JOACHIM VON ZUR GATHEN & IGOR SHPARLINSKI (1998). The CREW PRAM complexity of modular inversion. In *Proceedings of LATIN '98*, Campinas, Brazil, C. L. LUCCHESI & A. V. MOURA, editors, volume 1380 of *Lecture Notes in Computer Science*, 305–315. Springer-Verlag, Berlin, Heidelberg. ISBN 3-540-64275-7. ISSN 0302-9743. URL http://dx.doi.org/10.1007/BFb0054331. Final version in SIAM Journal on Computing.

The CREW PRAM complexity of modular inversion

JOACHIM VON ZUR GATHEN
and
IGOR SHPARLINSKI

FB Mathematik-Informatik, Universität-GH Paderborn,
33095 Paderborn, Germany
gathen@uni-paderborn.de

and

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

1 Introduction

In this paper we address the problem of parallel computation of the inverse of integers modulo an integer M. That is, given positive integers $M \geq 3$ and $x < M$, with $\gcd(x, M) = 1$, we want to compute its modular inverse $\mathrm{inv}_M(x) \in \mathbb{N}$ defined by the conditions

$$x \cdot \mathrm{inv}_M(x) \equiv 1 \bmod M, \qquad 1 \leq \mathrm{inv}_M(x) < M. \tag{1.1}$$

Since $\mathrm{inv}_M(x) \equiv x^{\varphi(M)-1} \bmod M$, where φ is the Euler function, inversion is a special case of the more general question of modular exponentiation. Both these problems can also be considered over finite fields and other algebraic domains.

For inversion, exponentiation and gcd, several parallel algorithms are in the literature [1, 2, 8, 9, 10, 11, 12, 13, 14, 19, 20, 17]. The question of obtaining a general parallel algorithm running in poly-logarithmic time $(\log n)^{O(1)}$ for n-bit integers M is wide open [10, 11].

Some lower bounds on the depth of arithmetic circuits are known [10, 14]. On the other hand, some examples indicate that for this kind of problem the Boolean model of computation may be more powerful than the arithmetic model; see discussions of these phenomena in [8, 10, 14].

In this paper we show that the method of [4, 24] can be adapted to derive non-trivial lower bounds on Boolean CREW PRAMs. It is based on estimates of exponential sums.

Our bounds are derived from lower bounds for the *sensitivity* $\sigma(f)$ (or *critical complexity*) of a Boolean function $f(X_1, \ldots, X_n)$ with binary inputs $X_1, \ldots, X_n$. It is defined as the largest integer $m \le n$ such that there is a binary vector $x = (x_1, \ldots, x_n)$ for which $f(x) \ne f(x^{(i)})$ for m values of $i \le n$, where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate. In other words, $\sigma(f)$ is the maximum, over all input vectors x, of the number of points y on the unit Hamming sphere around x with $f(y) \ne f(x)$; see e.g., [27].

Since [3], the sensitivity has been used as an effective tool for obtaining lower bounds of the CREW PRAM complexity, i.e., the complexity on a parallel random access machine with an unlimited number of all-powerful processors, where each machine can read from and write to one memory cell at each step, but where no write conflicts are allowed: each memory cell may be written into by only one processor, at each time step.

By [21], $0.5 \log_2(\sigma(f)/3)$ is a lower bound on the parallel time for computing f on such machines, see also [5, 6, 7, 27]. This yields immediately the lower bound $\Omega(\log n)$ for the OR and the AND of n input bits. It should be contrasted with the common CRCW PRAM, where write conflicts are allowed, provided every processor writes the same result, and where all Boolean functions can be computed in constant time (with a large number of processors).

The contents of the paper is as follows. In Section 2, we prove some auxiliary results on exponential sums. We apply these in Section 3 to obtain a lower bound on the sensitivity of the least bit of the inverse modulo a prime. In Section 4, we use the same approach to obtain a lower bound on the sensitivity of the least bit of the inverse modulo an odd square free M. The bound is somewhat weaker, and the proof becomes more involved due to zero-divisors in the residue ring modulo M, but for some such moduli we are able to match the known upper and the new lower bounds. Namely, we obtain the lower bound $\Omega(\log n)$ on the CREW PRAM complexity of inversion modulo an n-bit odd square free M with not 'too many' prime divisors, and we exhibit infinite sequences of M for which this bound matches the upper bound $O(\log n)$ from [10] on the depth of P-uniform Boolean circuits for inversion modulo a 'smooth' M with only 'small' prime divisors; see (4.2) and (4.3). For example, the bounds coincide for moduli $M = p_1 \cdots p_s$, where $p_1, \ldots, p_s$ are any $\lceil s/\log s \rceil$ prime numbers between s^3 and $2s^3$.

