THE CREW PRAM COMPLEXITY OF MODULAR INVERSION

JOACHIM VON ZUR GATHEN* AND IGOR SHPARLINSKI†

Abstract. One of the long-standing open questions in the theory of parallel computation is the parallel complexity of the integer gcd and related problems, such as modular inversion. We present a lower bound $\Omega(\log n)$ for the parallel time on an exclusive-write parallel random access machine (CREW PRAM) computing the inverse modulo certain n-bit integers, including all such primes. For infinitely many moduli, our lower bound matches asymptotically the known upper bound. We obtain a similar lower bound for computing a specified bit in a large power of an integer. Our main tools are certain estimates for exponential sums in finite fields.

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 can be considered as 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, 3, 9, 10, 11, 12, 13, 14, 15, 18, 20, 21, 23, 28, 30]. 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 [11, 12].

Some lower bounds on the depth of arithmetic circuits are known [11, 15]. 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 [9, 11, 15].

In this paper we show that the method of [5, 26] can be adapted to derive non-trivial lower bounds on Boolean concurrent-read exclusive-write parallel random access machines (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 $m \leq n$ such that there is a binary vector $x = (x_1, \ldots, x_n)$ for which $f(x) \neq f(x^{(i)})$ for m values of $i \leq n$, 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 $f(y) \neq f(x)$; see e.g., [31].

Since [4], the sensitivity has been used as an effective tool for obtaining lower bounds of the CREW PRAM complexity, i.e., the *time complexity* on a parallel random access

*Fachbereich Mathematik-Informatik, Universität Paderborn, 33095 Paderborn, Germany, gathen@uni-paderborn.de

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

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 [22], $0.5 \log_2(\sigma(f)/3)$ is a lower bound on the parallel time for computing f on such machines, see also [6, 7, 8, 31]. 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 squarefree integer 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 squarefree 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 [11] on the depth of P-uniform Boolean circuits for inversion modulo a 'smooth' M with only 'small' prime divisors; see (4.6) and (4.7). 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 [11]): 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 positive integers M and z, we write $\mathbf{e}_M(z) = \exp(2\pi i z/M) \in \mathbb{C}$. Thus $\mathbf{e}_M(z_1 + z_2) = \mathbf{e}_M(z_1) + \mathbf{e}_M(z_2)$ for any z_1, z_2.

The following identity follows from the formula for a geometric sum.

Lemma 2.1. *For any integer a,*

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

Lemma 2.2. *For positive integers M and H, we have*

$$\sum_{0\le a<M}\left|\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\right| = H^2+(r+1)(M-r-1)$$

where $r\equiv H-1 \bmod M$ with $0\le r<M$ is the remainder of $H-1$ modulo M.

Proof. We note that

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

Thus

$$\begin{aligned}\sum_{0\le a<M}\left|\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\right| &= \sum_{0\le a<M}\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\\ &= \sum_{0\le x,y<H}\sum_{0\le a<M}\mathbf{e}_M\left(a(y-x)\right).\end{aligned}$$

From Lemma 2.1 we see that the last sum is equal to MW, where W is the number of (x,y) with $x\equiv y \bmod M$ and $0\le x,y<H$. It is easy to see that

$$W=\sum_{i=0}^{M-1}\left(\left\lfloor\frac{H-1-i}{M}\right\rfloor+1\right)^2.$$

Let $s=r+1$ and $q=\lfloor (H-1)/M\rfloor$ thus $q=(H-s)/M$. Then,

$$\begin{aligned}W&=(r+1)(q+1)^2+(M-r-1)q^2 = Mq^2+s(2q+1)\\ &=(H-s)q+2sq+s=(H+s)q+s\\ &=\frac{H^2-s^2}{M}+s=\frac{1}{M}(H^2+sM-s^2)\end{aligned}$$

and the result follows. □

Taking into account that $(r+1)(M-r-1)\le M^2/4$ we derive from Lemma 2.2 that the bound

$$\sum_{0\le a<M}\left|\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\right| \le H^2+M^2/4 \tag{2.1}$$

holds for any H and M.

Also, it is easy to see that for $H\le M$, then $r=H-1$ the identity of Lemma 2.2 takes the form

$$\sum_{0\le a<M}\left|\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\right| = MH, \qquad 0\le H\le M. \tag{2.2}$$

Finally, we have

$$\sum_{1\le a<M}\left|\sum_{0\le x,y<H}\mathbf{e}_M\left(a(y-x)\right)\right| = (r+1)(M-r-1)\le M^2/4 \tag{2.3}$$

Indeed, this sum is smaller by the term corresponding to $a=0$, which equals H^2.

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, so that its denominator is relatively prime to the modulus. We give an explicit definition only in the example of the following statement, which is known as the *Weil bound*; see [19, 25, 32].

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*

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

Let $\omega(k)$ denote the number of distinct prime divisors of an integer k. The following statement is a combination of the Chinese Remainder Theorem and the Weil bound.

