb{F}_q[U, V]$ of degree*

$$\deg F < \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 1$$

and such that

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

satisfies the bound

$$P_{\varepsilon,\delta}(q, m) \leq c^m q^{-(\delta/3 - \varepsilon/2)m},$$

where $c > 0$ is an absolute constant.

Proof. We say that a set T is satisfied by a polynomial $F(U, V) \in \mathbb{F}_q[U, V]$ if the condition of the theorem is fulfilled for this pair (T, F),

and that T is maximally satisfied by a polynomial $F(U,V) \in \mathbb{F}_q[U,V]$ if it is satisfied by this polynomial but any superset of T is not.

Suppose there are N various sets $S_i \subseteq \{0,\ldots,q-2\}$, $i = 1,\ldots,N$, that are maximally satisfied by polynomials $F_i(U,V) \in \mathbb{F}_q[U,V]$ of degree at most $n = \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 2$. In particular, polynomials F_i, $i = 1,\ldots,N$ are pairwise distinct, thus

$$N \le q^{(n+2)(n+1)/2}.$$

From Theorem 7.5 we derive $|S_i| = O\left((nq)^{2/3}\right)$. Therefore

$$\begin{aligned} P_k(p,m) &= \binom{q-1}{m}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{m} \le \sum_{i=1}^{N} \left(\frac{|S_i|}{q-1}\right)^m \\ &\le q^{(n+2)(n+1)/2} \left(cn^{2/3}q^{-1/3}\right)^m \\ &\le c^m n^{2m/3} q^{(n+2)(n+1)/2 - m/3} \\ &\le c^m m^{m/3} q^{(\varepsilon/2 - 1/3)m} \\ &\le c^m q^{-(\delta/3 - \varepsilon/2)m} \end{aligned}$$

with some constant $c > 0$. □

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 whether $\operatorname{ind} v = \operatorname{ind}^2 u$ 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 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 or the value of one of two variables $u, v \in \mathbb{F}_q$ for which we want to verify that $\operatorname{ind} v = \operatorname{ind}^2 u$.

Each gate of level $d-1 \geq k \geq 1$ 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 $\#$ stands 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 7.7. *Let $\gamma, \delta > 0$ be constants such that*

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

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

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

and for any $u, v \in \mathbb{F}_q^*$ such that there is no $x \in \{0, \ldots, q-2\}$ with $u = g^x$, $v = g^{x^2}$ it outputs **NO** *with probability 1. 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 of random variables used by the circuit C. Obviously l 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, $C_\vartheta(u, v) = \mathbf{YES}$. Therefore, there is $\vartheta_0 \in \{0,1\}^l$ for which C_{ϑ_0} 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} has already been defined, $2 \le i \le d$. We define R_i as the set of $x \in R_{i-1}$ for which $\psi(g^x, g^{x^2}) \ne 0$ 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 follows from Theorem 7.5 that the number of $x \in R_{i-1} \subseteq S$ for which such a function vanishes is at most $O(2^{2i/3} H^{2/3})$. Therefore

$$|R_{i-1}| \ge |R_i| + O(5^{d-i} 2^{2i/3} H^{2/3}).$$

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

$$|R_d| \ge |S|^{1-\gamma} + O(5^d H^{2/3}) \ge 0.5 |S|^{1-\gamma}$$

if

$$d \le \log_6(|S|^{1-\gamma} H^{-2/3}) \le ((1-\gamma)\delta - 2/3) \log_6 H$$

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 7.5 we find

$$2^{d-1} \ge 0.3 |R_d| H^{-2/3} \ge 0.3 H^{(1-\gamma)\delta - 2/3}$$

and the claim follows. □

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

Also, we see that if $H \geq \exp\left((\log q)^{\varepsilon}\right)$ 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), but 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 [9, 10]. 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 7.8. *Let Boolean functions $B_i(U_1, \ldots, U_r)$, $i = 1, \ldots, r$, be such that*

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

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

$$\max_{1 \leq i \leq r} \deg B_i \geq r - \log(2s + 3).$$

Proof. Denote by

$$\mathrm{Tr}\,(z) = z + z^2 + z^4 + \ldots + z^{2^{r-1}}$$

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 [25]. 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

$$g^{x^2} = \sum_{i=1}^{r} \omega_i B_i\,(\mathrm{Tr}\,(\vartheta_1 g^x), \ldots, \mathrm{Tr}\,(\vartheta_r g^x))$$

for at least $2^r - 1 - s$ values of $x \in \mathbb{F}_{2^r}^*$. Let us consider the polynomial

$$f(U) = \sum_{i=1}^{r} \omega_i B_i\,(\mathrm{Tr}\,(\vartheta_1 U), \ldots, \mathrm{Tr}\,(\vartheta_r U))\,.$$

One sees, that after the reduction of all exponents modulo $2^r - 1$ the new polynomial $h(U)$ contains exponents which are integer numbers with at most n non-zero bits, where

$$n = \max_{1 \leq i \leq r} \deg B_i.$$

Therefore, the largest of such exponents is $\deg h \leq 2^r - 2^{r-n}$

As in the proof of Theorem 7.1 we obtain that the polynomial $\Psi(U) = gU^2 h(U) - h(gU)$ has at least $2^r - 1 - 2s$ zeros over $\mathbb{F}_{2^r}$ and is of degree at most $\deg \Psi \leq 2^r - 2^{r-n} + 2$. To finish the proof it is enough to show that $\Psi(U)$ is a non-zero polynomial.

