

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

Erion Plaku^{1*} and Igor E. Shparlinski^{2**}

¹ Department of Mathematics and Computer Science
Clarkson University, Potsdam, NY 13699-5815, USA
plakue@clarkson.edu

² Department of Computing, Macquarie University, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract. We say a polynomial P over \mathbb{Z}_M *strongly* M -represents a Boolean function F if $F(x) \equiv P(x) \pmod{M}$ for all $x \in \{0, 1\}^n$. Similarly, P *one-sidedly* M -represents F if $F(x) = 0 \iff P(x) \equiv 0 \pmod{M}$ for all $x \in \{0, 1\}^n$. Lower bounds are obtained on the degree and the number of monomials of polynomials over \mathbb{Z}_M , which strongly or one-sidedly M -represent the Boolean function deciding if a given n -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 function.

1 Introduction

In this paper, we obtain lower bounds on the degree and the number of monomials of polynomials over \mathbb{Z}_M , which strongly or one-sidedly M -represent the Boolean function deciding if a given n -bit integer is square-free. These results provide the first non-trivial lower bounds over \mathbb{Z}_M on the complexity of a number theoretic problem which is closely related to the integer factorization problem. Similar lower bounds are also obtained for polynomials over the reals which provide a threshold representation of the above Boolean function.

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 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

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

* Supported in part by NSF grant CCR-9877150.

** Supported in part by ARC grant A69700294.

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

We say a polynomial P over \mathbb{Z}_M *strongly* M -represents S if for all $1 \leq x \leq 2^n - 1$,

$$P(x_1, \dots, x_n) \equiv S(x) \pmod{M}, \quad (1)$$

where $x = x_1 \dots x_n$ is the bit representation of x .

Similarly, we say a polynomial P over \mathbb{Z}_M *one-sidedly* M -represents S if for all $1 \leq x \leq 2^n - 1$,

$$P(x_1, \dots, x_n) \equiv 0 \pmod{M} \iff S(x) = 0, \quad (2)$$

where $x = x_1 \dots x_n$ is the bit representation of x .

For Boolean inputs we simply need to consider multilinear polynomials. Each polynomial over \mathbb{Z}_M is of the form

$$P(x_1, \dots, x_n) = \sum_{H \in \mathcal{H}} A_H \prod_{i \in H} x_i, \quad (3)$$

where

$$\mathcal{H} \subseteq 2^{\{1, 2, \dots, n\}} \quad \text{and} \quad 0 \neq A_H \in \mathbb{Z}_M.$$

We call the largest value of $|H|$ in the representation (3) the *degree* of P and write $\deg P$. We call the number of coefficients A_H , or equivalently $|\mathcal{H}|$, the *sparsity* of P and write $\text{spr } P$.

In this paper, we obtain lower bounds on the degree $\deg P$ and the sparsity $\text{spr } P$ of polynomials over \mathbb{Z}_M , satisfying either (1) or (2) for all inputs.

Similarly to the case of polynomials over \mathbb{Z}_M , for a polynomial f in n variables over the reals \mathbb{R} , we define the total degree $\deg f$ as the largest sum $i_1 + \dots + i_n$ and the sparsity $\text{spr } f$ as the number of coefficients $A_{i_1 \dots i_n}$ in the representation

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} A_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}, \quad A_{i_1, \dots, i_n} \neq 0.$$

For a real w we define the sign-function as

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

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

$$\text{sign } f(x_1, \dots, x_n) = S(x),$$

where $x = x_1 \dots x_n$ is the bit representation of x , $1 \leq x \leq 2^n - 1$.

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 $\alpha_0 = 0$ and $\alpha_1 = 1$. 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 [19]. But it is shown in [19] that the sparsity $\text{spr } f$ 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 [19].

Threshold representations of Boolean functions via real polynomials have been studied in a number of works [8, 9, 14, 19, 24, 28]. These papers contain many general estimates together with lower bounds for some particular Boolean functions. However, these Boolean functions are usually specially constructed examples which are not related to any particular number theoretic or combinatorial problem.