Lemma 2.4. *Let $M\in\mathbb{N}$ be squarefree with $M\ge 2$, d a divisor of M, and $f,g\in\mathbb{Z}[X]$ of degrees n, m, respectively, such that the rational function f/g is defined and not constant modulo each prime divisor $p>\max\{n,m\}$ of M. Then*

$$\left|\sum_{0\le x<M}{}^{*}\,\mathbf{e}_M\left(d\,f(x)/g(x)\right)\right|\le (n+m-1)^{\omega(M)}M^{1/2}d^{1/2}.$$

Proof. In the following, p stands for a prime divisor of M. We define $M_p\in\mathbb{N}$ by the conditions

$$M_p\equiv 0 \bmod M/p,\qquad M_p\equiv 1 \bmod p,\qquad 1\le M_p\le M.$$

Then, one easily verifies the identity

$$\sum_{0\le x<M}{}^{*}\,\mathbf{e}_M\left(d\,f(x)/g(x)\right)=\prod_{p\mid M}\sum_{0\le x<p}{}^{*}\,\mathbf{e}_p\left(d\,f(M_px)/g(M_px)\right).$$

We use the estimate of Lemma 2.3 for those p for which $p\nmid d$ and $p>\max\{n,m\}$, and estimate trivially by p the sum for each other p. Then

$$\begin{aligned}\left|\sum_{0\le x<M}{}^{*}\,\mathbf{e}_M\left(d\,f(x)/g(x)\right)\right| &\le \prod_{p\nmid d}(n+m-1)p^{1/2}\prod_{p\mid d}p\\ &= (n+m-1)^{\omega(M/d)}(Md)^{1/2}.\end{aligned}$$

Since $\omega(M/d) \le \omega(M)$, we obtain the desired estimate. □

LEMMA 2.5. *Let $M \ge 2$ be a squarefree integer, $f, g \in \mathbb{Z}[X]$ of degrees n, m, respectively, such that f/g is defined and neither constant nor a linear function modulo each prime divisor p of M. Then for any $N, H, d \in \mathbb{N}$ with $H \le M$ and $d|M$, we have*

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

Proof. From Lemma 2.1 we obtain

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

From Lemma 2.4 we see that for each $a < M$ the sum over u can be estimated as $\left(\max\{n+m-1, 2m\}\right)^{\omega(M)} M^{1/2} \delta^{1/2}$ where $\delta = \gcd(d, a) \le d$. Applying the estimate (2.2), we obtain the result. □

The following result is the particular case $p = 2$ of Theorem 1 of [29].

LEMMA 2.6. *There exists a constant c such that for all polynomials $f = a_t X^t + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ with $\gcd(a_t, \ldots, a_1, 2) = 1$ and all integers $m \ge 1$ we have*

$$\left| \sum_{0 \le x < 2^m} \mathbf{e}_{2^m} \left(f(x) \right) \right| \le c \cdot 2^{m(1-1/t)}.$$

For $a_0, \ldots, a_{k-1} \in \mathbb{Z}$, not all zero, we define $\mu(a_0, \ldots, a_{k-1})$ to be the largest exponent e for which 2^e divides $a_0, \ldots, a_{k-1}$.

LEMMA 2.7. *Let $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ not be all zero, and*

$$b_j = \sum_{0 \le i < k} a_i 2^{ij}$$

for $0 \le j < k$. Then $\mu(b_0, \ldots, b_{k-1}) \le \mu(a_0, \ldots, a_{k-1}) + (k-1)(k-2)/2$.

Proof. We extend μ to $\mathbb{Q}$ by $\mu(a/b) = \mu(a) - \mu(b)$ and to nonzero matrices in $\mathbb{Q}^{k\times k}$ by taking the minimum value at all nonzero columns. Then $\mu(U \cdot v) \geq \mu(U) + \mu(v)$ for a matrix U and a vector v such that $Uv \neq 0$.

Let $C_k = (2^{ij})_{0\leq i,j<k}$. The determinant of this Vandermonde matrix has value

$$\mu(\det C_k) = \mu\left(\prod_{0\leq i<j<k} (2^j - 2^i)\right) = \sum_{0\leq i<j<k} i = \frac{1}{6}k(k-1)(k-2).$$

We consider an entry of the adjoint $\mathrm{ad}C_k$ of C_k. Each of the summands contributing to the determinant expansion of that entry is divisible by

$$2^{(k-3)+2(k-4)+\cdots+(k-3)},$$

so that

$$\mu(\mathrm{ad}C_k) \geq \sum_{1\leq i<k-2} i\cdot(k-2-i) = \frac{1}{6}(k-1)(k-2)(k-3).$$

(In fact, we have equality, since $\det C_{k-1}$ has the right hand side as its μ-value and is one entry of $\mathrm{ad}C_k$.) Therefore

$$\begin{aligned}\mu(C_k^{-1}) &\geq \mu(\mathrm{ad}C_k) - \mu(\det C_k)\\ &\geq \frac{1}{6}(k-1)(k-2)(k-3) - \frac{1}{6}k(k-1)(k-2)\\ &= -\frac{1}{2}(k-1)(k-2),\end{aligned}$$

Now from the inequality $\mu(a) = \mu(C_k^{-1}b) \geq \mu(C_k^{-1}) + \mu(b)$ the result follows. □

We also need an estimate on the number of terms in the sum of Lemma 2.5. For a polynomial $g \in \mathbb{Z}[X]$ and $M, H \in \mathbb{Z}$, we denote by $T_g(M, H)$ the number of $x \in \mathbb{Z}$ for which $0 \leq x < H$ and $\gcd(g(x), M) = 1$. The following result is, probably, not new and can be improved via more sophisticated sieve methods.