First of all we note, that $h(U)$ is a non-zero polynomial. Indeed, $h(g^x) = g^{x^2} \neq 0$, $x \in S$.

Let E denote the set of exponents of $h(U)$, $E \neq \emptyset$. Hence, if $\Psi(U)$ is identical to zero then $E \equiv E + 2 \pmod{2^r - 1}$. However the last property means that $E \equiv E + 2m \pmod{2^r - 1}$ for any integer m, thus $E = \{0, 1, \ldots, 2^r - 2\}$. Therefore, $\deg h = 2^r - 2$ thus $n \geq r - 1$. □

An analogue of Theorems 5.2 and 7.7 can be obtained as well (for deterministic Boolean circuits). Using Theorem 7.8 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 $C \log r$.

We note that there are several distinct natural interpretations of the Boolean model of computation over $\mathbb{F}_{2^r}$. The model we use here (related to coordinates with respect to a fixed basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$) has also been studied in [7].

Now we demonstrate how a lower bound on the Boolean complexity of breaking the Diffie–Hellman cryptosystem modulo a prime p can be derived from the general lower bound of Theorem 8.1 of Chapter 8.

Theorem 7.9. *Let p be a prime and let $r = \lfloor \log p \rfloor + 1$. Assume that a Boolean function $B(U_1, \ldots, U_r, V_1, \ldots, V_r)$ of $2r$ Boolean variables is such that for any x and y, $1 \leq x, y \leq p-1$, the value $B(u_1, \ldots, u_r, v_1, \ldots, v_r)$ equals the second leftmost bit of the smallest non-negative residue of g^t modulo p, where $t = \operatorname{ind} x \operatorname{ind} y$ and $x = u_1 \ldots u_r$ and $y = v_1, \ldots, v_r$ are the bit representations of x and y. Then there exists an absolute constant $c > 0$ such that the bound*

$$\sigma(B) \geq c r^{1/2}$$

holds.

Proof. Select $y \equiv g^3 \pmod{p}$. Then the function B gives the second leftmost bit of the the smallest non-negative residue of x^3. Applying Theorem 8.1 below we derive the result. □

Using Theorem 7.9 and Lemma 2.10 we derive that the CREW PRAM complexity CREW PRAM (DH_p) of breaking the Diffie–Hellman cryptosystem modulo a prime p satisfies the inequality

$$\text{CREW PRAM}\,(\mathrm{DH}_p) \geq 0.25 \log\log p + o(\log\log p).$$

Chapter 8

Trade-off Between the Boolean and Arithmetic Depths of Modulo p Functions

For a polynomial $f(X) \in \mathbb{Z}[X]$ we consider Boolean functions producing the second leftmost bit of the smallest non-negative residues of $f(x)$ modulo p from the bit representation of x and obtain lower bound on their sensitivity (see Chapter 5 for the definition of this notion). Then a similar but a weaker bound is obtained for the sensitivity of Boolean functions producing the second leftmost bit of rational functions modulo p.

We apply these results to show that at least one of arithmetic and Boolean depths of any non-linear function modulo p is large enough.

As before, we assume that all arguments x contain the same number r of bits (adding several leading zeros if necessary) where $r = \lfloor \log p \rfloor$. Thus, as before, each such function is defined on a portion $1 \leq x \leq 2^r - 1 \leq p - 1$ of the complete residue system modulo p. Moreover, we assume that the values of functions are all contain the same number $r+1$ bits. Certainly the leftmost bit could be zero for almost all values (if say $p = 2^r + 1$ is a Fermat number). This is why the second leftmost

bit is much more convenient to work with.

Theorem 8.1. *Suppose that $f(X) \in \mathbb{Z}[X]$ is a polynomial of degree $\deg f \geq 3$ with a non vanishing modulo p leading coefficient. Let $r = \lfloor \log p \rfloor$ and let a Boolean function $B(U_1, \ldots, U_r)$ be such that for any x, $0 \leq x \leq 2^r - 1$, $B(u_1, \ldots, u_r)$ equals the second leftmost bit of the the smallest non-negative residue of $f(x)$ modulo p where $x = u_1 \ldots u_r$ is the bit representation of x. For any $\varepsilon > 0$ there is a constant $c(\varepsilon) > 0$ depending on ε only such that if*

$$\deg f \leq 2^{(1-\varepsilon)r/2}$$

then the bound

$$\sigma(B) \geq c(\varepsilon) r^{1/2}$$

holds.

Proof. Let $n = \deg f$. We define

$$k = \left\lfloor r/2 - \log n - r^{1/2} \log^2 r \right\rfloor, \quad s = \left\lfloor k^{1/2} \right\rfloor, \quad m = \left\lfloor \frac{s}{\log 9C} \right\rfloor,$$

where C is the constant of Lemma 2.7.

We remark that

$$s(m+1) \leq k \leq r$$

for p large enough and that

$$m \geq c(\varepsilon) r^{1/2}$$

for some constant $c(\varepsilon) > 0$ depending on ε only.