Representations of Boolean functions via polynomials over \mathbb{Z}_M have been studied in [2, 3, 15, 30]. In these papers, lower and upper bounds are obtained for polynomials representing the OR, MOD_M (that determines if the sum of the inputs is not divisible by M), and $\neg\text{MOD}_M$ Boolean functions. We note that a polynomial of degree d over \mathbb{Z}_M is represented by a circuit consisting of an unbounded fan-in MOD_M gate at the top where each input wire is a function of no more than d variables. In [12, 29], some lower bounds are obtained for polynomials over \mathbb{Z}_2 strongly 2-representing the Boolean function deciding the quadratic residuacity of an n -bit integer x .

In the series of papers [4–7] lower bounds have been obtained on the circuit complexity, sensitivity, degree of polynomial representation and other complexity characteristics of testing square-free numbers and computing the greatest common divisor. As in [12, 29] the method of [4–7] is based on the uniformity of distribution of long patterns of 0, 1 in the values of $S(x)$. For the quadratic residuacity a similar property has been established in [12, 29] by using the very powerful Weil estimate, in [4–7] a sieve method has been used for this purpose. In particular, for a strongly 2-representing polynomial P the lower bound

$$\deg P \geq 0.165 \dots n$$

has been obtained in [5]. It has also been applied to obtain a lower bound of order $n^{1/2}$ on the degree of real polynomials P which approximate S in the following sense: for all $1 \leq x \leq 2^n - 1$,

$$|S(x) - P(x_1, \dots, x_n)| \leq 1/3$$

where $x = x_1 \dots x_n$ is the bit representation of x . These lower bounds are derived from the asymptotic formula for the sensitivity of the function S obtained in [5]. Unfortunately, there is no link between the sensitivity and the degrees of M -representing polynomials, $M \geq 3$, and of threshold representations.

Alternative methods of [1] and [32] yield stronger but less explicit complexity results (which apply to primality testing as well). However these approaches work neither for M -representing polynomials nor for threshold representations.

Here we use the technique of [4–7] to obtain several new results about polynomial representation of the function $S(x)$.

Throughout the paper we denote by $\log x$ the binary logarithm of x , by $\ln x$ the natural logarithm of x , and $\exp(x) = e^x$.

2 Auxiliary Results

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

We use the following well known asymptotic formulas (see [13] for example)

$$\ln \left(\prod_{\substack{p \leq x \\ p \in \mathcal{P}}} p \right) = x + O\left(\frac{x}{\ln x}\right), \quad x \rightarrow \infty. \quad (4)$$

and

$$\pi(x) = \frac{x}{\ln x} + O\left(\frac{x}{\ln^2 x}\right), \quad x \rightarrow \infty, \quad (5)$$

for the number of primes $p \leq x$.

The following estimate can be found in [20], Section 10.11.

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

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

holds, where $H(\gamma) = -\gamma \log \gamma - (1 - \gamma) \log(1 - \gamma)$, $0 < \gamma < 1$, is the binary entropy function.

Now we prove the following quite technical statement.

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

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

Let $m < p_1 < \dots < p_m$ be the first m primes which are greater than m . Then, for any m -dimensional binary vector $(\sigma_1, \dots, \sigma_m)$ exists an integer y , such that $0 \leq y \leq \exp(4m \ln m + O(m \ln \ln m))$ and

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

Proof. Put

$$Q = \prod_{\substack{p \leq m \\ p \in \mathcal{P}}} p \quad \text{and} \quad R = 2^k Q.$$

From (4) we see that $Q = \exp(O(m))$. Thus it is enough to show that there exists an integer u such that $0 \leq u \leq \exp(4m \ln m + O(m \ln \ln m))$ and

$$S(Ru + p_i) = \sigma_i, \quad i = 1, \dots, m. \quad (6)$$

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

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 , $0 \leq a \leq q - 1$, such that $Ra \equiv -p_i \pmod{p_i^2}$, for all $i \in \mathcal{I}$. Therefore, $R(qz + a) + p_i \equiv 0 \pmod{p_i^2}$, for all $i \in \mathcal{I}$ and any integer z . Now we show that one can select a not too large z for which