Lemma 2.8. *Let $M > 1$ be squarefree and $g \in \mathbb{Z}[x]$ of degree m such that* $\gcd(g(x), M) = 1$ *for some $x \in \mathbb{Z}$. Then for all integers $H \leq M$, we have*

$$T_g(M, H) \geq H \prod_{p|M}\left(1 - \frac{\min\{m,\, p-1\}}{p}\right) - (m+1)^{\omega(M)}.$$

Proof. We denote by $\rho(M, H)$ the number of $x \in \{0, \ldots, H-1\}$ such that

$$g(x) \equiv 0 \bmod M,$$

and set $\rho(M) = \rho(M, M)$. Since M is squarefree, the inclusion-exclusion principle yields

$$T_g(M, H) = H + \sum_{1\leq k\leq\omega(M)} (-1)^k \sum_{\substack{d|M\\ \omega(d)=k}} \rho(d, H).$$

For any divisor d of M we have

$$\left|\rho(d,H)-\rho(d)\frac{H}{d}\right| \le \rho(d)=\prod_{p|d}\rho(p).$$

Therefore,

$$\begin{aligned}T_g(M,H) &\ge H + H\sum_{1\le k\le\omega(M)}(-1)^k\sum_{\substack{d|M\\ \omega(d)=k}}\frac{\rho(d)}{d}-\sum_{d|M}\rho(d)\\ &= H\prod_{p|M}\left(1-\frac{\rho(p)}{p}\right)-\prod_{p|M}\left(1+\rho(p)\right).\end{aligned}$$

By assumption, g takes a nonzero value modulo every prime divisor p of M. Thus $\rho(p)\le\min\{m,\,p-1\}$, and the claim follows. □

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

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

Lemma 2.9. *For positive integers m and M, with $M>1$ squarefree, we have*

$$\prod_{p|M}\left(1-\frac{\min\{m,\,p-1\}}{p}\right)\ge\exp\left(-2m\operatorname{Ln}\ln\omega(M)-7m\right).$$

Proof. We split the logarithm of the product as follows

$$\ln\prod_{p|M}\left(1-\frac{\min\{m,\,p-1\}}{p}\right)\ge\sum_{\substack{p|M\\ p\le 2m}}\ln\left(\frac{1}{p}\right)+\sum_{\substack{p|M\\ p>2m}}\ln\left(1-\frac{m}{p}\right), \tag{2.4}$$

and prove a lower bound on each summand. For the first one, we use that

$$\sum_{p\le x}\ln p\le x\left(1+\frac{1}{2\ln x}\right)\quad\text{for } x>1$$

by [24], (3.15). Thus, for $m>1$

$$\sum_{\substack{p|M\\ p\le 2m}}\ln p\le\sum_{p\le 2m}\ln p\le 2m\left(1+\frac{1}{2\ln 2m}\right)\le 3m. \tag{2.5}$$

It is easy to verify that for $m=1$ the sum on the left hand side does not exceed $3m$ as well.

For the second summand, we use that $(1+2\delta)(1-\delta)=1+\delta(1-2\delta)\ge 1$ for $0\le\delta<1/2$, so that $\exp(2\delta)>1+2\delta\ge(1-\delta)^{-1}$ and $\ln(1-\delta)>-2\delta$. This implies that

$$\sum_{\substack{p|M\\ p>2m}}\ln\left(1-\frac{m}{p}\right)\ge -2m\sum_{\substack{p|M\\ p>2m}}\frac{1}{p}.$$

From [24], (3.20), we know that

$$\sum_{p\le x}\frac{1}{p}\le \mathrm{Lnln}\, x + B + \frac{1}{\ln^2 x},$$

where $B < 0.262$ is a constant. Let $s = \omega(M)$ and p_s be the sth prime number, so that $p_s \le s^2$ for $s \ge 2$. Thus for $s \ge 2$ we have

$$\sum_{\substack{p|M\\ p>2m}}\frac{1}{p}\le\sum_{p\le p_s}\frac{1}{p}\le\sum_{p\le s^2}\frac{1}{p}\le \mathrm{Lnln}(s^2)+B+(\ln s^2)^{-2}\le \mathrm{Lnln}(s)+2. \tag{2.6}$$

The inequality between the first and last term is also valid for $s = 1$. Now (2.4), (2.5), and (2.6) imply the claim. □

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 $f(x_0,\ldots,x_{n-2})$ satisfies the congruence (3.2). Then*

$$\sigma(f) \ge \frac{1}{6}n - \frac{1}{2}\log n - 1.$$

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 z with $1 \le z \le 2^{n-k-1}$ and

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

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

We set $e_0 = 0$, $\delta_0 = 1$, 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 $z, w_0, \ldots, w_k$ with

$$\begin{gathered}(2^k z + e_i)^{-1} \equiv 2w_i + \delta_i \bmod p,\\ 1 \le z \le 2^{n-k-1}, \quad 0 \le w_i \le (p-3)/2 \quad \text{for } 0 \le i \le k.\end{gathered} \tag{3.3}$$

