Electronic Colloquium on Computational Complexity, Report No. 54 (1998)

On Polynomial Representations of Boolean Functions Related to Some Number Theoretic Problems

Igor Shparlinski

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

Abstract

Lower bounds are obtained on the degree and the number of monomials of Boolean functions, considered as a polynomial over $\mathbb{F}_2$, which decide if a given r-bit integer is square-free. Similar lower bounds are also obtained for polynomials over the reals which provide a threshold representation of the above Boolean functions. These results provide first non-trivial lower bounds on the complexity of a number theoretic problem which is closely related to the integer factorization problem.

1 Introduction

In this paper we obtain lower bounds on the degree and the number of monomials of Boolean functions, considered as a polynomial over $\mathbb{F}_2$, which decide if a given r-bit integer is square-free. Similar lower bounds are also obtained for polynomials over the reals which provide a threshold representation of the above Boolean functions. These results are somewhat similar to lower bounds for the Boolean function deciding is a given integer x is a quadratic residue modulo a prime p which are obtained in [5, 25]. However, instead of

ISSN 1433-8092

the very strong Weil bound, which is the main tool of [5, 25], in this paper we use a sieve method and some classical results about distribution of prime numbers. Accordingly, our results are weaker that those of [5, 25]. Nevertheless they provide first non-trivial lower bounds on the complexity of a number theoretic problem which is closely related to the integer factorization problem.

We also show that some simple number theoretic observations allow us to obtain quite strong lower bounds on several other complexity characteristics of testing if a given integer is square-free.

We remark that testing if a given number is square-free is the only known problem, related to the integer factorization problem, for which an unconditional deterministic polynomials time algorithm is known, see [14].

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*. We define the function

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

For a given integer $r \geq 1$, we can identify x, $0 \leq x \leq 2^r - 1$, and its bit representation $x_1 \ldots x_r$ (if necessary we add several leading zeros) and consider $S(x)$ as a Boolean function of r variables.

We study Boolean functions deciding if a given r-bit integer is square-free, that is Boolean functions for which

$$B(x_1, \ldots, x_r) = S(x), \tag{1}$$

where $x = x_1 \ldots x_r$ is the bit representation of x, $1 \leq x \leq 2^r - 1$.

Each Boolean function $B(X_1, \ldots, X_r)$ can be represented by a multilinear polynomial over $\mathbb{F}_2$ of the form

$$B(X_1, \ldots, X_r) = \sum_{k=0}^{n} \sum_{1 \leq i_1 < \ldots < i_k \leq r} A_{i_1 \ldots i_k} X_{i_1} \ldots X_{i_k}, \tag{2}$$

where

$$A_{i_1 \ldots i_k} \in \mathbb{F}_2, \qquad 1 \leq i_1 < \ldots < i_k \leq r.$$

The minimal value of n in the representation (2) we call the *degree* of B and write $\deg B$. The number of non-zero coefficients $A_{i_1 \ldots i_k}$ we call the *sparsity* of B and write $\operatorname{spr} B$.

In this paper, we obtain lower bounds on the degree $\deg B$ and the sparsity $\operatorname{spr} B$ of Boolean functions, satisfying (1).

We note that the degree of B in the basis $\{+, \times\}$, which is has just been defined, is the same as the degree in the more common basis $\{\vee, \wedge, \neg\}$,

however it does not apply to the sparsity. Unfortunately it is not clear how to adjust our method to obtaining lower bounds on the sparsity of B in the basis $\{\vee, \wedge, \neg\}$.

Similarly to the case of Boolean functions, for a polynomial f in r variables over the reals we define the degree $\deg f$ as the largest sum $i_1 + \ldots + i_r$ and the sparsity $\operatorname{spr} f$ as the number of coefficients $A_{i_1 \ldots i_k}$ in the representation

$$f(X_1, \ldots, X_r) = \sum_{i_1, \ldots, i_r} A_{i_1, \ldots, i_r} X_1^{i_1} \ldots X_r^{i_r}, \qquad A_{i_1, \ldots, i_r} \neq 0.$$

For a real w we define the sign-function as

$$\operatorname{sign} w = \begin{cases} 1, & \text{if } w \geq 0, \\ 0, & \text{if } w < 0. \end{cases}$$

Here we also obtain lower bounds on the degree $\deg f$ and sparsity $\operatorname{spr} f$ of polynomials f providing a *threshold* representation of $S(x)$ for r-bit integers x, that is a representation of the form

$$\operatorname{sign} f(x_1, \ldots, x_r) = S(x),$$

where $x = x_1 \ldots x_r$ is the bit representation of x, $1 \leq x \leq 2^r - 1$.