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

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

$$\sum_{j \in \mathcal{J}} L_j(Z) < Z. \quad (7)$$

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

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

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

$$R(qz + a) + p_j \equiv 0 \pmod{p^2}, \quad 1 \leq z \leq Z,$$

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

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

$$\begin{aligned} L_j(Z) &\leq \sum_{\substack{m < p \leq V \\ \gcd(p, q) = 1}} \left(\frac{Z}{p^2} + 1 \right) \leq Z \sum_{p > m} \frac{1}{p^2} + O\left(\frac{V}{\ln V} \right) \\ &\leq Z \sum_{\nu \geq \lceil \log m \rceil} \sum_{2^{\nu+1} > p \geq 2^\nu} \frac{1}{p^2} + O\left(\frac{V}{\ln V} \right) \\ &\leq Z \sum_{\nu \geq \lceil \log m \rceil} \frac{\pi(2^{\nu+1})}{2^{2\nu}} + O\left(\frac{V}{\ln V} \right) \\ &\leq O\left(Z \sum_{\nu \geq \lceil \log m \rceil} \frac{1}{2^{\nu\nu}} + \frac{V}{\ln V} \right) = O\left(\frac{Z}{m \ln m} + \frac{V}{\ln V} \right). \end{aligned}$$

Putting $Z = m^2 Rq$ we obtain the inequality (7), provided that m is large enough. Therefore, there exists an integer u satisfying condition (6) and $0 \leq u \leq q(Z+1) \leq 2m^2 Rq^2$.

Now, from (5) we conclude that $p_m = m \ln m + O(m)$. Therefore, we have $q \leq \exp(2m \ln m + O(m \ln \ln m))$. Finally, from (4) we see that $R = \exp(O(m))$, and the result follows. \square

The result of Lemma 2 can be improved by means of some more sophisticated sieve methods, see [17] 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 polynomials in $\mathbb{Z}_M[X_1, \dots, X_n]$.

Theorem 1. *Assume that a polynomial*

$$P(X_1, \dots, X_n) \in \mathbb{Z}_M[X_1, \dots, X_n]$$

strongly M -represents $S(x)$, that is, it is such that for any x , $1 \leq x \leq 2^n - 1$,

$$P(x_1, \dots, x_n) \equiv S(x) \pmod{M},$$

where $x = x_1 \dots x_n$ is the bit representation of x . Then, for sufficiently large n , the bounds

$$\deg P \geq 0.14 \ln n \quad \text{and} \quad \text{spr } P \geq \frac{n}{5 \ln n}$$

hold.

Proof. Assuming that n is large enough, we put

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

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

We denote by τ the number of monomials $\mu_j(w)$, $j = 1, \dots, \tau$, in $w = (w_1, \dots, w_k)$, such that for every k -dimensional vector

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

we have a representation of the form

$$P(Y_1, \dots, Y_{n-k}, w) = \sum_{j=1}^{\tau} \mu_j(w) f_j(Y_1, \dots, Y_{n-k})$$

with some polynomials $f_j(Y_1, \dots, Y_{n-k}) \in \mathbb{Z}_M[Y_1, \dots, Y_{n-k}]$.

Obviously,

$$\tau \leq \sum_{l=0}^{\deg P} \binom{k}{l} \quad \text{and} \quad \tau \leq \text{spr } P. \quad (8)$$

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

If $\tau < m$, then there exist m integer coefficients c_1, \dots, c_m , not all equal to zero, with

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

Therefore we have the identity:

$$\sum_{i=1}^m c_i P(X_1, \dots, X_{n-k}, s_i) = 0.$$

Without loss of generality we can also assume that

$$\gcd(c_1, \dots, c_m) = 1.$$

Then, for some $1 \leq i_0 \leq m$ we have $c_{i_0} \not\equiv 0 \pmod{M}$.