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

$$\begin{array}{ll} (A(H+x-y)+e_i)^{-1} \equiv 2(u_i - v_i) + \Delta_i \bmod p, & \\ 0 \le x, y < H, \qquad 0 \le u_0, \dots, u_k, v_0, \dots, v_k < K. & \end{array} \tag{3.4}$$

Indeed from each solution of the system (3.4) we obtain a solution of the system (3.3) by putting $z = H + x - y$ and $w_i = K + u_i - v_i$, $i = 0, \dots, k$. On the other hand, the system (3.4) contains more variables and is somewhat easier to study. 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 (3.4) as

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

where the first summand corresponds to $a_0 = \cdots = a_k = 0$ and R to the remaining sum, and we used (2.2). For other $k+1$ tuples $(a_0, \dots, a_k)$, the sum over x, y satisfies the conditions of Lemma 2.5, with $n = k$ and $m = k+1$, indeed, we have

$$\sum_{0 \le i \le k} a_i \left(A(H+x-y)+e_i\right)^{-1} = \frac{f(H+x-y)}{g(H+x-y)},$$

where

$$g = \prod_{0 \le i \le k} (AX + e_i), \ f = \sum_{0 \le i \le k} a_i \frac{g}{AX + e_i} \in \mathbb{Z}[X].$$

Therefore f/g is neither constant nor linear modulo p. Thus,

$$|R| \le 2(k+1)Hp^{1/2} \sum_{0 \le a_0, \dots, a_k < p} \left| \sum_{\substack{0 \le u_0, \dots, u_k, \\ v_0, \dots, v_k < K}} \mathbf{e}_p\left(\sum_{0 \le i \le k} 2a_i(v_i - u_i) \right) \right|$$

$$\begin{aligned} &= 2(k+1)Hp^{1/2} \prod_{0\le i\le k} \sum_{0\le a_i<p} \left| \sum_{0\le u_i,v_i<K} \mathrm{e}_p\left(a_i(v_i-u_i)\right) \right| \\ &\le 2(k+1)Hp^{1/2}(pK)^{k+1}. \end{aligned}$$

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

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

$$HK^{k+1} > 2(k+1)p^{k+3/2}. \tag{3.5}$$

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

$$2^{n-k-2} > 2(k+1)\left(\frac{p}{p-6}\right)^{k+1} p^{1/2}4^{k+1}. \tag{3.6}$$

We now set $k = \lfloor (n - 3\log n)/6 \rfloor$, so that $6(k+1) \le n \le 2^{n-2}\ln 2 < (p-6)\ln 2$. 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, $p^{1/2} < 2^{n/2}$ and $32n/3 < n^{3/2}$, and (3.6) follows from

$$2^{n/2} > 2^{n/2} \cdot \frac{32}{3}n \cdot 2^{-\frac{3}{2}\log n} = 64 \cdot \frac{n}{6} \cdot 2^{n/2-\frac{3}{2}\log n} \ge 64(k+1)\cdot 2^{3k}.$$

Hence the inequality (3.5) holds, and we obtain $\sigma(f) \ge k \ge n/6 - 0.5\log n - 1$. □

From [22] 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 inversion modulo an odd squarefree integer.

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

To avoid complications with gcd computations, we make the following (generous) definition. Let M be an odd squarefree 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

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

for all $x \in \{0,1\}^{n-1}$ with $\gcd(\mathrm{num}(x), M) = 1$, where $\mathrm{num}(x)$ is the nonnegative integer with binary representation x, similar to (3.1). Thus no condition is imposed for integers $x \ge 2^n$ or that have a nontrivial common factor with M.

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

$$\sigma(f) \ge \frac{\ln M - 2\omega(M)\mathrm{Lnln}\, M}{4\mathrm{Lnln}\,\omega(M) + O(1)}.$$

Proof. We let $n = \lfloor \log_2 M \rfloor$, and k an integer parameter to be determined later. We want to show that there is some integer z with $1 \le z \le 2^{n-k-1}$ for which

$$\mathrm{inv}_M\,(2^k z) \equiv 1 \bmod 2, \qquad \mathrm{inv}_M\,(2^k z + 2^{i-1}) \equiv 0 \bmod 2, \qquad \text{for } 1 \le i \le k.$$

As in the proof of Theorem 3.1 we see that in this case $\sigma(f) \ge k$.