We apply our method in Section 5 to the following problem posed by Allan Borodin (see Open Question 7.2 of [10]): given n-bit positive integers m, x, e, compute the mth bit of x^e.

Generally speaking, a parallel lower bound $\Omega(\log n)$ for a problem with n inputs is not a big surprise. Our interest in these bounds comes from their following features:

- some of these questions have been around for over a decade;
- no similar lower bounds are known for the gcd;
- on the common CRCW PRAM, the problems can be solved in constant time;
- for some types of inputs, our bounds are asymptotically optimal;
- the powerful tools we use from the theory of finite fields might prove helpful for other problems in this area.

2 Exponential sums

The main tool for our bounds are estimates of exponential sums. For a prime p and a positive integer z, we write $\mathbf{e}_p(z) = \exp(2\pi i z/p) \in \mathbf{C}$. The following identity follows from the formula for a geometric sum.

Lemma 2.1. *For any prime p and any integer a,*

$$\sum_{0 \le u < p} \mathbf{e}_p(au) = \begin{cases} 0, & \text{if } a \not\equiv 0 \bmod p, \\ p, & \text{if } a \equiv 0 \bmod p. \end{cases}$$

Lemma 2.2. *and any positive integer $H \le p$, we have*

$$\sum_{0 \le a < p} \left| \sum_{0 \le x, y < H} \mathbf{e}_p(a(y-x)) \right| = pH$$

Proof. We note that

$$\sum_{0 \le x, y < H} \mathbf{e}_p(a(y-x)) = \left| \sum_{0 \le x < H} \mathbf{e}_p(ax) \right|^2 \ge 0.$$

Thus

$$\sum_{0\le a<p}\left|\sum_{0\le x,y<H}\mathbf{e}_p\left(a(y-x)\right)\right| = \sum_{0\le a<p}\sum_{0\le x,y<H}\mathbf{e}_p\left(a(y-x)\right)$$
$$= \sum_{0\le x,y<H}\sum_{0\le a<p}\mathbf{e}_p\left(a(y-x)\right).$$

From Lemma 2.1 we see that the last sum is equal to pW, where W is the number of (x,y) with $x\equiv y \bmod p$ and $0\le x,y<H$. Obviously $W=H$. □

In the sequel, we consider several sums over values of rational functions in residue rings, which may not be defined for all values. We use the symbol $\sum^*$ to express that the summation is extended over those arguments for which the rational function is well-defined, i.e., its denominator is relatively prime to the modulus. We give an explicit definition only in the example of the following statement, which is essentially the Weil bound, see [18, 23, 28].

Lemma 2.3. *Let $f,g\in\mathbb{Z}[X]$ be two polynomials of degrees n, m, respectively, and p a prime number such that the rational function f/g is defined and not constant modulo p. Then*

$$\left|\sum_{0\le x<p}{}^{*}\,\mathbf{e}_p\left(f(x)/g(x)\right)\right| = \left|\sum_{\substack{0\le x<p\\ \gcd(g(x),p)=1}}\mathbf{e}_p\left(f(x)/g(x)\right)\right| \le (n+m-1)p^{1/2}.$$

Lemma 2.4. *Let $p=$ be a prime number, $f,g\in\mathbb{Z}[X]$ of degrees n, m, respectively, such that f/g is defined and neither constant nor a linear function modulo p. Then for any $N,H\in\mathbb{N}$ with $H\le p$ we have*

$$\left|\sum_{0\le x,y<H}{}^{*}\,\mathbf{e}_p\left(\frac{f(N+x-y)}{g(N+x-y)}\right)\right| \le (n+m-1)Hp^{1/2}.$$

