Electronic Colloquium on Computational Complexity, Report No. 56 (1998)

Circuit Complexity of Testing Square-Free Numbers

ANNA BERNASCONI and IGOR SHPARLINSKI

Institut für Informatik, Technische Universität München
D-80290 München, Germany
bernasco@informatik.tu-muenchen.de

and

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

Abstract

In this paper we extend the area of applications of the Abstract Harmonic Analysis to the field of Boolean function complexity. In particular, we extend the class of functions to which a spectral technique developed in a series of works of the first author can be applied. This extension allows us to prove that testing square-free numbers by unbounded fan-in circuits of bounded depth requires a superpolynomial size. This implies the same estimate for the integer factorization problem.

1 Introduction

In recent years spectral techniques based on the Abstract Harmonic Analysis on the hypercube have been shown to represent a very useful tool for obtaining lower complexity bounds. Various links between Fourier coefficients of

ISSN 1433-8092

Boolean functions and their complexity characteristics have been studied in a number of works, see [1, 2, 3, 4, 5, 6, 10, 16, 17, 19, 20]. In particular, these spectral techniques have been successfully applied to the parity function and to threshold functions.

However, a limitation of such approach to the study of Boolean function complexity is that, besides the results for parity and threshold functions, spectral methods have provided lower bounds for specially constructed Boolean functions, which are not related to any particular number theoretic or combinatorial problem. In fact, there are very few known examples of functions coming from natural combinatorial or number theoretic problems for which the spectral techniques have produced non-trivial results. The only examples we are aware of are the lower bounds on integer multiplication [6] and on the complexity of computing the discrete logarithm [7, 21]. There are also some very interesting results about determinants [11, 12].

In this paper we pursue two purposes:

- extend the area of applications of the spectral techniques to the study of Boolean function complexity;
- obtain the first non-trivial lower bound on the circuit complexity of testing square-free numbers.

To this aim, we first provide a generalization of the spectral technique developed in [1, 2] for getting lower bounds on the size complexity of Boolean functions computed by constant-depth circuits.

We then apply the generalized technique to evaluate the complexity of the Boolean function which decides whether a given $(n+1)$-bit odd integer is square-free, that is the function for which

$$f(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } 2x+1 \text{ is square-free,} \\ 0, & \text{if } 2x+1 \text{ is square-full,} \end{cases} \tag{1}$$

where $2x+1 = x_1 \ldots x_n 1$ is the bit representation of $2x+1$, $0 \le x \le 2^n - 1$ (if necessary we add several leading zeros).

More precisely, we provide an estimate the Fourier coefficients of (1) and derive a complexity lower bound showing that this function does not belong to the complexity class $\mathbf{AC}^o$.

In [7, 21], some lower bounds are obtained for the function deciding if a given integer x is a quadratic residues modulo p. Here we show that some of the techniques used in [7, 21] can be applied to the function (1). This approach is based on the uniformity of distribution of square-free numbers with some fixed binary digits. For the quadratic residuacity a similar property has been established by using the very powerful Weil estimate. Here we use a sieve method.

Notice that our estimate compliments the results of [22] on polynomial representations of the Boolean function deciding whether a given integer x is square-free. Moreover, it provides the first non-trivial lower bound on the circuit complexity of a number theoretic problem which is closely related to the integer factorization problem. We finally remark that testing square-free numbers is the only known problem, related to the integer factorization problem, for which an unconditional deterministic polynomial time algorithm is known, see [15].

2 Basic Definitions

First of all, we provide some of the notation we use.

Let $\mathfrak{B}_n = \{0,1\}^n$ denote the n dimensional Boolean cube.

We will use the notation $|f|$ to denote the number of strings accepted by the function f, that is $|f| = |\{w \in \mathfrak{B}_n \mid f(w) = 1\}|$. Moreover, p_f denotes the probability that the function f takes the value 1 (over the uniform distribution), that is $p_f = |f|/2^n$.