We put $e_0 = 0$, $\delta_0 = 1$, and $e_i = 2^{i-1}$, $\delta_i = 0$ for $1 \le i \le k$. It is sufficient to show that there exist integers $z, w_0, \dots, w_k$ such that

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

Next, we set $A = 2^k$, $H = 2^{n-k-2}$, $K = \lfloor (M-3)/4 \rfloor$, and $\Delta_i = 2K + \delta_i$ for $0 \le i < k$. As in the proof of Theorem 3.1 we see that it is sufficient to find integers $x, y, u_0, \dots, u_k, v_0, \dots, v_k$ satisfying the following conditions for $0 \le i \le k$:

$$\begin{gathered}\left(A(H + x - y) + e_i\right)^{-1} \equiv 2(u_i - v_i) + \Delta_i \bmod M,\\ 0 \le x, y < H, \qquad 0 \le u_0, \dots, u_k, v_0, \dots, v_k < K.\end{gathered}$$

Lemma 2.1 expresses the number of solutions as

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

where S_d is the subsum over those $0 \le a_0, \dots, a_k < M$ for which

$$\gcd(a_0, \dots, a_k, M) = d.$$

It is sufficient to show that

$$S_M > \sum_{\substack{d \mid M\\ d < M}} |S_d|. \tag{4.1}$$

First we note that S_M consists of only one summand corresponding to $a_0 = \cdots = a_k = 0$. Since all values to be added equal 1, we only have to estimate the number of terms for which the argument of $\sum^*$ is defined. For each y with $0 \le y < H$, we apply Lemma 2.8 to the polynomial

$$g = \prod_{0\le i\le k} (A(H + X - y) + e_i) \in \mathbb{Z}[X]$$

of degree $k+1$. We set $s = \omega(M)$, and using Lemmas 2.8 and 2.9, we deduce that

$$S_M \ge H\Big(H \exp\left(-2(k+1)\mathrm{Lnln}\, s - 7(k+1)\right) - (k+2)^s\Big) K^{2(k+1)}. \tag{4.2}$$

The other $|S_d|$ are bounded from above by

$$|S_d| \le \sum_{\substack{0\le a_0,\dots,a_k<M\\ \gcd(a_0,\dots,a_k,M)=d}} \left| \sum_{0\le x,y<H}{}^{*}\, \mathbf{e}_M \left(\sum_{0\le i\le k} a_i \left(A(H+x-y)+e_i\right)^{-1} \right) \right|$$
$$\cdot \left| \sum_{\substack{0\le u_0,\dots,u_k,\\ v_0,\dots,v_k<K}} \mathbf{e}_M \left(2 \sum_{0\le i\le k} a_i(v_i - u_i) \right) \right| .$$

Now let $d = \gcd(a_0, \dots, a_k, M)$ and

$$g = \prod_{0\le i\le k} (AX + e_i), \quad f = \sum_{0\le i\le k} \frac{a_i}{d} \frac{g}{AX+e_i} \in \mathbb{Z}[X].$$

Then

$$\sum_{0\le i\le k} \frac{a_i}{d} \left(A(H+x-y)+e_i\right)^{-1} = \frac{f(H+x-y)}{g(H+x-y)},$$

and f/g is neither constant nor linear modulo any prime divisor $p \ge k+1$ of M. Thus we can apply Lemma 2.5 and find that

$$\left| \sum_{0\le x,y<H}{}^{*}\, \mathbf{e}_M \left(d \sum_{0\le i\le k} a_i/d \left(A(H+x-y)+e_i\right)^{-1} \right) \right| \le (2k+2)^s H M^{1/2} d^{1/2};$$

the hypothesis of the lemma is satisfied because M is squarefree. If $d < M$, then $a_i = d b_i$ for some $0 \le b_0, \dots, b_k < M/d$, with at least one $b_i \ne 0$. Then

$$\sum_{\substack{0\le a_0,\dots,a_k<M\\ \gcd(a_0,\dots,a_k,M)=d}} \left| \sum_{\substack{0\le u_0,\dots,u_k,\\ v_0,\dots,v_k<K}} \mathbf{e}_{M/d} \left(\sum_{0\le i\le k} 2a_i(v_i - u_i) \right) \right|$$
$$\le (k+1) \sum_{\substack{1\le b_0<M/d\\ 0\le b_1,\dots,b_k<M/d}} \left| \sum_{\substack{0\le u_0,\dots,u_k,\\ v_0,\dots,v_k<K}} \mathbf{e}_{M/d} \left(\sum_{0\le i\le k} 2b_i(v_i - u_i) \right) \right|$$

$$= (k+1) \sum_{1 \le b_0 < M/d} \left| \sum_{0 \le u_0, v_0 < K} \mathbf{e}_{M/d}\left(2b_0(v_0 - u_0)\right) \right|$$

$$\cdot \prod_{1 \le i \le k} \sum_{0 \le b_i < M/d} \left| \sum_{0 \le u_i, v_i < K} \mathbf{e}_{M/d}\left(2b_i(v_i - u_i)\right) \right| .$$

Since M/d is odd, we may replace the summation index $2b_i$ by b_i. From the inequalities (2.3) and (2.1) we find

$$\sum_{1 \le b_0 < M/d} \left| \sum_{0 \le u_0, v_0 < K} \mathbf{e}_{M/d}\left(b_0(v_0 - u_0)\right) \right| \le \frac{M^2}{4d^2},$$

$$\sum_{0 \le b_i < M/d} \left| \sum_{0 \le u_i, v_i < K} \mathbf{e}_{M/d}\left(b_i(v_i - u_i)\right) \right| \le K^2 + \frac{M^2}{4d^2} \le \frac{5}{16} M^2 \le M^2.$$