Proof. From Lemma 2.1 we obtain

$$\begin{aligned}
&\left|\sum_{0\le x,y<H}{}^{*}\,\mathbf{e}_p\left(\frac{f(N+x-y)}{g(N+x-y)}\right)\right|\\
&= \frac{1}{p}\left|\sum_{0\le u<p}{}^{*}\,\mathbf{e}_p\left(d\,f(u)/g(u)\right)\sum_{0\le a<p}\sum_{0\le x,y<H}\mathbf{e}_p\left(a(u-N-x+y)\right)\right|\\
&= \frac{1}{p}\left|\sum_{0\le a<M}\mathbf{e}_p(-aN)\sum_{0\le u<p}{}^{*}\,\mathbf{e}_p\left(\frac{f(u)}{g(u)}+au\right)\sum_{0\le x,y<H}\mathbf{e}_p\left(a(y-x)\right)\right|\\
&\le \frac{1}{p}\sum_{0\le a<p}\left|\sum_{0\le u<p}{}^{*}\,\mathbf{e}_p\left(\frac{f(u)}{g(u)}+au\right)\right|\cdot\left|\sum_{0\le x,y<H}\mathbf{e}_p\left(a(y-x)\right)\right|.
\end{aligned}$$

From Lemma 2.3 we see that for each $a<p$ the sum over u can be estimated as $(n+m-1)p^{1/2}$. Applying Lemma 2.2, we obtain the result. □

Throughout this paper, $\log z$ means the logarithm of z in base 2, $\ln z$ means the natural logarithm, and

$$\operatorname{Ln} z = \begin{cases} \ln z, & \text{if } z > 1, \\ 1, & \text{if } z \le 1. \end{cases}$$

3 PRAM complexity of the least bit of the inverse modulo a prime number

In this section, we prove a lower bound on the sensitivity of the Boolean function representing the least bit of the inverse modulo p, for an n-bit prime p. For $x \in \mathbb{N}$ with $\gcd(x, p) = 1$, we recall the definition of $\mathrm{inv}_p\,(x) \in \mathbb{N}$ in (1.1). Furthermore, for $x_0, \ldots, x_{n-2} \in \{0, 1\}$, we let

$$\mathrm{num}(x_0, \ldots, x_{n-2}) = \sum_{0 \le i \le n-2} x_i 2^i \tag{3.1}$$

We consider Boolean functions f with $n-1$ inputs which satisfy the congruence

$$f(x_0, \ldots, x_{n-2}) \equiv \mathrm{inv}_p\,(\mathrm{num}(x_0, \ldots, x_{n-2})) \bmod 2 \tag{3.2}$$

for all $x_0, \ldots, x_{n-2} \in \{0, 1\}$ with $(x_0, \ldots, x_{n-2}) \ne (0, \ldots, 0)$. Thus no condition is imposed for the value of $f(0, \ldots, 0)$.

Finally we recall the sensitivity σ from the introduction.

Theorem 3.1. *Let p be a sufficiently large n-bit prime. Suppose that a Boolean function $f(X_O, \ldots, X_{n-2})$ satisfies the congruence (3.2). Then*

$$\sigma(f) \ge \frac{1}{6}n - \frac{1}{3}\log n - 1.$$

Proof. We let k be an integer parameter to be determined later, with $2 \le k \le n-3$, and show that $\sigma(f) \ge k$ for p large enough. For this, we prove that there is some integer x with $1 \le x \le 2^{n-k-1}$ and

$$\mathrm{inv}_p\,(2^k x) \equiv 1 \bmod 2, \qquad \mathrm{inv}_p\,(2^k x + 2^{i-1}) \equiv 0 \bmod 2 \quad \text{for } 1 \le i \le k,$$

provided that p is large enough. We note that all these $2^k x$ and $2^k x + 2^i$ are indeed invertible modulo p.