We claim that it is enough to prove that there exists x, $0 \leq x \leq 2^{r-k}-1$, such that the fractional parts

$$\left\{ \frac{f(2^k x)}{p} \right\} < \frac{2^{r-2}}{p},$$

and

$$\frac{2^{r-2}}{p} \leq \left\{ \frac{f(2^k x + 2^{si})}{p} \right\} < \frac{2^{r-1}}{p}, \qquad i = 1, \ldots, m.$$

Indeed from these inequalities one sees that the second leftmost bit of the smallest non-negative residue of $f(2^k x)$ modulo p is 0 and the second leftmost bit of the smallest non-negative residue of $f(2^k x + 2^{si})$ modulo p is 1 for $i = 1, \ldots, m$. Hence the existence of such x implies that $\sigma(B) \geq m$ which yields the required estimate.

To proof that such x exists we show that the discrepancy Δ of the sequence

$$\left(\left\{\frac{f(2^k x)}{p}\right\}, \left\{\frac{f(2^k x + 2^s)}{p}\right\}, \ldots, \left\{\frac{f(2^k x + 2^{sm})}{p}\right\}\right)_{x=0}^{2^{r-k}-1}$$

of 2^{r-k} points of the $(m+1)$-dimensional unit cube satisfies the inequality

$$\Delta < \left(\frac{2^{r-2}}{p}\right)^{m+1}.$$

Let us put $L = 2^s - 1$. From Lemmas 2.5, 2.8 and 2.7 we derive that the discrepancy of this sequence satisfies

$$\begin{aligned}
\Delta &\leq C^{m+1} 2^{-s+O(1)} + n 2^{k-r+O(m)} p^{1/2} \log p \sum_{0<\|\mathbf{a}\|\leq L} \frac{1}{r(\mathbf{a})} \\
&\leq 9^{-m+O(1)} + n 2^{k-r/2+O(m)} r^{m+2} \\
&= 9^{-m+O(1)} + 2^{-r^{1/2}\log^2 r + O(m \log r)} \leq 8^{-m-1} \\
&< \left(\frac{2^{r-2}}{p}\right)^{m+1},
\end{aligned}$$

provided that p is large enough. Therefore the claimed x exits and the desired result follows. □

Theorem 8.2. *Suppose that $f(X)/g(X) \in \mathbb{Z}[X]$ is a rational function which is not a polynomial modulo p,*

$$n = \max\{\deg f, \deg g\} \leq 0.6 r^{1/2},$$

where $r = \lfloor \log p \rfloor$. Let a Boolean function $B(U_1, \ldots, U_r)$ be such that for any x, $0 \leq x \leq 2^r - 1$, with $g(x) \not\equiv 0 \pmod p$, $B(u_1, \ldots, u_r)$

equals the second leftmost bit of the smallest non-negative residue of $h(x)$ *modulo* p *where* $x = u_1 \dots u_r$ *is the bit representation of* x. *Then the bound*

$$\sigma(B) \geq \frac{1}{16} r + o(r)$$

holds.

Proof. Without loss of generality we assume that p is large enough. We proceed as in the proof of Theorem 8.1.

We define

$$k = \lfloor r/4 \rfloor, \qquad m = \left\lfloor \frac{r}{16} - r^{1/2} \right\rfloor.$$

It is easy to verify that

$$m \leq k - n(n-1)/2,$$

thus we can select the first m elements $s_1, \dots, s_m$ of the sequence defined in Lemma 2.9 and put

$$e_0 = 0, \qquad e_i = 2^{s_i}, \quad i = 1, \dots, m.$$

For $g(x) \not\equiv 0 \pmod p$ we denote by $h(x)$ the smallest non-negative residue of $f(x)/g(x)$ modulo p.

Denote by X the set of x, $0 \leq x \leq 2^{r-k} - 1$ for which

$$\prod_{i=0}^{m} g(2^k x + e_i) \not\equiv 0 \pmod p.$$

Obviously $2^{r-k} - (m+1)n \leq |X| \leq 2^{r-k}$.

We claim that it is enough to prove that there exists $x \in X$ such that

$$\left\{ \frac{h(2^k x)}{p} \right\} < \frac{2^{r-2}}{p},$$

and

$$\frac{2^{r-2}}{p} \leq \left\{ \frac{h(2^k x + e_i)}{p} \right\} < \frac{2^{r-1}}{p}, \qquad i = 1, \dots, m.$$

Indeed from these inequalities one sees that the second leftmost bit of $h(2^k x)$ modulo p is 0 and the second leftmost bit of $h(2^k x + 2^{s_i})$ modulo p is 1 for $i = 1, \ldots, m$. Hence the existence of such x implies that $\sigma(B) \geq m$ which yields the required estimate.

To proof that such x exists we show that there following system of congruences discrepancy Δ of the sequence

$$h(2^k x + e_i) \equiv b_i + y_i - z_i \pmod{p}, \qquad i = 0, \ldots, m,$$

where $b_0 = 2^{r-3}$, $b_i = 2^{r-2} + 2^{r-3}$, $i = 1, \ldots, m$, has a solution with

$$x \in X, \qquad 0 \leq y_i, z_i \leq 2^{r-3} - 1, \quad i = 0, \ldots, m.$$

For the number T of such solutions we have

$$T = \frac{1}{p^{m+1}} \sum_{x \in X} \sum_{\substack{y_0, \ldots, y_m = 0 \\ z_0, \ldots, z_m = 0}}^{2^{r-3}-1} \times \sum_{|\mathbf{a}| \leq (p-1)/2} \mathbf{e}\left(\sum_{i=0}^{m} a_i \left(h(2^k x + e_i) - b_i - y_i + z_i \right) / p \right),$$