Combining these inequalities, we obtain

$$|S_d| \le (k+1)(2k+2)^s H M^{2k+5/2} d^{-3/2},$$

therefore

$$\sum_{\substack{d|M \\ d<M}} |S_d| \le (k+1)(2k+2)^s H M^{2k+5/2} \sum_{d|M} d^{-3/2}$$
$$< \zeta(3/2)(k+1)^{s+1} 2^s H M^{2k+5/2},$$

where

$$\zeta(3/2) = \sum_{h \ge 1} h^{-3/2} = 2.61\ldots$$

Using (4.1) and (4.2) it is now sufficient to prove that

$$H\left(H \exp\left(-2(k+1)\mathrm{Lnln}\, s - 7(k+1)\right) - (k+2)^s\right) K^{2(k+1)}$$
$$> \zeta(3/2)(k+1)^{s+1} 2^s H M^{2k+5/2}$$

for some

$$k \ge \frac{\ln M - 2s \mathrm{Lnln}\, M}{4 \mathrm{Lnln}\, s + O(1)}. \tag{4.3}$$

To do so we suppose that

$$\left(H \exp\left(-2(k+1)\mathrm{Lnln}\, s - 7(k+1)\right) - (k+2)^s\right) K^{2(k+1)} \le \zeta(3/2)(k+1)^{s+1} 2^s M^{2k+5/2} \tag{4.4}$$

and will show that k satisfies the opposite inequality. Obviously, we may assume that

$$k \le 0.5 \ln M - 1.$$

We also recall that $K \geq (M-6)/4$ and $H = 2^{n-k-2} \geq M2^{-k-3}$. Now if

$$(k+2)^s \leq 0.5H \exp\left(-2(k+1)\mathrm{Lnln}\, s - 7(k+1)\right)$$

then, because $s \leq \log_2 M$, we immediately obtain (4.3). Otherwise, we derive from (4.4) that

$$\exp\left(-2(k+1)\mathrm{Lnln}\, s + O(k)\right) \leq (2k+2)^s M^{-1/2} \leq M^{-1/2} \exp(s\mathrm{Lnln}\, M).$$

Comparing this inequality with the inequality (4.3) we obtain the desired statement. □

Our bound takes the form

$$\sigma(f) = \Omega(n/\mathrm{Lnln}\, n) \tag{4.5}$$

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

We denote by $i_{PRAM}(M)$ and $i_{\mathrm{BC}}(M)$ the CREW PRAM complexity and the Boolean circuit complexity, respectively, of inversion modulo M. We know from [11, 21] that

$$i_{\mathrm{P}RAM}(M) \leq i_{\mathrm{BC}}(M) = O(n) \tag{4.6}$$

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 $\gamma(M) \leq b$. Then

$$i_{\mathrm{P}RAM}(M) \leq i_{\mathrm{B}C}(M) = O(\log(n\gamma(M))). \tag{4.7}$$

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

Corollary 4.2.

$$i_{\mathrm{B}C}(M) \geq i_{\mathrm{P}RAM}(M) \geq (0.5+o(1)) \log n \tag{4.8}$$

for any odd squarefree n-bit integer M with $\omega(M) \leq 0.49 \ln M/\mathrm{Lnln}\, M$.

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 squarefree integers M with $\omega(M) \leq 0.34 \ln M/\mathrm{Lnln}\, M$, thus satisfying the lower bound (4.8), and with smoothness $\gamma(M) = O(\log^3 M)$, thus satisfying the upper bound $O(\ln\ln M) = O(\log n)$ of [11] 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, $M \geq s^{3s/\ln s} = \exp(3s)$, and thus $\omega(M) \leq s/\ln s \leq 0.34 \ln M/\ln\ln M$, 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 squarefree 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

$$\sigma(f) \geq \gamma m^{1/2} + O(m^{1/3}),$$

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

Proof. We set $e = \lceil m^{1/2} \rceil$, and consider $g(x) = f(x, e)$, so that $\sigma(f) \geq \sigma(g)$. Furthermore, k is an integer parameter with $e \geq k \geq 2$ to be determined later.

To prove that $\sigma(g) \geq k$, it is sufficient to show that there exists an integer x with $0 \leq x < 2^{n-e}$, $\mathrm{Bt}_{m-1}\left((2^e x)^e\right) = 0$, and $\mathrm{Bt}_{m-1}\left((2^e x + 2^i)^e\right) = 1$ for $0 \leq i < k$.

The first equality holds for any such x because $e^2 \geq m$, and thus the conditions are equivalent to the existence of integers $x, u_0, \ldots, u_{k-1}$ such that

$$\begin{gathered} (2^e x + 2^i)^e \equiv 2^{m-1} + u_i \bmod 2^m, \\ 0 \leq x < 2^{n-e}, \qquad 0 \leq u_0, \ldots, u_{k-1} < 2^{m-1} \quad \text{for } 0 \leq i < k, \end{gathered}$$

which is implied by the existence of $x, u_0 \ldots, u_{k-1}, v_0, \ldots, v_{k-1}$ with

$$\begin{gathered} (2^e x + 2^i)^e \equiv 2^{m-1} + 2^{m-2} + u_i - v_i \bmod 2^m, \\ 0 \leq x < 2^{n-e}, \qquad 0 \leq u_i, v_i < 2^{m-2} \quad \text{for } 0 \leq i < k. \end{gathered} \tag{5.1}$$

We set $H = 2^{m-2}$ and $K = 2^{m-1} + 2^{m-2}$.