We put $e_0 = 0$, $\delta_0 = 1$, and $e_i = 2^{i-1}$, $\delta_i = 0$ for $1 \le i \le k$. Then it is sufficient to show that there exist integers $x, u_0, \ldots, u_k$ with

$$\begin{gathered} (2^k x + e_i)^{-1} \equiv 2u_i + \delta_i \bmod p, \\ 1 \le x \le 2^{n-k-1}, \quad 0 \le u_i \le (p-3)/2 \quad \text{for } 0 \le i \le k. \end{gathered}$$

Next we put $A = 2^k$, $H = 2^{n-k-2}$, $K = \lfloor (p-3)/4 \rfloor$, and $\Delta_i = 2K + \delta_i$ for $0 \le i \le k$. Then it is sufficient to find integers $x, y, u_0, \ldots, u_k, v_0, \ldots, v_k$ satisfying

$$\begin{array}{l} (A(H+x-y)+e_i)^{-1} \equiv 2(u_i - v_i) + \Delta_i \bmod p, \\ 0 \le x, y < H, \qquad 0 \le u_0, \ldots, u_k, v_0, \ldots, v_k < K. \end{array} \tag{3.3}$$

A typical application of character sum estimates to systems of equations proceeds as follows. One expresses the number of solutions as a sum over $a \in \mathbb{Z}_p$, using Lemma 2.1, then isolates the term corresponding to $a = 0$, and (hopefully) finds that the remaining sum is less than the isolated term. Usually, the challenge is to verify the last part. In the task at hand, Lemma 2.1 expresses the number of solutions of (3.3) as

$$\begin{aligned} & p^{-(k+1)} \sum_{0 \le x,y < H}{}^{*} \sum_{\substack{0 \le u_0, \ldots, u_k, \\ v_0, \ldots, v_k < K}} \\ & \quad \cdot \sum_{0 \le a_0, \ldots, a_k < p} \mathbf{e}_p \left(\sum_{0 \le i \le k} a_i \left((A(H+x-y)+e_i)^{-1} - 2(u_i - v_i) - \Delta_i \right) \right) \\ & \qquad = p^{-(k+1)} \sum_{0 \le a_0, \ldots, a_k < p} \mathbf{e}_p \left(- \sum_{0 \le i \le k} a_i \Delta_i \right) \\ & \qquad\qquad \cdot \sum_{0 \le x,y < H}{}^{*} \mathbf{e}_p \left(\sum_{0 \le i \le k} a_i \left(A(H+x-y)+e_i \right)^{-1} \right) \\ & \qquad\qquad\quad \cdot \sum_{\substack{0 \le u_0, \ldots, u_k, \\ v_0, \ldots, v_k < K}} \mathbf{e}_p \left(\sum_{0 \le i \le k} 2a_i (v_i - u_i) \right) \\ & \qquad = p^{-(k+1)} (H^2 K^{2(k+1)} + R), \end{aligned}$$

where the first summand corresponds to $a_0 = \cdots = a_k = 0$. For other indices $(a_0, \ldots, a_k)$, the sum over x, y satisfies the conditions of Lemma 2.4, with $n = k$ and $m = k+1$, and thus

$$\begin{aligned} |R| & \le 2kHp^{1/2} \sum_{0 \le a_0, \ldots, a_k < p} \left| \sum_{\substack{0 \le u_0, \ldots, u_k, \\ v_0, \ldots, v_k < K}} \mathbf{e}_p \left(\sum_{0 \le i \le k} 2a_i (v_i - u_i) \right) \right| \\ & = 2kHp^{1/2} \prod_{0 \le i \le k} \sum_{0 \le a_i < p} \left| \sum_{0 \le u_i, v_i < K} \mathbf{e}_p \left(a_i (v_i - u_i) \right) \right| \\ & \le 2kHp^{1/2} (pK)^{k+1}. \end{aligned}$$

We have left out the factors $|\mathbf{e}_p(-a_i \Delta_i)|$, which equal 1, transformed the summation index $2a_i$ into a_i, and used Lemma 2.2.

It is sufficient to show that $H^2 K^{2(k+1)}$ is larger than $|R|$, or that

$$HK^{k+1} > 2kp^{k+3/2}.$$

Since $K \geq (p-6)/4$, it is sufficient that

$$2^{n-k-2} > 2k(\frac{p}{p-6})^{k+1} p^{1/2} 4^{k+1}. \tag{3.4}$$

We now set $k = \lfloor (n - 3\log n)/6 \rfloor$, so that $6(k+1) \leq n \leq 2^{n-2} \ln 2 < (p-6)\ln 2$. Now $(1+z^{-1})^z < e$ for real $z > 0$, and

$$\left(\frac{p}{p-6}\right)^{k+1} < e^{6(k+1)/(p-6)} < 2.$$

Furthermore, $p^{1/2} \leq 2^{n/2}$ and $32n/3 < n^{3/2}$, and (3.4) follows from

$$2^{n/2} > 2^{n/2} \cdot \frac{32}{3} n \cdot 2^{-\frac{3}{2}\log n} \geq 64 \cdot \frac{n}{6} \cdot 2^{n/2 - \frac{3}{2}\log n} \geq 64k \cdot 2^{3k}. \qquad \square$$

From [21] we know that the CREW PRAM complexity of any Boolean function f is at least $0.5 \log(\sigma(f)/3)$, and we have the following consequence.