where $\mathbf{a} = (a_0, \ldots, a_m) \in \mathbb{Z}^{m+1}$ runs through all p^{m+1} integer $(m+1)$-dimensional vectors with

$$|va| = \max_{i=0,\ldots,m+1} |a_i| \leq (p-1)/2.$$

Making the summation over $\mathbf{a}$ external and separating the term corresponding to the zero vector we obtain

$$|T - |X| 2^{(m+1)(r-3)} p^{-m-1}| \leq \frac{1}{p^{m+1}} \sum_{0 < |\mathbf{a}| \leq (p-1)/2} \left| \sum_{x \in X} \mathbf{e}\left(\sum_{i=0}^{m} a_i h(2^k x + e_i)/p \right) \right| \times \left| \prod_{i=0}^{m} \sum_{y_i=0}^{2^{r-3}-1} \mathbf{e}\left(\sum_{i=0}^{m} a_i y_i / p \right) \right|^2.$$

From Lemmas 2.5 and 2.9 we obtain that

$$\left| \sum_{x \in X} \mathbf{e}\left(\sum_{i=0}^{m} a_i h(2^k x + e_i)/p \right) \right| \leq n(m+1) p^{1/2} \log p + n(m+1)$$

(the last term takes care about the values which are not in X and are not poles of the rational function in the exponent either). Therefore

$$\begin{aligned}
&|T - |X|2^{2(m+1)(r-3)}p^{-m-1}| \\
&\quad \le \frac{2n(m+1)p^{1/2}\log p}{p^{m+1}} \sum_{0<|\mathbf{a}|\le (p-1)/2} \left| \prod_{i=0}^{m} \sum_{y_i=0}^{2^{r-3}-1} \mathbf{e}\left(\sum_{i=0}^{m} a_i y_i/p\right)\right|^2 \\
&\quad \le \frac{2n(m+1)p^{1/2}\log p}{p^{m+1}} \left| \prod_{i=0}^{m} \sum_{a_i=-(p-1)/2}^{(p-1)/2} \sum_{y_i=0}^{2^{r-3}-1} \mathbf{e}(a_i y_i/p)\right|^2 \\
&\quad = \frac{2n(m+1)p^{1/2}\log p}{p^{m+1}} \left(\sum_{a=0}^{p-1} \left| \sum_{y=0}^{2^{r-3}-1} \mathbf{e}\left(ay/p\right)\right|^2 \right)^{m+1}.
\end{aligned}$$

Taking into account that

$$\sum_{a=0}^{p-1} \left| \sum_{y=0}^{2^{r-3}-1} \mathbf{e}\left(ay/p\right)\right|^2 = p2^{r-3}$$

we derive

$$|T - |X|2^{2(m+1)(r-3)}p^{-m-1}| \le 2n(m+1)2^{(m+1)(r-3)}p^{1/2}\log p$$

Hence

$$T \ge 2^{(m+1)(r-3)}Q,$$

where

$$\begin{aligned}
Q &= |X|2^{(m+1)(r-3)}p^{-m-1} - 2n(m+1)p^{1/2}\log p \\
&= 2^{r-k+0(1)}\left(\frac{2^{r-3}}{p}\right)^{m+1} - 2^{r/2+O(\log r)} \\
&\ge 2^{r-k-4m+0(1)} - 2^{r/2+O(\log r)} \\
&= 2^{r/2+4r^{1/2}+O(1)} - 2^{r/2+O(\log r)} > 0
\end{aligned}$$

provided that p is large enough.

Therefore the claimed x exits and the desired result follows. □

Now let us consider the class $\mathrm{BC}(d)$ of Boolean circuits of depth d which has been defined in Chapter 5 and the class $\mathrm{AC}_p(d)$ of arithmetic circuits of depth d which is defined quite analogously with only difference that the gates of the starting level accept either constants or the value of the input variable x, and each gate of level $k \geq 1$ accepts two values from some gates of previous levels, ϕ_1, ϕ_2, and then computes and outputs the value of $\phi_1 \# \phi_2$, where $\#$ stands for an arithmetic operation modulo p, that is, $\# \in \{+, -, \times, /\}$.

We also consider the class $\mathrm{DFAC}_p(d)$ of division free arithmetic circuits of depth d we make use addition, subtraction or multiplication modulo p only.

We define modulo p functions as functions taking values in the range $0 \leq f(x) \leq p-1$ for any $x = 0, \ldots, 2^r - 1$.

For a modulo p function f one can define its Boolean depth $D_B(f)$ as the smallest d for which there exist $r+1$ circuits $C_j \in \mathrm{BC}(d)$, $j = 1, \ldots, r+1$, such that the binary vector

$$(C_1(u_1, \ldots, u_r), \ldots, C_{r+1}(u_1, \ldots, x_r)), \qquad 0 \leq x \leq 2^r - 1,$$

gives the bit representation of $f(x)$, where $x = u_1 \ldots u_r$ is the bit representation of x, $r = \lfloor \log p \rfloor$.