Lemma 2.1 expresses the number of solutions of (5.1) as

$$\begin{aligned} & 2^{-mk} \sum_{0 \leq x < 2^{n-e}} \sum_{\substack{0 \leq u_0, \ldots, u_{k-1} \\ v_0, \ldots, v_{k-1} < H}} \\ & \quad \cdot \sum_{0 \leq a_0, \ldots, a_{k-1} < 2^m} \mathbf{e}_{2^m} \left(\sum_{0 \leq i < k} a_i \left((2^e x + 2^i)^e - (K + u_i - v_i) \right) \right) \\ & = 2^{-mk} \sum_{0 \leq a_0, \ldots, a_{k-1} < 2^m} \mathbf{e}_{2^m}(-K \sum_{0 \leq i < k} a_i) \sum_{0 \leq x < 2^{n-e}} \mathbf{e}_{2^m} \left(\sum_{0 \leq i < k} a_i (2^e x + 2^i)^e \right) \\ & \quad \cdot \sum_{\substack{0 \leq u_0, \ldots, u_{k-1}, \\ v_0, \ldots, v_{k-1} < H}} \mathbf{e}_{2^m}(\sum_{0 \leq i < k} a_i (v_i - u_i)) \\ & = 2^{-mk} \sum_{0 \leq \delta \leq m} S_\delta, \end{aligned}$$

where S_δ is the subsum over all integers $0 \le a_0, \dots, a_{k-1} < 2^m$ with

$$\gcd(a_0, \dots, a_{k-1}, 2^m) = 2^\delta.$$

It is sufficient to show that

$$S_m > \sum_{0 \le \delta < m} |S_\delta|. \tag{5.2}$$

S_m contains only one summand, for $a_0 = \dots = a_{k-1} = 0$, and equals

$$S_m = 2^{n-e} H^{2k} = 2^{n+2mk-4k-e}. \tag{5.3}$$

Using the function μ from Section 2, we have for $\delta < m$ that

$$\begin{aligned} |S_\delta| \le \sum_{\substack{0 \le a_0, \dots, a_{k-1} < 2^m \\ \mu(a_0, \dots, a_{k-1}) = \delta}} & \left| \sum_{0 \le x < 2^{n-e}} \mathbf{e}_{2^m} \left(\sum_{0 \le i < k} a_i (2^e x + 2^i)^e \right) \right| \\ & \cdot \left| \sum_{\substack{0 \le u_0, \dots, u_{k-1}, \\ v_0, \dots, v_{k-1} < H}} \mathbf{e}_{2^m} \left(\sum_{0 \le i < k} a_i (v_i - u_i) \right) \right|. \end{aligned}$$

Now let $a_0, \dots, a_{k-1} < 2^m$. We set

$$h(X) = \sum_{0 \le i < k} a_i (2^e X + 2^i)^e = \sum_{0 \le j \le e} A_j X^j \in \mathbb{Z}[X], \tag{5.4}$$

so that

$$A_j = 2^{ej} \binom{e}{j} \sum_{0 \le i < k} a_i 2^{i(e-j)}, \qquad \text{for } 0 \le j \le e.$$

We put

$$\Delta = \mu(A_1, \dots, A_e).$$

If $\Delta < m$, then h is periodic modulo 2^m with period $2^{m-\Delta}$:

$$h(X + 2^{m-\Delta}) \equiv h(X) \bmod 2^m.$$

Since $n - e \ge m$ and $\mathbf{e}_M(z)$ is periodic with period M then

$$\begin{aligned} & \left| \sum_{0 \le x < 2^{n-e}} \mathbf{e}_{2^m} \left(\textstyle\sum_{0 \le i < k} a_i (2^e x + 2^i)^e \right) \right| \\ & \quad = 2^{n-e-m+\Delta} \left| \sum_{0 \le x < 2^{m-\Delta}} \mathbf{e}_{2^{m-\Delta}} \left(2^{-\Delta} h(x) \right) \right| \\ & \quad \le 2^{n-e-m+\Delta} \cdot c \cdot 2^{m-\Delta-(m-\Delta)/e} = c \cdot 2^{n-e-(m-\Delta)/e}, \end{aligned} \tag{5.5}$$

where c is the constant from Lemma 2.6. This bound also holds for $\Delta \geq m$, because the sum contains 2^{n-e} terms with absolute value 1. Using the (crude) estimate

$$\mu\left(\binom{e}{j}\right) \leq \log_2 \binom{e}{j} \leq \log_2 2^e \leq e,$$

and noting that

$$A_{k-j} = 2^{e(k-j)} \binom{e}{k-j} \sum_{0 \leq i < k} \left(a_i 2^{i(e-k)}\right) 2^{ij},$$

from Lemma 2.7 we derive that for tuples with $\mu(a_0, \ldots, a_{k-1}) = \delta$,