One easily verifies that $2^{n-k} = \exp(5m \ln m + O(m))$. Hence, from Lemma 2 we derive that there exists y , $0 \leq y \leq 2^{n-k}$, such that for $i = 1, \dots, m$,

$$P(y_1, \dots, y_{n-k}, s_i) \equiv S(2^k y + p_i) \equiv \begin{cases} 1, & \text{if } i = i_0, \\ 0, & \text{if } i \neq i_0, \end{cases} \pmod{M}$$

where $y = y_1 \dots y_{n-k}$ is the bit representation of y (with several leading zeroes, if necessary, to make it of length $n - k$). Hence,

$$\sum_{i=1}^m c_i P(y_1, \dots, y_{n-k}, s_i) \equiv c_{i_0} \not\equiv 0 \pmod{M}.$$

From the obtained contradiction we see that $\tau \geq m \geq 2^{(k-1)/2}$. Taking into account that $H(0.1) < 1/2$ and $0.1/\ln 2 \geq 0.14$, from the inequalities (8) and Lemma 1 we obtain the desired result. \square

Theorem 2. *Let $M = p^\nu$ be a prime power. Assume that a polynomial*

$$P(X_1, \dots, X_n) \in \mathbf{Z}_M[X_1, \dots, X_n]$$

one-sidedly M -represents $S(x)$, that is, it is such that for any x , $1 \leq x \leq 2^n - 1$,

$$P(x_1, \dots, x_n) \equiv 0 \pmod{M} \iff S(x) = 0,$$

where $x = x_1 \dots x_n$ is the bit representation of x . Then, for sufficiently large n , the bounds

$$\deg P \geq 0.14 \ln n \quad \text{and} \quad \text{spr } P \geq \frac{n}{5 \ln n}$$

hold.

Proof. As in the proof of Theorem 1 we obtain that, for some $1 \leq i_0 \leq m$, and some $u \not\equiv 0 \pmod{M}$,

$$P(y_1, \dots, y_{n-k}, s_i) \equiv \begin{cases} u, & \text{if } i = i_0, \\ 0, & \text{if } i \neq i_0, \end{cases} \pmod{M}.$$

Also $c_{i_0} \not\equiv 0 \pmod{p}$, and hence, $\gcd(c_{i_0}, M) = 1$. Therefore,

$$\sum_{i=1}^m c_i P(y_1, \dots, y_{n-k}, s_i) \equiv c_{i_0} u \not\equiv 0 \pmod{M},$$

and as in the proof of Theorem 1 we obtain the desired result. \square

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

Theorem 3. *Let α_0, α_1 be two distinct real numbers, and $n \geq 1$ be an integer. Suppose that a polynomial*

$$f(X_1, \dots, X_n) \in \mathbb{R}[X_1, \dots, X_n]$$

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

$$\text{sign } f(\alpha_{x_1}, \dots, \alpha_{x_n}) = S(x),$$

where $x = x_1 \dots x_n$ is the bit representation of x . Then, for sufficiently large n , the bounds

$$\deg f \geq 0.14 \ln n \quad \text{and} \quad \text{spr } f \geq \frac{n}{5 \ln n}$$

hold.

Proof. We proceed as in the proof of Theorem 2. Assuming that n is large enough, we put

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

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

We denote by τ the number of monomials $\mu_j(w)$, $j = 1, \dots, \tau$, in $w = (w_1, \dots, w_k)$, such that for every k -dimensional vector

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

we have a representation of the form

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

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

Obviously,

$$\tau \leq \binom{\deg f + k}{\deg f} \quad \text{and} \quad \tau \leq \text{spr } f. \quad (9)$$

As in the proof of Lemma 2, we note that $p_1 < \dots < p_m < m^2 \leq 2^k$. For every $i = 1, \dots, m$, we add several leading zeroes 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 , $i = 1, \dots, m$, not all equal to zero, at least one of them negative, and such that

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

Therefore, we have the identity:

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

One can easily verify that

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

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

$$c_i f(\alpha_{y_1}, \dots, \alpha_{y_{n-k}}, s_i) > 0, \quad \text{for every } c_i < 0,$$

$$c_i f(\alpha_{y_1}, \dots, \alpha_{y_{n-k}}, s_i) \geq 0, \quad \text{for every } c_i \geq 0,$$

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

$$\sum_{i=1}^m c_i f(\alpha_{y_1}, \dots, \alpha_{y_{n-k}}, s_i) > 0.$$

From the obtained contradiction we see that $\tau \geq m \geq 2^{(k-1)/2}$ and as in the proof of Theorem 1 we obtain the desired result. \square

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 than those which are known for polynomials over \mathbf{Z}_2 , see [5].

In addition, it would be very interesting to obtain analogues of the results of this paper 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 sieve techniques than those used in Lemma 2 are still not powerful enough to produce such results, even under the assumption of the Extended Riemann Hypothesis.

Finally, it would be very interesting to extend Theorem 2 to arbitrary composite moduli M .

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

Let us define the *additive complexity* $C_{\pm}(f)$ of a polynomial f over reals as the smallest number of ‘+’ and ‘-’ signs necessary to write down a polynomial [11, 16, 18, 26, 27]. Obviously, for any univariate polynomial f

$$C_{\pm}(f) \leq \text{spr}(f) - 1 \leq \deg f$$

but neither $\text{spr}(f)$ nor $\deg f$ can be estimated in terms of $C_{\pm}(f)$. However, it is shown in [18, 26, 27] that if a non-zero polynomial $f(X) \in \mathbb{R}[X]$ has at least N real zeroes, then

$$C_{\pm}(f) \geq \left(\frac{1}{5} \log N\right)^{1/2}.$$

The notion of additive complexity is related to the straight-line complexity of f , see [11, 16, 18, 26, 27]

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

$$\text{sign } f(x) = S(x), \quad 0 \leq x \leq 2^n - 1.$$

If $4x + 1$ is a square-full number and $p > 1$ is a prime number such that $p^2 | (4x + 1)$, then $p^2 \equiv 1 \pmod{4}$ and $4x + 1 = (4q + 1)p^2$ for some positive integer q . For a fixed prime p , there are at most $2^n/p^2 + 1$ integers q that satisfy the above condition. Hence, the number of square-full numbers of the form $4x + 1$ is bounded above by

$$\sum_{3 \leq p \leq (2^n - 1)^{1/2}} \left(\frac{2^n}{p^2} + 1\right) \leq 2^{n-1}.$$

It follows then, that there is a constant $c > 0$ such that there are at least $c2^n$ square-free numbers of the form $4x + 1$ and, thus, $f(4x)f(4x + 1) \leq 0$ for them. Therefore, $f(x)$ has at least $c2^n$ zeroes. This immediately provides the same bound on the degree of f and the lower bound

$$C_{\pm}(f) \geq (0.2n)^{1/2} + O(1).$$

Following [22], for a function

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

we define the $M_f(n)$ -invariant as the smallest integer M , such that for any $\lambda < M$ there are two n -bit integers $0 \leq x_1 < x_2 \leq 2^n - 1$, both divisible by λ ,

and such that $f(x_1) \neq f(x_2)$; see also [10, 21–23] for applications to complexity theory.

It is easy to show that, for any integer λ , there exists $u \leq p^2$ 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 [17] 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 $0 \leq x \leq 2^n - 1$, then, for any $\varepsilon > 0$ the bound

$$M_f \geq C(\varepsilon)2^{9n/13-\varepsilon}$$

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

Acknowledgement. The authors thank Tat-Hung Chan and Alexis Mael for their interest and several helpful discussions.