Accordingly, for a modulo p function f one can define its arithmetic depth $D_A(f)$ as the smallest d for which there exists a circuit $C \in \mathrm{AC}_p(d)$ such that

$$f(x) = C(x), \qquad 0 \leq x \leq 2^r - 1.$$

Theorem 8.3. *Suppose that a modulo p function h is neither a constant nor a linear function modulo p. Then the bound*

$$\max\{D_A(h),\, D_B(h)\} \geq 0.125 \log r + o(\log r)$$

holds.

Proof. Assume that $D_A(h) \leq 0.4 \log r$.

Then h is given by a rational function of $f(X)/g(X) \in \mathbb{F}_p(X)$ with

$$n = \max\{\deg f, \deg g\} \le 2^{D_A(f)} \le r^{2/5}.$$

If this is a 'proper' rational function (i.e., not a polynomial) then we apply Theorem 8.2 and we derive that the sensitivity of any Boolean function B coinciding with the second leftmost bit of $h(x)$ is $\Omega(r)$. Hence, from Lemma 2.10 we derive

$$D_B(f) \ge \text{CREW PRAM}\,(B) \ge 0.5 \log r + o(\log r).$$

If this function is a polynomial of degree $n \ge 3$ we apply Theorem 8.1 we derive that the sensitivity of any Boolean function B coinciding with the second leftmost bit of $f(x)$ is $\Omega(r^{1/2})$. Hence, from Lemma 2.10 we derive

$$D_B(f) \ge \text{CREW PRAM}\,(B) \ge 0.25 \log r + o(\log r).$$

If this function is a polynomial of degree $n = 2$, then we note that $h_0(X) = h(h(X))$ is a polynomial over $\mathbb{F}_p$ of degree $\deg h = 4$. Therefore, we have the inequality

$$D_B(h) \ge 0.5 D_B(h_0) \ge 0.125 \log r + o(\log r),$$

which finishes the proof. □

In the partial case of the modular inversion $f(X) \equiv 1/X \pmod p$ a result similar to Theorem 8.3 has been obtained in [13].

For division free arithmetic a stronger bound can be obtained.

For a modulo p function f one can define its division-free arithmetic depth $D_{DFA}(f)$ as the smallest d for which there exists a circuit $C \in \text{DFAC}_p(d)$ such that

$$f(x) = C(x), \qquad 0 \le x \le 2^r - 1.$$

Theorem 8.4. *Suppose that a modulo p function f is neither a constant nor a linear function modulo p. Then for any $\varepsilon > 0$ and sufficiently large p at least one of the bounds*

$$D_{DFA}(f) \geq (0.5 - \varepsilon)r$$

or

$$D_B(f) \geq (0.125 - \varepsilon)\log r.$$

holds.

Proof. Assume that $D_{DFA}(f) \leq (0.5 - \varepsilon)r/2$.

Let $n \geq 2$ be the degree of f as a polynomial over $\mathbb{F}_p$. Obviously

$$n \leq 2^{D_{DFA}(f)} \leq 2^{(1-2\varepsilon)r/2}.$$

provided that p is large enough.

If $n \geq 3$ then from Theorem 8.1 we derive that the sensitivity of any Boolean function B coinciding with the second leftmost bit of $f(x)$ is $\Omega(r^{1/2})$. Hence, from Lemma 2.10 we derive

$$D_B(f) \geq \text{CREW PRAM}\,(B) \geq 0.25\log r + o(\log r).$$

If $n = 2$, then we note that $f_0(X) = f(f(X))$ is of degree $\deg f_0 = 4$. Therefore, we have the inequality

$$D_{DFA}(f) \geq 0.5 D_{DFA}(f_o) \geq 0.125\log r + o(\log r),$$

which finishes the proof. □

Chapter 9

Permutation Polynomials, Powers, Zech's Logarithm, Primitive Root Testing 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 [29], Problem 10, that apparently both of these polynomials cannot be of small degree. Here we show that this is really the case.

Theorem 9.1. *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. □

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

Theorem 9.2. *Let d be an integer with $0 \le d \le q-1$ and let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree n such that $f(X) \ne a_n X^n$. Assume that*

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

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

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

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

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, $T^2 \le (q-1)n + (q-1)Q$, 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 $a_m X^m$, $a_n a_m \ne 0$, $0 \le m < n$, we find then this is possible only if $z^m = z^d$ and $z^n = z^d$. In particular, $z^m = z^n$; therefore $Q \le n$ and the result follows. □

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

Let g be a primitive root of $\mathbb{F}_q$. For $x \in \{0, \ldots, q-2\}$, *Zech's logarithm* $Z(x)$ is defined by the relation

$$g^{Z(x)} = g^x + 1, \qquad 0 \le Z(x) \le q-2.$$

if $g^x \neq -1$ and $Z(x) = 0$ if $g^x = -1$. (When q is odd we will have $g^x = -1$ if $x = (q-1)/2$; when q is even, $g^x = -1$ if $x = 0$.)