Given a binary string $w \in \mathfrak{B}_n$, we denote with $|w|$ the number of ones in w, which is sometimes called the **cardinality** of the string because of the correspondence between sets of positive integers and strings over the alphabet $\{0,1\}$.

We now review some basic definitions.

An **unbounded fan-in Boolean circuit** $\mathcal{C}$ with input variables $x_1, \ldots, x_n$, consists of several levels of *AND*, *OR* and *NOT* gates. The gates at the bottom level accept values from the input variables $x_1, \ldots, x_n$. Each of the other gates may accept output values from any number of gates of the previous levels. The only top level gate contains the output $\mathcal{C}(x_1, \ldots, x_n)$. For a more detailed description, see [6, 17, 20].

The number of levels is called the **depth** of the circuit, the number of gates is called the **size**.

The class of **AC^o circuits** consists of circuits whose size is bounded by a polynomial in n, and whose depth is bounded by a constant.

A **restriction** ρ is a mapping of the set of the subscripts of input variables $x_1, \ldots, x_n$ to the set $\{0, 1, \star\}$, where

- $\rho(i) = 0$ means that we substitute the value 0 for x_i;
- $\rho(i) = 1$ means that we substitute the value 1 for x_i;
- $\rho(i) = \star$ means that x_i remains a variable.

Given a function f depending on n binary variables, we will denote by f_ρ the function obtained from f by applying the restriction ρ; f_ρ will be a function of the variables x_i for which $\rho(x_i) = \star$, $1 \leq i \leq n$.

The subscripts i and the corresponding variables x_i are called **fixed** if $\rho(i) = 0, 1$, and **free** if $\rho(i) = \star$.

We recall that an integer x is called **square-free** if there is no prime p such that $p^2 | x$. Otherwise x is called **square-full**.

Throughout the paper we denote by $\log x$ the binary logarithm of x.

3 Abstract Harmonic Analysis and Circuits

We give some background on abstract harmonic analysis on the hypercube. We refer to [17, 20] for a more detailed exposition.

We consider the space $\mathcal{F}$ of all the two-valued functions on $\mathfrak{B}_n$. The domain of $\mathcal{F}$ is a locally compact Abelian group and the elements of its range, that is 0 and 1, can be added and multiplied as complex numbers. The above properties allow one to analyze $\mathcal{F}$ by using tools from harmonic analysis. This means that it is possible to construct an orthogonal basis set of Fourier transform kernel functions for $\mathcal{F}$. The kernel functions of the Fourier transform are defined in terms of a group homomorphism from $\mathfrak{B}_n$ to the direct product of n copies of the multiplicative subgroup $\{\pm 1\}$ on the unit circle of the complex plane. The functions $Q_w(x) = (-1)^{w_1 x_1}(-1)^{w_2 x_2} \ldots (-1)^{w_n x_n} = (-1)^{w^T x}$ are known as **Fourier transform kernel functions**, and the set $\{Q_w \mid w \in \mathfrak{B}_n\}$ is an orthogonal basis for $\mathcal{F}$.

We can now define the **Abstract Fourier Transform** of a Boolean function f as the rational valued function f^* which defines the coordinates of f with respect to the basis $\{Q_w(x) \mid w \in \mathfrak{B}_n\}$, that is

$$f^*(w) = 2^{-n} \sum_{x \in \mathfrak{B}_n} Q_w(x) f(x) = 2^{-n} \sum_{x \in \mathfrak{B}_n} (-1)^{w^T x} f(x) .$$

Then

$$f(x) = \sum_{w \in \mathfrak{B}_n} Q_w(x) f^*(w) = \sum_{w \in \mathfrak{B}_n} (-1)^{w^T x} f^*(w)$$

is the **Fourier expansion** of f.

It is interesting to note that the zero-order Fourier coefficient, that is the coefficient related to the all zeros string, is equal to the probability that the function takes the value 1, while the other Fourier coefficients measure the correlation between the function and the parity of subsets of its input bits (see [16] for more details).