Corollary 3.2. *Any CREW PRAM computing the least bit of the inverse modulo a sufficiently large n-bit prime needs at least $0.5 \log n - 3$ steps.*

4 PRAM complexity of the least bit of the inverse modulo an odd square free integer

In this section, we prove a lower bound on the PRAM complexity of finding the least bit of the inverse modulo an odd square free integer.

To avoid complications with gcd computations, we make the following (generous) definition. Let M be an odd square free n-bit integer, and f a Boolean function with n inputs. Then f *computes the least bit of the inverse modulo M* if and only if

$$\mathrm{inv}_M(\mathrm{num}(x)) \equiv f(x) \bmod 2$$

for all $x \in \{0,1\}^{n-1}$ with $\gcd(\mathrm{num}(x), M) = 1$. Thus no condition is imposed for integers $x \geq 2^n$ or that have a nontrivial common factor with M.

Theorem 4.1. *Let $M > 2$ be an odd square free integer with $\omega(M)$ distinct prime divisors, and f the Boolean function representing the least bit of the inverse modulo M, as above. Then*

$$\sigma(f) \geq \frac{0.5 \ln M - \omega(M) \mathrm{Lnln} M}{\mathrm{Lnln}\,\omega(M) + O(1)}.$$

The proof follows the same way as the proof of Theorem 3.1, with replacement Lemma 2.3 by its analogue for square free moduli (where the distinct prime divisors shows up) and a lower bound on the number of values of rational function which are relatively prime to M.

Our bound takes the form

$$\sigma(f) = \Omega(n/\text{Lnln}n) \tag{4.1}$$

for an odd square free n-bit M with $\omega(M) \le \beta \ln M/\text{Lnln}M$ for some constant $\beta < 0.5$. We recall that $\omega(M) \le (1 + o(1)) \ln M/\text{Lnln}M$ for any $M > 1$, and that $\omega(M) = O(\text{Lnln}M)$ for almost all odd square free numbers M.

We denote by $i_{\text{PRAM}}(M)$ and $i_{\text{BC}}(M)$ the CREW PRAM complexity and the Boolean circuit complexity, respectively, of inversion modulo M. We know from [10, 20] that

$$i_{\text{PRAM}}(M) \le i_{\text{BC}}(M) = O(n) \tag{4.2}$$

for any n-bit integer M. The *smoothness* $\gamma(M)$ of an integer M is defined as its largest prime divisor, and M is b-smooth if and only if $\gamma(M) \le b$. Then

$$i_{\text{PRAM}}(M) \le i_{\text{BC}}(M) = O(\log(n\gamma(M))). \tag{4.3}$$

Since we are mainly interested in lower bounds in this paper, we do not discuss the issue of uniformity.

Corollary 4.2.

$$i_{\text{BC}}(M) \ge i_{\text{PRAM}}(M) \ge (0.5 + o(1)) \log n \tag{4.4}$$

for any odd square free n-bit integer M with $\omega(M) \le 0.49 \ln M/\text{Lnln}M$.

Theorem 4.3. *There is an infinite sequence of moduli M such that the CREW PRAM complexity and the Boolean circuit complexity of computing the least bit of the inverse modulo M are both $\Theta(\log n)$, where n is the bit length of M.*

Proof. We show how to construct infinitely many odd square free integers M with $\omega(M) \le 0.34 \ln M/\text{Lnln}M$, thus satisfying the lower bound (4.4), and with smoothness $\gamma(M) = O(\log^3 M)$, thus satisfying the upper bound $O(\ln\ln M) = O(\log n)$ of [10] on the depth of Boolean circuits for inversion modulo such M.