Theorem 9.3. *Let $-1 \le N < N+H \le q-2$ and let $d > 1$ be a divisor of $q-1$. Let $(u(x))$ be an integer linear recurring sequence of order n such that*

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

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

$$n \ge \frac{H}{2s + 4 + q^{1/2} \log q} - 1.$$

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

$$Z(x+i) \equiv u(x+i) \pmod{d}, \qquad i = 0, \dots, n$$

and

$$g^{x+i} \neq -1, \qquad i = 0, \dots, n.$$

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

$$\sum_{i=0}^{n} c_i Z(x+i) \equiv 0 \pmod{d}. \tag{9.1}$$

for at least $H - (n+1)(s+2)$ values of $x = N+1, \dots, N+H$. The congruence (4.1) is equivalent to the statement that the product

$$(g^x + 1)^{c_0} (g^{x+1} + 1)^{c_1} \dots (g^{x+n} + 1)^{c_n}$$

is a d-th power residue modulo p. Thus, for a non-trivial character χ of $\mathbb{F}_p^*$ of order d, we have

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

On the other hand, because $c_n = -1$ Lemma 2.6 can be applied. Therefore,

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

and the result follows. □

==========

Now we obtain an analogue of Theorem 5.3 for Boolean functions deciding if a given number is a primitive root modulo p.

Theorem 9.4. *Let a Boolean function $B(U_1, \ldots, U_r)$ of $r = \lfloor \log p \rfloor$ Boolean variables be such that for any x, $1 \le x \le 2^r - 1$,*

$$B(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } x \text{ is not a primitive root modulo } p, \\ 1, & \text{if } x \text{ is a primitive root modulo } p, \end{cases}$$

where $x = u_1 \ldots u_r$ is the bit representation of x. Then

$$\sigma(B) \ge 0.25r + o(r).$$

Proof. We put

$$k = \left\lfloor 0.25r - r \log^{-1/2} r \right\rfloor.$$

It is easy to see that the theorem will be proved if we to show that there exist y, $1 \le y \le 2^{r-k}$ such that $2^k y$ is a primitive root modulo p but $2^k y + 2^i$, $i = 0, \ldots, k-1$ are quadratic residues. Indeed in this case $\sigma(B) \ge k$.

Quite similar to the Exercise 12.c to Chapter 6 of [44] one obtain that the number N of such y can be expressed as

$$N = \sum_{d \mid p-1} \frac{\mu(d)}{2^k d} \sum_{y=1}^{2^{r-k}} \prod_{i=0}^{k-1} \left(1 + \chi(2^k y + 2^i)\right) \sum_{\lambda=0}^{d-1} \mathbf{e}\left(\lambda \mathrm{ind}\,(2^k y)/d\right)$$

where $\mu(m)$ is the Möbius function, $\chi(z)$ is the quadratic character modulo p.

For each divisor d of $p-1$ the inner sum contains $d2^k$ character sums of the form

$$\sum_{y=1}^{2^{r-k}} \prod_{i=0}^{m} \chi(2^k y + 2^{j_i}) \mathbf{e}\left(\lambda \mathrm{ind}\,(2^k y)/d\right),$$

where $0 \le m \le k-1$, $0 \le j_1 < \ldots < j_m \le 2^{k-1}$. The sum corresponding to $m = 0$ equals 2^{r-k}, to others Lemma 2.3 can be applied thus

each of them does not exceed $(k+1)p^{1/2}\log p$. Therefore

$$N = \sum_{d|p-1} \frac{\mu(d)}{2^k d} \left(2^{r-k} + O(d2^k k p^{1/2}\log p)\right).$$

Let $\varphi(m)$ denote the Euler function and let $\nu(k)$ denote the number of prime divisors of m. We make use of the following known identities

$$\sum_{d|m} |\mu(d)| = 2^{\nu}(m), \qquad \sum_{d|m} \frac{\mu(d)}{d} = \frac{\varphi(m)}{m},$$

see Sections 2.b and 4.b to Chapter 2 of [44], which yield the bound

$$N = \frac{2^r \varphi(p-1)}{2^{2k} p} + O(2^{\nu(p-1)} p^{1/2} \log^2 p).$$

From the following well known estimates

$$\frac{k}{\varphi(k)} = O\left(\log\log k\right), \qquad \nu(k) = O\left(\frac{\log k}{\log\log k}\right)$$

which holds for $k \geq 3$. Therefore,

$$N \geq 2^{r-2k+O(\log\log r)} - 2^{r/2+O(r/\log r)} > 0,$$

provided that p is large enough. □

As in Chapter 5 one may apply the result of Theorem 9.4 to obtain the lower bound $0.5\log p + O(1)$ on the CREW PRAM complexity of primitive root testing modulo p.

There are also some applications of the method of this work to constructing symmetric Boolean functions which cannot be approximated by polynomials of small degree; 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 [25, 37]) 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 $2^r - s$ values of $x \in \mathbb{F}_{2^r}$ then $f(x) = f(x^2)$ for at least $2^r - 2s$ points, thus $2\deg f \geq 2^r - 2s$ and $\deg f \geq 2^{r-1} - s$.

Chapter 10

Some Remarks, Generalizations and Open Questions

In this work we considered the discrete logarithm over prime fields only. This is because there is an obvious bijective mapping between the residue ring $\mathbb{Z}/(p-1)$ and the multiplicative group $\mathbb{F}_p^*$, sending x to $x+1$ for $x \in \{0, 1, \ldots, p-2\} = \mathbb{Z}/(p-1)$. For $\mathbb{Z}/(q-1)$ and $\mathbb{F}_q^*$, where $q = p^r$ is a prime power a similar map also exists [30] (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 work can be extended onto arbitrary finite fields $\mathbb{F}_q$.

One can see that Theorems 3.1, 3.2, 7.1 and 7.2 can easily be extended to rational functions (with somewhere stronger bounds than those following from more general Theorems 3.6, 3.7, 7.4 and 7.5).