Furthermore, in the case of real polynomials, the Boolean values 0 and 1 can be interpreted as two arbitrary real values α_0 and α_1, not necessarily $\alpha_0 = 0$, $\alpha_1 = 1$. It is easy to see that the degree of the corresponding polynomials does not depend on the particular choice of α_0, α_1 because they are equivalent under a linear transformation of variables [13]. But it is shown in [13] that the sparsity $\operatorname{spr} f$, depends on the choice of α_0 and α_1. In fact, there are examples of Boolean functions, demonstrating that for $(\alpha_0, \alpha_1) = (0, 1)$ and $(\alpha_0, \alpha_1) = (1, -1)$ the gap between the numbers of monomials of the corresponding polynomials for these two representations can be exponentially large [13].

Threshold representations of Boolean functions via real polynomials have been studied in a number of works [1, 2, 9, 13, 19, 24]. These papers contain many general estimates together with lower bounds for some particular Boolean functions. However these Boolean functions are usually a specially constructed examples which are not related to any particular number theoretic or combinatorial problem.

In [5, 25], some lower bounds are obtained for the Boolean function deciding the quadratic residuacity of x. Here we show that some of the used in [5, 25] techniques can be applied to the function $S(x)$. This approach is based on the uniformity of distribution of long patters or $0, 1$ in the values of $S(x)$.

For the quadratic residuacity a similar property has been established by using the very powerful Weil estimate. Here we use a sieve method.

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

2 Auxiliary Results

Let $\mathcal{P}$ denote the set of primes.

We use the following well known asymptotic formulas (see [21] for example)

$$\ln\left(\prod_{\substack{p\le x\\ p\in\mathcal{P}}} p\right) \sim x, \qquad x\to\infty. \tag{3}$$

and

$$\pi(x) \sim \frac{x}{\ln x}, \qquad x\to\infty, \tag{4}$$

for the number of primes $p \le x$. The following estimate can be found in [15], Section 10.11.

Lemma 1. *For any integers M and N with $0 \le M < N/2$ the bound*

$$\sum_{K=0}^{M} \binom{N}{K} \le 2^{H(M/N)N}$$

holds, where

$$H(\gamma) = -\gamma\log\gamma - (1-\gamma)\log(1-\gamma), \qquad 0<\gamma<1,$$

is the binary entropy function.

Now we prove the following quite technical statement.

Lemma 2. *Let $m \ge 1$ be an integer and let us define k from the inequalities*

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

Let $m < p_1 < \ldots < p_m$ be the first m primes which are greater than m. Then for any m-dimensional binary vector $(\sigma_1,\ldots,\sigma_m)$ there exists an integer y such that

$$0 \le y \le \exp\left(4m\ln m + O(m)\right)$$

and

$$S(2^k y + p_i) = \sigma_i, \qquad i = 1,\ldots,m.$$

Proof. Put

$$Q = \prod_{\substack{p \le m \\ p \in \mathcal{P}}} p \qquad \text{and} \qquad M = 2^k Q.$$

From (3) we see that $Q = \exp(O(m))$. Thus it is enough to show that there exists an integer u such that

$$0 \le u \le \exp(4m \ln m + O(m))$$

and

$$S(Mu + p_i) = \sigma_i, \qquad i = 1, \dots, m. \tag{5}$$

We remark that $\gcd(p_i, M) = 1$, $i = 1, \dots, m$.