As a consequence of the orthogonality of the functions Q_w, it is also possible to derive a very useful identity, the **Parseval identity:**

$$\sum_{v \in \mathfrak{B}_n} (f^*(v))^2 = 2^{-n} \sum_{v \in \mathfrak{B}_n} f(v) = f_0^* \,, \tag{2}$$

where f_0^* denotes the zero-order Fourier coefficient.

We finally present an interesting application of harmonic analysis to circuit complexity which is due to [16].

Lemma 1. *Let f be a Boolean function on n variables computable by a Boolean circuit of depth d and size M, and let ϑ be any integer. Then*

$$\sum_{|w|>\vartheta} (f^*(w))^2 \leq \frac{1}{2} M \, 2^{-\frac{\vartheta^{1/d}}{20}} \,,$$

where the sum is taken over all strings $w \in \mathfrak{B}_n$ of cardinality $|w| > \vartheta$. □

4 A Technique to Prove Lower Bounds on the Size/Depth of Circuits

In [1] and [2] a new technique has been developed with the aim of proving lower bounds on the size-complexity of Boolean functions presenting a rather strong combinatorial structure. This technique is based both on the abstract harmonic analysis on the hypercube, and on the spectral characterization of the size-depth trade-off of Boolean circuits which has been given in Lemma 1.

Let $f : \mathfrak{B}_n \to \{0,1\}$ be a Boolean function depending on n variables and let p_f denote the probability, over the uniform distribution, that the function takes the value 1, that is $p_f = |f|/2^n$. Now, let k, $1 \leq k \leq n$, be the smallest integer such that f has the following property: for any subfunction f_ρ depending on k variables, $p_{f_\rho} = p_f$, where $p_{f_\rho} = |f_\rho|/2^k$. In this case, we say that the function f is **of level** k (see [2] for more details).

Then, if f is computable by a circuit of constant depth d and size M, it is possible to derive a lower bound on the size M of such a circuit, which depends both on the probability p_f and on the level k:

$$M \geq (p_f - p_f^2) \, 2^{0.05(n-k)^{1/d}+1} \,.$$

Notice that this result can be viewed as a generalization of the exponential lower bound for the size of constant depth circuits computing the parity function [6, 10]. Indeed, parity and its complement are the only two non-constant Boolean functions of level 1 [1].

The above lower bound can be proved by combining Lemma 1 with some results of [2].

The paper [2] also gives a complete characterization of functions of level k. A Boolean function $f : \mathfrak{B}_n \to \{0,1\}$ is of level k if and only if $f_0^* = p_f$ and $f^*(w) = 0$ for any string w such that $0 < |w| \leq n - k$.

We now show how the above technique can be generalized in order to be applied also to functions which present such combinatorial structure only in an "approximate sense".

A Boolean function $f : \{0.1\}^n \to \{0,1\}$ is called **δ-approximately of level k** if

$$|p_{f_\rho} - p_f| \leq \delta$$

for any subfunction f_ρ depending on at least k variables.

In the following theorem we derive a spectral characterization of functions δ-approximately of level k.

Theorem 2. *Let $f : \mathfrak{B}_n \to \{0,1\}$ be δ-approximately of level k. Then,*

$$|f^*(w)| \leq \delta$$

for any string w such that $0 < |w| \leq n - k$.

Proof. Let $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ be a Boolean string such that $0 < |\mu| = n - \ell \leq n - k$. Moreover, let $\mathcal{I} = \{i \mid \mu_i = 1\}$.