We mention that using the same 'symmetrization' trick which is used in the proof of Theorem 8.2 one can replace $p^{1/2} \log p$ by $p^{1/2}$ in Theorems 3.4, 3.5, 4.1, 5.1 and 9.3 with slightly worse constants (the constants of this work are not the best possible anyway). We use it for Theorem 8.2 because it leads to the estimate of $\sigma(B)$ which is of cor-

rect order (obviously $\sigma(B) \le r$). In a very general form this trick is described in [5].

Moreover, using the improvements of the Weil bound from [23, 28] (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 [40].

Also, instead of Lemma 2.4 one could use a more general estimate of [34] of character sums with algebraic functions (including rational functions of course). That would allow to generalize Theorems 3.4 and 3.5 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, 3.5, 7.1 and 7.2. Moreover, Theorems 3.3 and 7.3 show that this bound is precise for almost all sets.

Question 10.1. Find examples of sets S for which the aforementioned trivial upper bound can be improved.

Unfortunately, a modulo $p-1$ 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.

Question 10.2. Obtain an explicit expression for a polynomial $f(X) \in \mathbb{Z}[X]$ of the smallest degree such that

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

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

Question 10.3. 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 $S \subseteq \{1, \dots, p-1\}$.

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 work but if M is composite some additional considerations are required. Indeed, although analogues of our auxiliary results (bounds for the number of zeros [21, 22], bounds of character sum [18, 39, 41] , 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

$$B(u_1, \dots, u_r) = \begin{cases} 0, & \text{if } \operatorname{ind} x \leq (p-3)/2, \\ 1, & \text{if } \operatorname{ind} x \geq (p-1)/2, \end{cases} \tag{10.1}$$

where $x = u_1 \dots u_r$ is the bit representation of x, $1 \leq x \leq 2^r - 1$, $r = \lfloor \log p \rfloor$. 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).

Question 10.4. Obtain a non-trivial lower bound on the degree of a Boolean function satisfying (10.1).

A randomized version of Theorem 5.1 would be of interest as well.

Question 10.5. Obtain a non-trivial lower bound on the degree of a Boolean function $B(U_1, \ldots, U_r, V_1, \ldots, V_s)$ such that for any x, $1 \le x \le 2^r - 1$,

$$B(u_1, \ldots, u_r, v_1, \ldots, v_s) \equiv \operatorname{ind} x \pmod 2,$$

where $x = u_1 \ldots u_r$ is the bit representation of x, $r = \lfloor \log p \rfloor$, for at least $\alpha 2^s$ binary vectors $(v_1, \ldots, v_s)$ with some constant $\alpha > 0.5$.

The most important case is apparently $s = r^{O(1)}$.

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

Question 10.6. Obtain analogues of Theorem 5.2 for branching and randomized Boolean circuits.

In this work we have arithmetic and Boolean circuits with bounded fan-in (that is, the number arguments each gate can accept). The same method enables us to consider circuits with unbounded fan-in with respect to addition (over $\mathbb{F}_q$ for arithmetic circuits and modulo 2 for Boolean circuits) and to get trade-off results between the size and the depth of such circuits. Such circuits are of interest and have been considered in the literature [8]. On the other hand, circuits with totally unbounded fan-in are, apparently, more difficult to study.

Question 10.7. Obtain analogues of Theorems 5.2 and 7.7 for circuits with unbounded fan-in.

One of the possible ways of doing that is using the Lemma 1 of [35] which claims that for any $l \ge 0$ the product $F = f_1 \ldots f_N$ of any number N of multilinear polynomials

$$f_i \in \mathbb{F}_2[U_1, \ldots, U_r]$$

of degree at most d there is a polynomial f of degree at most ld which disagree with F at at most 2^{r-l} points of $\mathbb{F}_2^r$. The only missing link

in answering Question 10.7 is obtaining a good generalization of the bound (5.2) to Boolean functions giving the rightmost bit of $\operatorname{ind} x$ for all but at most s values of $x = 1, \ldots, 2^r - 1$. Unfortunately the bounds (5.4) and (5.5) are not strong enough for that purpose. For example they get trivial if s is of order p.

We remark that in [42], for any positive α, probabilistic Boolean circuits with unbounded fan-in of depth

$$D = O(\log\log^{2\alpha+2} p + \log\log^3 p),$$

and of size

$$S = \exp\left(O\left(\frac{\log p}{\log\log^{\alpha} p}\right)\right)$$

are constructed for computing discrete logarithms modulo p.

Results of Chapter 6 are rather weak. Probably they can be improved in several particular cases.

Question 10.8. Improve Theorem 6.1 for above for reals polynomials $f(X) \in \mathbb{R}[X]$ reals satisfying the inequality

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

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

One can also consider more general than in Theorem 6.2 multivariate functions on bits of x.

Question 10.9. Obtain lower bounds on the degree of a rational function $f(X_1, \ldots, X_r) \in \mathbb{R}(X_1, \ldots, X_r)$ such that $f(u_1, \ldots, u_r) > 0$ if x is a quadratic residue modulo p and $f(u_1, \ldots, u_r) \le 0$ otherwise, where $x = u_1 \ldots u_r$ is the bit representation of x, $1 \le x \le 2^r - 1$, $r = \lfloor \log p \rfloor$.

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 shown 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 fulfill this program one needs to answer the following question.