Let $\mathcal{I}$ be the set of subscripts i for which $\sigma_i = 0$ and let $\mathcal{J}$ be the set of subscripts j for which $\sigma_j = 1$. Put

$$q = \prod_{i \in \mathcal{I}} p_i^2.$$

From the Chinese Remainder Theorem we conclude that there exists an integer a, $0 \le a \le q - 1$, such that

$$Ma \equiv -p_i \pmod{p_i^2}, \qquad i \in \mathcal{I}.$$

Therefore

$$M(qz + a) + p_i \equiv 0 \pmod{p_i^2}, \qquad i \in \mathcal{I},$$

for any integer z. Now we show that one can select not too large z for which

$$S(M(qz + a) + p_j) = 1, \qquad j \in \mathcal{J}.$$

For $Z \ge 1$, we denote by $L_j(Z)$ the number of square-full numbers of the form $M(qz + a) + p_j$ with $1 \le z \le Z$, $j \in \mathcal{J}$. To prove the lemma it is sufficient to show that

$$\sum_{j \in \mathcal{J}} L_j(Z) < Z. \tag{6}$$

First of all we remark that, for $i \in \mathcal{I}$ and $j \in \mathcal{J}$,

$$M(qz + a) + p_j \not\equiv 0 \pmod{p_i^2}.$$

Indeed, otherwise we have $p_i^2 | (p_j - p_i)$ which is impossible.

For any prime $p \in \mathcal{P}$ with $\gcd(p, q) = 1$ the congruence

$$M(qz + a) + p_j \equiv 0 \pmod{p^2}, \qquad 1 \le z \le Z,$$

has at most $Z/p^2 + 1$ solutions. Obviously, it does not have solutions for $p^2 > Mq(Z + 1) + M$. Put $V = (3MqZ)^{1/2}$.

The smallest prime divisor of any number $M(qz+a)+p_j$ exceeds m. Therefore,

$$L_j(Z) \le \sum_{\substack{m \le p \le V \\ \gcd(p,q)=1}} \left(\frac{Z}{p^2}+1\right) = O\left(\frac{Z}{m \ln m} + \frac{V}{\ln V}\right).$$

Putting $Z = m^2 Mq$ we obtain the inequality (6), provided that m is large enough. Therefore, there exists y satisfying the condition (5) and such that $u \le q(Z+1) \le 2m^2 Mq^2$.

Now, from the asymptotic formula (4) we conclude that $p_m = O(m \ln m)$. Therefore, we have $q \le \exp(2m \ln m + O(m))$. Finally, from (3) we see that $M \le \exp(O(m))$ and the result follows. □

The result of Lemma 2 can be improved by means of some more sophisticated sieve methods, see [11] for example. However this does not improve our main results.

3 Main Results

First of all we consider deciding the property of being square-free via Boolean functions.

Theorem 3. *Assume that a Boolean function $B(X_1, \ldots, X_r)$ is such that for any x, $1 \le x \le 2^r - 1$,*

$$B(x_1, \ldots, x_r) = S(x),$$

where $x = x_1 \ldots x_r$ is the bit representation of x. Then, for sufficiently large r, the bounds

$$\deg B \ge 0.14 \ln r \qquad \textit{and} \qquad \operatorname{spr} B \ge \frac{r}{5 \ln r}$$

hold.

Proof. Assuming that p is large enough, we put

$$m = \left\lceil \frac{r}{5 \ln r} \right\rceil.$$

Let $p_1, \ldots, p_m$ and k be defined as in Lemma 2.

Let τ be the number of monomials $\mu_j(w)$, $j = 1, \ldots, \tau$, in $w = (w_1, \ldots, w_k)$ such that for every k-dimensional vector

$$w = (w_1, \ldots, w_k) \in \{0,1\}^k$$

we have a representation of the form

$$B(Y_1, \ldots, Y_{r-k}, w) = \sum_{j=1}^{\tau} \mu_j(w) f_j(Y_1, \ldots, Y_{r-k})$$

with some polynomials $f_j(Y_1, \ldots, Y_{r-k}) \in \mathbb{F}_2[Y_1, \ldots, Y_{r-k}]$.

Obviously,

$$\tau \le \sum_{l=0}^{\deg B} \binom{k}{l} \qquad \text{and} \qquad \tau \le \operatorname{spr} B. \tag{7}$$

As in the proof of Lemma 2, we note that $p_1 < \ldots < p_m < m^2 \le 2^k$. For every $i = 1, \ldots, m$, we add several leading zeros to the binary representation of p_i to obtain binary strings s_i of length k.