For any string $u \in \{0,1\}^{n-\ell}$, let $f_{\rho_{\mu,u}}$ denote the subfunction defined by the restriction $\rho_{\mu,u}$ that assigns to the variables x_i such that $i \in \mathcal{I}$, the $(n-\ell)$ values taken from the string u, and leaves free the other ℓ variables. Then, we have

$$\begin{aligned} f^*(\mu) &= \frac{1}{2^n} \sum_{w \in \mathfrak{B}_n} (-1)^{\mu^T w} f(w) = \frac{1}{2^n} \sum_{w \in \mathfrak{B}_n} (-1)^{\sum_{i \in \mathcal{I}} w_i} f(w) \\ &= \frac{1}{2^n} \sum_{u \in \mathfrak{B}_{n-\ell}} (-1)^{|u|} \sum_{v \in \mathfrak{B}_\ell} f_{\rho_{\mu,u}}(v) = \frac{1}{2^n} \sum_{u \in \mathfrak{B}_{n-\ell}} (-1)^{|u|} \, |f_{\rho_{\mu,u}}| \,. \end{aligned}$$

For any $u \in \mathfrak{B}_{n-\ell}$, the subfunction $f_{\rho_{\mu,u}}$ depends on $\ell \geq k$ variables and, since f is δ-approximately of level k, we have

$$\left| |f_{\rho_{\mu,u}}| - 2^\ell p_f \right| \leq 2^\ell \delta.$$

Thus, we get

$$\begin{aligned}|f^*(\mu)| &= \frac{1}{2^n}\left|2^\ell p_f \sum_{u\in\mathfrak{B}_{n-\ell}} (-1)^{|u|} + \sum_{u\in\mathfrak{B}_{n-\ell}} (-1)^{|u|}\left(|f_{\rho_{\mu,u}}| - 2^\ell p_f\right)\right| \\ &= \frac{1}{2^{n-\ell}}\left|\sum_{u\in\mathfrak{B}_{n-\ell}} (-1)^{|u|}\left(p_{f_{\rho_{\mu,u}}} - p_f\right)\right| \le \frac{1}{2^{n-\ell}} \sum_{u\in\mathfrak{B}_{n-\ell}} \delta\,,\end{aligned}$$

and the result immediately follows. □

We are now able to state and prove a theorem which provides a lower bound on the size required by a depth d circuit to compute functions which are δ-approximately of level k.

Theorem 3. *Let $f : \mathfrak{B}_n \to \{0,1\}$ be a function δ-approximately of level k. If f is computable by a circuit of constant depth d and size M, then*

$$M \ge 2^{0.05(n-k)^{1/d}+1}\left(p_f - p_f^2 - \delta^2 2^{(n-k)\log n}\right).$$

Proof. An application of Lemma 1 yields the following inequality:

$$M \ge 2^{0.05\vartheta^{1/d}+1} \sum_{|w|>\vartheta} (f^*(w))^2\,.$$

Let us choose $\vartheta = n-k$. Then, by using the Parseval identity (2) we obtain

$$\begin{aligned}\sum_{|w|>n-k} (f^*(w))^2 &= \sum_{w\in\mathfrak{B}_n} (f^*(w))^2 - (f_0^*)^2 - \sum_{1\le|w|\le n-k} (f^*(w))^2 \\ &= p_f - p_f^2 - \sum_{1\le|w|\le n-k} (f^*(w))^2\,,\end{aligned}$$

where, as before, f_0^* denotes the zero-order Fourier coefficient.

We are now left with the evaluation of the sum of the squares of the Fourier coefficients of order less or equal to our threshold $n-k$. From Theorem 2 it follows that

$$\sum_{1\le|w|\le n-k}^{n-k} (f^*(w))^2 \le \delta^2 \sum_{j=1}^{n-k}\binom{n}{j} \le \delta^2\, 2^{(n-k)\log n}\,,$$

where we have applied the inequality

$$\sum_{j=1}^{\ell}\binom{n}{j} \le n^\ell\,.$$

Therefore, we obtain

$$\sum_{|w|>n-k} (f^*(w))^2 \ge p_f - p_f^2 - \delta^2\, 2^{(n-k)\log n}$$

and the result follows. □

Note that such a lower bound turns out to be meaningful provided that

$$\delta^2 \, 2^{(n-k)\log n} = o(p_f) \, .$$

5 Circuit Complexity of Testing Square-Free Numbers

First of all we need a result about the uniformity of distribution of odd square-free numbers with some fixed binary digits.