References

1. E. Allender, M. Saks and I. E. Shparlinski, ‘A lower bound for primality’, *J. of Comp. and Syst. Sci.*, **62** (2001), 356–366.
2. D. Barrington, R. Beigel, and S. Rudich, ‘Representing Boolean functions as polynomials modulo composite integers’, *Comp. Compl.*, **4**, (1994), 367–382.
3. D. Barrington and G. Tardos, ‘A lower bound on the MOD 6 degree of the OR function’ *Comp. Compl.*, **7** (1998), 99–108.
4. A. Bernasconi, C. Damm and I. E. Shparlinski, ‘On the average sensitivity of testing square-free numbers’, *Proc. 5th Intern. Computing and Combinatorics Conf.*, Tokyo, 1999, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 1999, v.1627, 291–299.
5. A. Bernasconi, C. Damm and I. E. Shparlinski, ‘The average sensitivity of square-freeness’, *Comp. Compl.* **9** (2000), 39–51.
6. A. Bernasconi, C. Damm and I. E. Shparlinski, ‘Circuit and decision tree complexity of some number theoretic problems’, *Inform. and Comp.*, **168** (2001), 113–124.
7. A. Bernasconi and I. E. Shparlinski, ‘Circuit complexity of testing square-free numbers’, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1563** (1999), 47–56.
8. J. Bruck, ‘Harmonic analysis of polynomial threshold functions’, *SIAM J. Discr. Math.*, **3** (1990), 168–177.
9. J. Bruck and R. Smolensky, ‘Polynomial threshold functions, \mathcal{AC}^0 functions, and spectral norms’, *SIAM J. Comp.*, **21** (1992), 33–42.
10. N. H. Bshouty, Y. Mansour, B. Schieber and P. Tiwari, ‘Fast exponentiation using the truncation operations’, *Comp. Compl.*, **2** (1992), 244–255.
11. P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, Berlin, 1996.
12. D. Coppersmith and I. E. Shparlinski, ‘On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping’, *J. Cryptology*, **13** (2000), 339–360.
13. H. Davenport, *Multiplicative number theory*, Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

14. C. Gotsman and N. Linial, ‘Spectral properties of threshold functions’, *Combinatorica*, **14** (1994), 35–50.
15. F. Green, ‘A complex-number Fourier technique for lower bounds on the mod- m degree’, *Comp. Compl.*, **9** (2000), 16–38.
16. 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).
17. D. R. Heath-Brown, ‘The least square-free number in an arithmetic progression’, *J. Reine Angew. Math.*, **332** (1982), 204–220.
18. A. G. Khovanski, *Fewnomials*, Amer. Math. Soc., Providence, RI, 1997.
19. M. Krause and Pudlák, ‘On computing Boolean functions by sparse real polynomials’, *Proc. 36th IEEE Symp. on Foundations of Comp. Sci.*, 1995, 682–691.
20. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
21. Y. Mansour, B. Schieber and P. Tiwari, ‘A lower bound for integer greatest common divisor computations’, *J. Assoc. Comp. Mach.*, **38** (1991), 453–471.
22. Y. Mansour, B. Schieber and P. Tiwari, ‘Lower bounds for computation with the floor operations’, *SIAM J. Comp.*, **20** (1991), 315–327.
23. J. Meidânis, ‘Lower bounds for arithmetic problems’, *Inform. Proc. Letters*, **38** (1991), 83–87.
24. N. Nisan and M. Szegedy, ‘On the degree of Boolean functions as real polynomials’, *Comp. Compl.*, **4** (1994), 301–313.
25. 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.
26. J.-J. Risler, ‘Khovansky’s theorem and complexity theory’, *Rocky Mountain J. Math.*, **14** (1984), 851–853.
27. J.-J. Risler, ‘Additive complexity of real polynomials’, *SIAM J. Comp.*, **14** (1985), 178–183.
28. 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.
29. I. E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser, 1999.
30. S.-C. Tsai, ‘Lower bounds on representing Boolean functions as polynomials in \mathbb{Z}_m ’, *SIAM J. Discr. Math.*, **9**(1) (1996), 55–62.
31. I. Wegener, *The complexity of Boolean functions*, Wiley-Teubner Series in Comp. Sci., Stuttgart, 1987.
32. A. Woods, ‘Subset sum “cubes” and the complexity of prime testing’, *Preprint*, 2001, 1–17. Available from http://www.maths.uwa.edu.au/~woods/alan_research.html.