If $\tau < m$ then there exist m coefficients $c_i \in \mathbb{F}_2$, $i = 1, \ldots, m$, not all equal to zero and such that

$$\sum_{i=1}^{m} c_i \mu_j(s_i) = 0, \qquad i = j, \ldots, \tau.$$

Therefore we have the identity:

$$\sum_{i=1}^{m} c_i B(X_1, \ldots, X_{r-k}, s_i) = 0.$$

Let us fix some i_0 with $c_{i_0} \ne 0$.

One easily verifies that

$$2^{r-k} = \exp\left(5m \ln m + O(m)\right).$$

Hence, from Lemma 2 we derive that there exists y, $0 \le y \le 2^{r-k}$ such that for $i = 1, \ldots, m$

$$B(y_1, \ldots, y_{r-k}, s_i) = \begin{cases} 1, & \text{if } i = i_0, \\ 0, & \text{if } i \ne i_0, \end{cases}$$

where $y = y_1 \ldots y_{r-k}$ is the bit representation of y (with several leading zeros, if necessary, to make it of length $r - k$). Thus

$$\sum_{i=1}^{m} c_i B(X_1, \ldots, X_{r-k}, s_i) = 1.$$

From the obtained contradiction we see that

$$\tau \ge m \ge 2^{(k-1)/2}.$$

Taking into account that $H(0.1) < 1/2$ and $0.1/\ln 2 \ge 0.14$, from the inequalities (7) we obtain the desired result. $\square$

Now we consider deciding if a given r-bit integer is square-free via real polynomials.

Theorem 4. *Let α_0, α_1 be two distinct real numbers and $r \geq 1$ be an integers. Suppose that a polynomial*

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

is such that for any x, $1 \leq x \leq 2^r - 1$,

$$\operatorname{sign} f(x_1, \ldots, x_r) = S(x),$$

where $x = x_1 \ldots x_r$ is the bit representation of x. Then, for sufficiently large r, the bounds

$$\deg f \geq 0.14 \ln r \qquad \textit{and} \qquad \operatorname{spr} f \geq \frac{r}{5 \ln r}$$

hold.

Proof. We proceed as in the proof of Theorem 3. Assuming that p is large enough we put

$$m = \left\lceil \frac{r}{5 \ln r} \right\rceil.$$

Let $p_1, \ldots, p_m$ and k be defined as in Lemma 2.

Let τ be the number of monomials $\mu_j(w)$, $j = 1, \ldots, \tau$, in $w = (w_1, \ldots, w_k)$ such that for every k-dimensional vector

$$w = (w_1, \ldots, w_k) \in \{\alpha_0, \alpha_1\}^k$$

we have a representation of the form

$$f(Y_1, \ldots, Y_{r-k}, w) = \sum_{j=1}^{\tau} \mu_j(w) f_j(Y_1, \ldots, Y_{r-k})$$

with some polynomials $f_j(Y_1, \ldots, Y_{r-k}) \in \mathbb{R}[Y_1, \ldots, Y_{r-k}]$.

Obviously

$$\tau \leq \binom{\deg f + k}{\deg f} \quad \text{and} \quad \tau \leq \operatorname{spr} f. \tag{8}$$

As in the proof of Lemma 2, we note that $p_1 < \ldots < p_m < m^2 \leq 2^k$. For every $i = 1, \ldots, m$, we add several leading zeros to the binary representation of p_i to obtain a binary string of length k. In this string we replace 0 by α_0 and 1 by α_1 and denote by $s_i \in \{\alpha_0, \alpha_1\}^k$ this new vector.

If $\tau < m$ then there exist m real coefficients c_i, $i = 1, \ldots, m$, not all equal to zero and such that

$$\sum_{i=1}^{m} c_i \mu_i(s_i) = 0, \qquad i = 1, \ldots, \tau.$$

Therefore we have the identity:

$$\sum_{i=1}^{m} c_i f(X_1, \ldots, X_{r-k}, s_i) = 0.$$

One easily verifies that

$$2^{r-k} = \exp\left(5m \ln m + O(m)\right).$$

Hence, from Lemma 2 we derive that there exists y, $0 \le y \le 2^{r-k}$, such that