For each integer $s > 1$ we select $\lfloor s/\ln s \rfloor$ primes between s^3 and $2s^3$, and let M be the product of these primes. Then, $M \ge s^{3s/\ln s} = \exp(3s)$, and thus $\omega(M) \le s/\ln s \le 0.34 \ln M/\ln\ln M$, provided that s is large enough. □

5 Complexity of one bit of an integer power

For nonnegative integers u and m, we let $\mathrm{Bt}_m(u)$ be the mth lower bit of u, i.e., $\mathrm{Bt}_m(u) = u_m$ if $u = \sum_{i \geq 0} u_i 2^i$ with each $u_i \in \{0, 1\}$. If $u < 2^m$, then $\mathrm{Bt}_m(u) = 0$.

In this section, we obtain a lower bound on the CREW PRAM complexity of computing $\mathrm{Bt}_m(x^e)$. For small m, this function is simple, for example $\mathrm{Bt}_0(x^e) = \mathrm{Bt}_0(x)$ can be computed in one step. However, we show that for larger m this is not the case, and the PRAM complexity is $\Omega(\log n)$ for n-bit data.

Exponential sums modulo M are easiest to use when M is a prime, as in Section 3. In Section 4 we had the more difficult case of a square free M, and now we have the extreme case $M = 2^m$.

Theorem 5.1. *Let m and n be positive integers with $n \geq m + m^{1/2}$, and let f be the Boolean function with $2n$ inputs and*

$$f(x_0, \ldots, x_{n-1}, e_0, \ldots, e_{n-1}) = \mathrm{Bt}_{m-1}(x^e),$$

where $x = \mathrm{num}(x_0, \ldots, x_{n-1})$ and $e = \mathrm{num}(e_0, \ldots, e_{n-1})$; see (3.1). Then

$$\sigma(f) \geq \gamma m^{1/2} + o(m),$$

where $\gamma = 3 - 7^{1/2} = 0.3542\ldots$.

The proof is based on similar considerations as the proofs of Theorems 3.1 and 4.1 with using the bound of [26] of exponential sums with the denominator 2^m.

Corollary 5.2. *Let $n \geq m + m^{1/2}$. The CREW PRAM complexity of finding the mth bit of an n-bit power of an n-bit integer is at least $0.25 \log m - o(\log m)$. In particular, for $m = \lceil n/2 \rceil$ it is $\Omega(\log n)$.*

6 Conclusion and open problems

Inversion in arbitrary residue rings can be considered along these lines. There are two main obstacles for obtaining similar results. Instead of the powerful Weil estimate of Lemma 2.3, only essentially weaker (and unimprovable) estimates are available [16, 25, 26]. Also, we need a good explicit estimate, while the bounds of [16, 25] contain non-specified constants depending on the degree of the rational function in the exponential sum. The paper [26] deals with polynomials rather than with rational functions, and its generalization has not been worked out yet.

Open Question 6.1. *Extend Theorem 4.1 to arbitrary moduli M.*

Moduli of the form $M = p^m$, where p is a small prime number, are of special interest because Hensel's lifting allows to design efficient parallel algorithms for them [2, 10, 14]. Theorem 5.1 and its proof demonstrate how to deal with such moduli and what kind of result should be expected.

Each Boolean function $f(X_1, \ldots, X_n)$ can be uniquely represented as a multilinear polynomial of degree n over $\mathbb{F}_2$ of the form

$$f(X_1, \ldots, X_n) = \sum_{0 \le k \le d} \sum_{1 \le i_1 < \ldots < i_k \le r} A_{i_1 \ldots i_k} X_{i_1} \ldots X_{i_k} \in \mathbb{F}_2[X_1, \ldots, X_n].$$

We define its weight $\operatorname{wt} f$ as the number of nonzero coefficients in this representation. Both the weight and the degree can be considered as measures of complexity of f. In [4, 24], the same method was applied to obtain good lower bounds on these characteristics of the Boolean function f deciding whether x is a quadratic residue modulo p. However, for the Boolean functions of this paper, the same approach produces rather poor results.

Open Question 6.2. *Obtain lower bounds on the weight* $\operatorname{wt} B$ *and the degree* $\deg B$ *of the Boolean function of Theorem 4.1.*

It is well known that the modular inversion problem is closely related to the GCD-problem.