Question 10.10. 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 well known [19, 24] and have already produced a large number of results on computational complexity of various classes of functions [14]. For example, using those bounds and the presented here method, one can easily obtain lower bound on the additive complexity of real polynomials $f(X) \in \mathbb{R}[X]$ or $F(X,Y) \in \mathbb{R}[X,Y]$ for which $\operatorname{ind} x = f(x)$ or $F(x, \operatorname{ind} x) = 0$, $x \in S$ for various sets $S \in \{0, \ldots, p-1\}$. 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.

Question 10.11. Extend Theorem 8.1 to the case of quadratic modulo p polynomials $f(X) \in \mathbb{Z}[X]$.

In particular, it would lead to a more direct treatment of the case of quadratic polynomials in Theorems 8.3 and 8.4 and to their possible improvements. We note that for the partial case $f(X) = X^2$ it is done in [38] (for the rightmost bit) but that method does not work for quadratic functions with 'large' leading coefficients.

The constants 0.6 and 1/16 in Theorem 8.2 are not the best possible ones but we still don't know how to get a nontrivial result for rational functions of degree of order greater than $r^{1/2}$.

Question 10.12. Extend Theorem 8.2 to the case of rational functions of larger degree, say of order $2^{\alpha r}$ with some $\alpha > 0$.

Such a result would immediate lead to an improvement of Theorem 8.3. In particular we believe that the result similar to that of Theorem 8.4 holds for general arithmetic circuits modulo p, not necessary division free ones. The main obstacle is obtaining a better version of Lemma 2.9.

Question 10.13. Extend Theorems 8.1 and 8.2 to the case of functions modulo an arbitrary integer M.

There are two classes of moduli M for which this question is especially interesting. The first one is the class of moduli of the form $M = 2^k$ which corresponds to the 'computer' arithmetic. The second one is the class of square-free moduli M having only small prime divisor (of order $\log^{O(1)} M$, say). The latter class is interesting because those moduli admit a very efficient parallel algorithms relying on the Chinese Reminder Theorem. Thus for such moduli there are good chances to match upper and lower bound of complexity of various functions. For example, in [13] this was done for the modular inversion.

Finally we mention that many of the results of this work can be generalized to the discrete logarithm and the Diffie–Hellman cryptosystem over elliptic curves.

Bibliography

[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] D. Boneh and R. Lipton, 'Algorithms for black-box fields and their applications to cryptography', *Lect. Notes in Comp. Sci.*, **1109** (1996), 283–297.

[3] D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secrete keys in Diffie–Hellman and related schemes', *Lect. Notes in Comp. Sci.*, **1109** (1996), 129–142.

[4] D. Boneh and R. Venkatesan, 'Rounding in lattices and its cryptographic applications *Preprint*, 1996, 1–9.

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

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

[7] G. S. Frandsen, M. Valence and D. A. M. Barrington, 'Some result on uniform arithmetic circuit complexity', *Math. System Theory*, **27** (1994), 105–124.

[8] A. Gál and A. Wigderson, 'Boolean complexity classes vs. their arithmetic analogues', *Electronic Colloq. on Comp. Compl.*, **TR95-049** (1995), 1–16.

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

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

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

[12] 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.

[13] J. von zur Gathen and I. E. Shparlinski, 'The CREW PRAM complexity of modular inversion', *Preprint*, 1996, 1–20.

[14] 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).

[15] D. Grigoriev, 'Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines', *Proc. Intern. Symp. on Algebraic and Comput.*, 1996, 49–54.

[16] J. Håstad, A. W. Schrift and A. Shair, 'The discrete logarithm modulo a composite hides $O(n)$ bits', *J. Computer and Syst. Science*, 471(1995), 376–404.

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

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

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

[20] J. F. Koksma, 'Some theorems on diophantine inequalities', *Math. Centrum Scriptum no. 5*, Amsterdam, 1950.

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

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

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

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

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

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

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

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

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

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

[31] V.I. Nečaev, 'Complexity of a deterministic algorithm for the discrete logarithm', *Matem. Zametki*, **55** (1994), no. 2, 91–101 (in Russian).

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

[33] I. Parberry and P. Yuan Yan, 'Improved upper and lower time bounds for parallel random access machines without simultaneous writes', *SIAM J. Comp.*, **20** (1991), 88–99.

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

[35] A. A. Razborov, 'Lower bounds on the size of bounded depth circuits over a complete basis with logical addition', *Matem. Zametki*, **41** (1987), 598–607 (in Russian).

[36] V. Shoup, 'Lower bounds for discrete logarithms and related problems', *Preprint*, 1996, 1–9.

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

[38] I. E. Shparlinski, 'The CREW PRAM complexity of the division-free arithmetic modulo an r bit prime p is $\Theta(\log r)$' *Preprint*, 1996, 1–9.

[39] 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).

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

[41] S. B. Stečkin , 'An estimates of a complete rational exponential sum', *Proc. Math. Inst. Acad. Sci. of the USSR*, Moscow, **143** (1989), 188–207 (in Russian).

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

[43] P. Szüsz, 'On a problem in the theory of uniform distribution', *Comp. Rend. Premier Congrès Hongrois*, Budapest, 1952, 461–472 (in Hungarian).

[44] I. M. Vinogradov, *Elements of number theory*, Dover Publ., NY, 1954.

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

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