Let ρ be a restriction on the set $\{1, \dots, n\}$. We denote by $\mathcal{N}_\rho(n)$ the set of integers x, $0 \le x \le 2^n - 1$ such that $x_i = \rho(i)$ for all fixed subscripts $i \in \{1, \dots, n\}$, where $x_1 \dots x_n 1$ is the binary expansion of $2x+1$. We also denote by $S_\rho(n)$ the number of $x \in \mathcal{N}_\rho(n)$ for which $2x+1$ is square free.

Lemma 4. *For any restriction ρ with $r \le n^{1/2}/3 - 1$ fixed positions,*

$$S_\rho(n) = \frac{8}{\pi^2} 2^{n-r} + O(2^{n-r-n/3(r+1)}).$$

Proof. Let $T_\rho(n,m)$ be the number of $x \in \mathcal{N}_\rho(n)$ with $m^2 | 2x+1$. From the inclusion-exclusion principle it follows that

$$S_\rho(n) = \sum_{\substack{1 \le m \le 2^{(n+1)/2} \\ m \equiv 1 \pmod 2}} \mu(m) T_\rho(n,m) \, ,$$

where $\mu(m)$ is the Möbius function. We recall that $\mu(1) = 1$, $\mu(m) = 0$ if m is square-full and $\mu(m) = (-1)^{\nu(m)}$ otherwise, where $\nu(m)$ is the number of prime divisors of $m \ge 2$.

Let t be the length of the largest substring of free positions. It is obvious that the elements of $\mathcal{N}_\rho(n)$ can be separated into 2^{n-r-t} groups such that in each group the numbers are of the form $2^s z + a$, $0 \le z \le 2^t - 1$, for some integers s and a.

For an odd integer $m \ge 1$, each such group contains $2^t/m^2 + O(1)$ numbers which are congruent to zero modulo m^2. Taking into account that $t \ge n/(k+1)$, we then obtain

$$T_\rho(n,m) = 2^{n-r}/m^2 + O(2^{n-r-n/(r+1)}).$$

Put $K = 2^{2n/3(r+1)}$. Applying the above asymptotic formula for $m \le K$ and the trivial bound

$$T_\rho(n,m) \le 2^n/m^2 + 1$$

for $m \geq K$, we obtain

$$S_\rho(n) = \sum_{\substack{1 \leq m \leq K \\ m \equiv 1 \pmod 2}} \mu(m) \left(\frac{2^{n-r}}{m^2} + O(2^{n-r-n/(r+1)}) \right) + O\left(\sum_{\substack{K < m \leq 2^{(n+1)/2} \\ m \equiv 1 \pmod 2}} \frac{2^n}{m^2} \right).$$

We also have

$$\sum_{\substack{1 \leq m \leq K \\ m \equiv 1 \pmod 2}} \frac{\mu(m)}{m^2} = \sum_{m \equiv 1 \pmod 2} \frac{\mu(m)}{m^2} + O(K^{-1}).$$

From Theorem 237 of [14] we derive

$$\begin{aligned} \sum_{m \equiv 1 \pmod 2} \frac{\mu(m)}{m^2} &= \sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} - \sum_{m \equiv 0 \pmod 2} \frac{\mu(m)}{m^2} \\ &= \frac{3}{4} \sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} = \frac{3}{4} \zeta(2)^{-1} = \frac{8}{\pi^2}. \end{aligned}$$

Therefore,

$$S_\rho(n) = \frac{8}{\pi^2} 2^{n-r} + O(K\, 2^{n-r-n/(r+1)} + 2^n/K)\,.$$

Finally, since for $r \leq n^{1/2}/3 - 1$ the first term in the 'O'-symbol dominates, the result follows. □

At this point we are able to derive our main result, namely a lower bound on the size complexity of testing square-free numbers.