Open Question 6.3. *Obtain a lower bound on the the PRAM complexity of computing integers u, v such that $Mu + Nv = 1$ for given relatively prime integers $M \ge N > 1$.*

In the previous question we assume that $\gcd(N, M) = 1$ is guaranteed. Otherwise one can easily obtain the lower bound $\sigma(f) \ge \Omega(n)$ on the *sensitivity* of the Boolean function f which on input of two n-bit integers M and N, returns 1 if they are relatively prime, and 0 otherwise. Indeed, if $M = p$ is an n bit integer, then the function returns 0 for $N = p$ and 1 for all other n bit integers. That is, the PRAM complexity of this Boolean function is at least $0.5 \log n + O(1)$.

Acknowledgment. This paper was essentially written during a sabbatical visit by the second author to the University of Paderborn, who gratefully acknowledges its hospitality and excellent working conditions.

References

[1] L. M. Adleman and K. Kompella, 'Using smoothness to achieve parallelism', *Proc. 20th ACM Symp. on Theory of Comp.*, (1988), 528–538.

[2] P. W. Beame, S. A. Cook and H. J. Hoover, 'Log depth circuits for division and related problems', *SIAM J. Comp.*, **15** (1986) 994–1003.

[3] S. A. Cook, C. Dwork and R. Reischuk, 'Upper and lower time bounds for parallel random access machines without simultaneous writes', *SIAM J. Comp.*, **15** (1986), 87–97.

[4] D. Coppersmith and I. E. Shparlinski, 'On polynomial approximation and the parallel complexity of the discrete logarithm and breaking the Diffie–Hellman cryptosystem', *Research Report RC 20724*, IBM T. J. Watson Research Centre, 1997, 1–103.

[5] M. Dietzfelbinger, M. Kutyłowski and R. Reischuk, 'Exact time bounds for computing Boolean functions on PRAMs without simultaneous writes', *J. Comp. and Syst. Sci.*, **48** (1994), 231–254.

[6] 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.

[7] 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.

[8] E. Fich and M. Tompa, 'The parallel complexity of exponentiating polynomials over finite fields', *J. ACM*, **35** (1988), 651–667.

[9] S. Gao, J. von zur Gathen and D. Panario, 'Gauss periods and fast exponentiation in finite fields', *Lecture Notes in Comp. Sci.*, **911** (1995), 311–322.

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

[11] J. von zur Gathen, 'Inversion in finite fields using logarithmic depth', *J. Symb. Comp.*, **9** (1990), 175–183.

[12] J. von zur Gathen, 'Efficient and optimal exponentiation in finite fields', *Comp. Complexity*, **1** (1991), 360–394.

[13] J. von zur Gathen, 'Processor–efficient exponentiation in finite fields', *Inform. Proc. Letters*, **41** (1992), 81–86.

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

[15] L.-K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[16] D. Ismailov, 'On a method of Hua Loo-Keng of estimating complete trigonometric sums', *Adv. Math. (Benijing)*, **23** (1992), 31–49.

[17] R. Kannan and G. Miller and L. Rudolph, 'Sublinear parallel algorithm for computing the greatest common divisor of two integers', *SIAM J. Comp.*, **16** (1987), 7–16.

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

[19] B. E. Litow and G. I. Davida, '$O(\log(n))$ parallel time finite field inversion', *Lect. Notes in Comp. Science*, **319** (1988), 74–80.

[20] M. Mňuk, 'A div (n) depth Boolean circuit for smooth modular inverse', *Inform. Proc. Letters*, **38** (1991), 153–156.

[21] 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.

[22] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some Functions of Prime Numbers', *Ill. J. Math.* **6** (1962), 64-94.

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

[24] I. E. Shparlinski, 'Number theoretic methods in lower bounds of the complexity of the discrete logarithm and related problems', *Preprint*, 1997, 1–168.

[25] I. E. Shparlinski and S. A. Stepanov, 'Estimates of exponential sums with rational and algebraic', *Automorphic Functions and Number Theory*, Vladivostok, 1989, 5–18 (in Russian).

[26] S. B. Stečkin , 'An estimate of a complete rational exponential sum', *Proc. Math. Inst. Acad. Sci. of the USSR*, Moscow, **143** (1977), 188–207 (in Russian).

[27] I. Wegener, *The complexity of Boolean functions*, Wiley Interscience Publ., 1987.

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