$$c_i f(\alpha_{y_1}, \ldots, \alpha_{y_{r-k}}, s_i) > 0$$

for every $c_i \neq 0$, where $y = y_1 \ldots y_{r-k}$ is the bit representation of y (with several leading zeros, if necessary, to make it of length $r - k$). Thus

$$\sum_{i=1}^{m} c_i f(X_1, \ldots, X_{r-k}, s_i) > 0.$$

From the obtained contradiction we see that

$$\tau \ge m \ge 2^{(k-1)/2}.$$

Taking into account that $1.1H(0.1/1.1) < 1/2$, and $0.1/\ln 2 \ge 0.14$, from the inequalities (8) and Lemma 1 we obtain the desired result. □

4 Remarks

It is not hard to see that the constants in our estimates can be improved.

On the other hand, we do not know how to obtain more substantial improvements of our lower bounds. In particular, they are exponentially weaker that those of [5, 25] which are obtained for functions deciding quadratic residuacity.

Also, it would be very interesting to obtain analogues of the results of this papers for other Boolean functions related to various number theoretic problems. For example, for Boolean functions deciding primality or the parity of the number of prime divisors of x. Unfortunately, even more advanced than used in Lemma 2 sieve techniques are still not powerful enough to produce

such results, even under the assumption of the Extended Riemann Hypothesis.

Finally, we remark that that some elementary number theoretic considerations can be used to obtain a very tight lower bound on the sensitivity of $S(x)$.

We recall that the *sensitivity*, $\sigma(B)$, which is also known as the *critical complexity*, of a Boolean function $B(U_1, \ldots, U_r)$ is defined as the largest integer $s \leq r$ such that there is a binary vector $x = (x_1, \ldots, x_r) \in \{0,1\}^r$ 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,

$$\sigma(B) = \max_{x \in \{0,1\}^r} \sum_{i=1}^{r} \left| B(x) - B(x^{(i)}) \right|.$$

In other words, $\sigma(B)$ is the maximum, over all binary vectors

$$x = (x_1, \ldots, x_r) \in \{0,1\}^r,$$

of the number of points $y \in \{0,1\}^r$ on the unit *Hamming sphere* around x with $B(y) \neq B(x)$.

This parameter is of interest because it can be used to obtain lower bounds for the CREW PRAM complexity of B, see [6, 7, 8, 20, 26]. 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.

Now, let us select an r-bit square-free integer x with $x \equiv 1 \pmod 9$ and $x \equiv -1 \pmod{25}$, for example one can select a prime number $x = p$. We note that $2^{60} \equiv 1 \pmod{225}$. Therefore, flipping the ith bit of x with i of the form $i = 60j + 1$ we obtain either

$$x - 2^{i-1} \equiv x - 2^{60j} \equiv 0 \pmod 9$$

or

$$x + 2^{i-1} \equiv x + 2^{60j} \equiv 0 \pmod{25}.$$

Therefore the sensitivity of a Boolean function B satisfying the conditions of Theorem 3 is at least $\sigma(B) \geq \lfloor r/60 \rfloor$. Obviously, $\sigma(B) \leq r$.

Similar considerations can be used to derive the lower bound $\lfloor r/4 \rfloor$ on the sensitivity of primality testing, see [25].

Several more lower bounds on some other inportant complexity characteristics can be obtained from quite simple considerations.

Let us define the *additive complexity* $\mathrm{C}_{\pm}(f)$ of a polynomial f over reals as the smallest number of '$+$' and '$-$' signs necessary to write down a polynomial [4, 10, 12, 22, 23]. Obviously, for any univariate polynomial f

$$\mathrm{C}_{\pm}(f) \le \mathrm{spr}(f) - 1 \le \deg f$$

but neither $\mathrm{spr}(f)$ nor $\deg f$ can be estimated in terms of $\mathrm{C}_{\pm}(f)$. However, if a non-zero polynomial $f(X) \in \mathbb{R}[X]$ has at lease N real zeros then

$$\mathrm{C}_{\pm}(f) \ge \left(\frac{1}{5}\log N\right)^{1/2}$$

The notion of additive complexity is related to the straight-line complexity of f, see [4, 10, 12, 22, 23]