Theorem 5. *Assume that the Boolean function f given by (1) is computed by an unbounded fan-in Boolean circuit $\mathcal{C}$ of depth d and of size M. Then, for sufficiently large n,*

$$d \log\log M \geq 0.5 \log n + O(\log\log n).$$

Proof. Put $k = n - \left\lfloor n^{1/2} \log^{-2} n \right\rfloor - 1$. It follows from Lemma 4 that, for sufficiently large n, f is δ-approximately of level k with $p_f = 8/\pi^2$ and $\delta = \exp(-Cn^{1/2} \log^2 n)$, where $C > 0$ is some absolute constant. Applying Theorem 3 we derive the desired statement. □

In particular, if the depth d is a constant, then the size turns out to be superpolynomial $M \geq \exp(cn^\gamma)$, for some constants $c > 0$ and $\gamma > 0$. In particular, this means that testing square-free numbers, and thus integer factorization, cannot be done by a circuit of the class $\mathbf{AC}^o$.

Apparently the result of Lemma 4 can be improved by means of some more sophisticated sieve methods (see for instance [13]). However this would not improve our main result.

6 Concluding Remarks

It would be very interesting to obtain analogous results for other Boolean functions related to number theoretic problems, for example for Boolean functions deciding primality or the parity of the number of prime divisors of the input x. Unfortunately, sieve techniques even more advanced than those used in Lemma 4 are still not powerful enough to produce such results, even under the assumption of the Extended Riemann Hypothesis.

We also remark that that some elementary number theoretic considerations have been used in [22] to obtain a very tight lower bound on the sensitivity of the function which decides whether its input x is a square-free integer.

Recall that the **sensitivity**, $\sigma(f)$, of a Boolean function $f : \mathfrak{B}_n \to \{0,1\}$ (which is also known as the *critical complexity*) is defined as the largest integer $s \le n$ such that there is a binary vector $x \in \mathfrak{B}_n$ for which $f(x) \neq f(x^{(i)})$ for s values of i, $1 \le i \le n$, where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate,

$$\sigma(f) = \max_{x\in\mathfrak{B}_n} \sum_{i=1}^{n} \left| f(x) - f(x^{(i)}) \right| .$$

In other words, $\sigma(f)$ is the maximum, over all binary vectors $x \in \mathfrak{B}_n$, of the number of vectors $y \in \mathfrak{B}_n$ on the unit *Hamming sphere* around x with $f(y) \neq f(x)$. In [22] it has been shown that for the function

$$g(x) = \begin{cases} 1, & \text{if } x \text{ is square-free,} \\ 0, & \text{if } x \text{ is square-full,} \end{cases}$$

the bound $\sigma(g) \ge \lfloor n/60 \rfloor$ holds.

This parameter is of interest because it can be used to obtain lower bounds for the CREW PRAM complexity of a Boolean function f (see [8, 9, 18, 23]), that is the complexity on a *parallel random access machine* with an unlimited number of all-powerful processors, such that simultaneous reads of a single memory cell by several processors are permitted, but simultaneous writes are not. In particular, from the above bound on $\sigma(g)$ one immediately concludes that the CREW PRAM complexity of g is at least $0.5\log n + O(1)$, see [18].

It is also known that the **average sensitivity**

$$\sigma_{av}(f) = 2^{-n} \sum_{x\in\mathfrak{B}_n} \sum_{i=1}^{n} \left| f(x) - f(x^{(i)}) \right|$$

can be expressed via the Fourier coefficients of f, see [1, 4, 5]. Applying our results, one can derive the estimate $\sigma_{av}(f) \ge c n^{1/2} \log^{-2} n$ for the function

f given by (1), where $c > 0$ is an absolute constant. It would be interesting to obtain a linear lower bound on the average sensitivity of f and g.

There are also close relations between the Fourier coefficients and the formula size of a Boolean function, see [4], and we hope that our methods will apply to this complexity characteristic as well.

References

[1] A. Bernasconi, 'On the complexity of balanced Boolean functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1203** (1997), 253–263.

[2] A. Bernasconi, 'Combinatorial properties of classes of functions hard to compute in constant depth', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1449** (1998), 339–348.

[3] A. Bernasconi and B. Codenotti, 'Measures of Boolean function complexity based on harmonic analysis', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **778** (1994), 63–72.

[4] A. Bernasconi, B. Codenotti and J. Simon, 'On the Fourier analysis of Boolean functions', *Preprint* (1996), 1–24.

[5] R. B. Boppana, 'The average sensitivity of bounded-depth circuits', *Inform. Proc. Letters*, **63** (1997), 257–261.

[6] R. B. Boppana and M. Sipser, 'The complexity of finite functions', *Handbook of Theoretical Comp. Sci., Vol. A*, Elsevier, Amsterdam (1990), 757–804.

[7] D. Coppersmith and I. E. Shparlinski, 'On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping', *J. Cryptology* (to appear).

[8] M. Dietzfelbinger, M. Kutyłowski and R. Reischuk, 'Feasible time-optimal algorithms for Boolean functions on exclusive-write parallel random access machine', *SIAM J. Comp.*, **25** (1996), 1196–1230.

[9] F. E. Fich, 'The complexity of computation on the parallel random access machine', *Handbook of Theoretical Comp. Sci., Vol. A*, Elsevier, Amsterdam (1990), 757–804.

[10] M. Goldmann, 'Communication complexity and lower bounds for simulating threshold circuits', *Theoretical Advances in Neural Computing and Learning*, Kluwer Acad. Publ., Dordrecht (1994), 85–125.

[11] D. Grigoriev and M. Karpinski, 'An exponential lower bound for depths 3 arithmetic circuits' *Proc. 30 ACM Symp. on Theory of Comp.* (1998), 577–582.

[12] D. Grigoriev and A. Razborov, 'Exponential lower bounds for depths 3 arithmetic circuits in algebras of functions over finite fields' *Proc. 39 IEEE Symp. on Found. of Comp. Sci.*, 1998 (to appear).

[13] D. R. Heath-Brown, 'The least square-free number in an arithmetic progression', *J. Reine Angew. Math.*, **332** (1982), 204–220.

[14] G. H. Hardy and E. M. Wright, *An introduction to the number theory*, Oxford Univ. Press, Oxford (1965).

[15] H. W. Lenstra, 'Miller's primality test', *Inform. Proc. Letters*, **8** (1979), 86–88.

[16] N. Linial, Y. Mansour and N. Nisan, 'Constant depth circuits, Fourier transform, and learnability', *Journal of the ACM*, **40** (1993), 607-620.

[17] Y. Mansour, 'Learning Boolean functions via the Fourier transform', *Theoretical Advances in Neural Computing and Learning*, Kluwer Acad. Publ., Dordrecht (1994), 391–424.

[18] 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.

[19] R. Raz, 'Fourier analysis for probabilistic communication complexity', *Comp. Compl.*, **5** (1995), 205–221.

[20] V. Roychowdhry, K.-Y. Siu and A. Orlitsky, 'Neural models and spectral methods', *Theoretical Advances in Neural Computing and Learning*, Kluwer Acad. Publ., Dordrecht (1994), 3–36.

[21] I. E. Shparlinski, *Number-theoretic methods in lower nounds of the complexity of the discrete logarithm and related problems*, Birkhäuser, to appear.

[22] I. Shparlinski, 'On polynomial representations of Boolean functions related to some number theoretic problems', *Tech. Report C/TR 98-07*, Macquarie Univ., Sydney (1998), 1–13.

[23] I. Wegener, *The complexity of Boolean functions*, Wiley-Teubner Series in Comp. Sci., Stuttgart (1987).