Now, let $f(x) \in \mathbb{R}(x)$ be such that

$$\mathrm{sign}\, f(x) = S(x), \qquad 0 \le x \le 2^r - 1.$$

It is easy to show that there is a constant $c > 0$ such that there are at least $c2^r$ square-free numbers of the form $4x+1$ and, thus, $f(4x)f(4x+1) < 0$ for them. Therefore $f(x)$ has at least $c2^r$ zeros. This immediately provide the same bound on the degree of f and the lower bound

$$\mathrm{C}_{\pm}(f) \ge 0.2r^{1/2} + O(1).$$

Following [17], for a function

$$f : \mathbb{R} \to \{0, 1\}$$

we define the $M_f(r)$-*invariant* as the smallest integer M such that for any $\lambda < M$ there are two r-bit integers $0 \le x_1 < x_2 \le 2^r - 1$, both divisible by λ, and such that $f(x_1) \ne f(x_2)$; see also [3, 16, 17, 18] for applications to complexity theory.

It is easy to show that for any integer λ there exists $u \le p^2$ such that $\lambda u + 1$ is square-full, where p is the smallest prime number with $\gcd(\lambda, p) = 1$. Thus $p = O(\log(\lambda+1))$. It has been shown in [11] that, for any $\varepsilon > 0$ there exists a square-free number of the form $\lambda v + 1$ with $v = O(\lambda^{4/9+\varepsilon})$, where the implied constant depends only on ε.

Therefore, if $f(x) = S(x+1)$ for $0 \le x \le 2^r - 1$ then for any $\varepsilon > 0$ the bound

$$M_f \ge C(\varepsilon)2^{9r/13-\varepsilon}$$

holds where $C(\varepsilon) > 0$ depends only on ε.

References

[1] J. Bruck, 'Harmonic analysis of polynomial threshold functions', *SIAM J. Discr. Math.*, **3** (1990), 168–177.

[2] J. Bruck and R. Smolensky, 'Polynomial threshold functions, $\mathcal{AC}^0$ functions, and spectral norms', *SIAM J. Comp.*, **21** (1992), 33–42.

[3] N. H. Bshouty, Y. Mansour, B. Schieber and P. Tiwari, 'Fast exponentiation using the truncation operations', *Comp. Compl.*, **2** (1992), 244–255.

[4] P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, Berlin, 1996.

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

[6] M. Dietzfelbinger, M. Kutyłowski and R. Reischuk, 'Exact lower time bounds for computing Boolean functions on CREW PRAMs', *J. Comp. and Syst. Sci.*, **48** (1994), 231–254.

[7] 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.

[8] 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.

[9] C. Gotsman and N. Linial, 'Spectral properties of threshold functions', *Combinatorica*, **14** (1994), 35–50.

[10] 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).

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

[12] A. G. Khovanski, *Fewnomials*, Amer. Math. Soc., Providence, RI, 1997.

[13] M. Krause and Pudlák, 'On computing Boolean functions by sparse real polynomials', *Proc. 36th IEEE Symp. on Foundations of Comp. Sci.*, 1995, 682–691.

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

[15] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[16] Y. Mansour, B. Schieber and P. Tiwari, 'A lower bound for integer greatest common divisor computations', *J. Assoc. Comp. Mach.*, **38** (1991), 453–471.

[17] Y. Mansour, B. Schieber and P. Tiwari, 'Lower bounds for computation with the floor operations', *SIAM J. Comp.*, **20** (1991), 315–327.

[18] J. Meidânis, 'Lower bounds for arithmetic problems', *Inform. Proc. Letters*, **38** (1991), 83–87.

[19] N. Nisan and M. Szegedy, 'On the degree of Boolean functions as real polynomials', *Proc. 24th ACM Symp. on Theory of Comp.*, 1992, 462–467.

[20] 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.

[21] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

[22] J.-J. Risler, 'Khovansky's theorem and complexity theory', *Rocky Mountain J. Math.*, **14** (1984), 851–853.

[23] J.-J. Risler, 'Additive complexity of real polynomials', *SIAM J. Comp.*, **14** (1985), 178–183.

[24] 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.

[25] I. E. Shparlinski, *Number-Theoretic Methods in Lower Bounds of the Complexity of the Discrete Logarithm and Related Problems*, Birkhäuser, to appear.

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

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'