$$\begin{aligned} \Delta \leq \mu(A_1, \ldots, A_k) &\leq ek + e + \delta + (k-1)(e-k) + (k-1)(k-2)/2 \\ &= 2ek + \delta - (k-1)(k+2)/2 \leq 2ek + \delta - k^2/2, \end{aligned}$$

provided that $k \geq 2$. Substituting this bound in (5.5), we obtain

$$|S_\delta| \leq c \cdot 2^{n-e-(m-2ek-\delta+k^2/2)/e} T_\delta = c \cdot 2^{n-e-m/e+\delta/e+2k-k^2/2e} T_\delta$$

where

$$T_\delta = \sum_{\substack{0 \leq a_0, \ldots, a_{k-1} < 2^m \\ \mu(a_0, \ldots, a_k) = \delta}} \left| \sum_{\substack{0 \leq u_0, \ldots, u_{k-1}, \\ v_0, \ldots, v_{k-1} < H}} \mathbf{e}_{2^m} \left(\sum_{0 \leq i < k} a_i (v_i - u_i) \right) \right|.$$

We set

$$U_\delta = \begin{cases} 2^{2(m-\delta)} + 2^{2(m-2)} & if\ \delta \geq 3, \\ 2^{2m-\delta-2} & if\ 0 \leq \delta \leq 2. \end{cases}$$

Then $U_\delta \leq 2^{2m-3}$ for all $\delta \geq 0$, and as in the proof of Theorem 4.1, from Lemma 2.2 we find

$$\begin{aligned} T_\delta &\leq k \cdot \sum_{1 \leq b_0 < 2^{m-\delta}} \sum_{0 \leq b_1, \ldots, b_{k-1} < 2^{m-\delta}} \left| \sum_{\substack{0 \leq u_0, \ldots, u_{k-1}, \\ v_0, \ldots, v_{k-1} < H}} \mathbf{e}_{2^{m-\delta}} \left(\sum_{0 \leq i < k} b_i (v_i - u_i) \right) \right| \\ &\leq k \cdot 2^{2(m-\delta)} U_\delta^{k-1} \leq k \cdot 2^{2mk-3k-2\delta+3}. \end{aligned}$$

Next, we obtain

$$\begin{aligned} \sum_{0 \leq \delta < m} |S_\delta| &\leq c \cdot \sum_{0 \leq \delta < m} 2^{n-e-m/e+\delta/e+2k-k^2/2e} \cdot k \cdot 2^{2mk-3k-2\delta+3} \\ &= ck \cdot 2^{n+2mk-k-e-m/e-k^2/2e+3} \sum_{0 \leq \delta < m} 2^{-\delta(2-1/e)} \\ &< ck \cdot 2^{n+2mk-k-e-m/e-k^2/2e+4}. \end{aligned}$$

We set

$$k = \left\lfloor \gamma m^{1/2} - m^{1/3} \right\rfloor$$

where $\gamma = 3 - 7^{1/2} = 0.3542\ldots$ satisfies $-\gamma - 1 - \gamma^2/2 = -4\gamma$. It easy to verify that the inequality (5.2) holds for this choice of k, provided that m is large enough. □

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 [17, 27, 29]. Also, we need a good explicit estimate, while the bounds of [17, 27] contain non-specified constants depending on the degree of the rational function in the exponential sum. The paper [29] 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, 11, 15]. 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

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

We define its weight 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 [5, 26], 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 and the degree of the Boolean function f 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 PRAM complexity of computing integers u, v such that $Mu + Nv = 1$ for given relatively prime integers $M \geq N > 1$.*

In the previous question we assume that $\gcd(N, M) = 1$ is guaranteed. Otherwise one can easily obtain the lower bound $\sigma(f) \geq \Omega(n)$ 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, and he gratefully acknowledges its hospitality and excellent working conditions.

REFERENCES

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

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

[3] Giovanni Cesari, 'Parallel Implementation of Schönhage's Integer GCD Algorithm', *Proc. ANTS-III, Lecture Notes in Comp. Sci.*, **1423** (1998), 64–76.

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

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

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

[7] Martin Dietzfelbinger, Mirosław Kutyłowski and R "udiger 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', *Synthesis of parallel algorithms* , Morgan Kaufmann Publ., San Mateo, CA, 1993, 843–899.

[9] Faith E. Fich and Martin Tompa, 'The Parallel Complexity of Exponentiating Polynomials over Finite Fields', *J. ACM*, **35** (1988), 651–667.

[10] Shuhong Gao, Joachim von zur Gathen and Daniel Panario, 'Gauss periods and fast exponentiation in finite fields', *Proc. LATIN'95, Lecture Notes in Comp. Sci.*, **911** (1995), 311–322.

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

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

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

[14] Joachim Von Zur Gathen, 'Processor–efficient exponentiation in finite fields', *Inform. Proc. Letters*, **41** (1992), 81–86.

[15] Joachim von zur Gathen and G. Seroussi, 'Boolean Circuits versus Arithmetic Circuits', *Inform. and Comp.*, **91** (1991), 142–154.

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

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

[18] 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.

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

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

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

[22] 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.

[23] George B. Purdy, 'A carry-free algorithm for finding the greatest common divisor of two integers', *Computers and Mathematics with Applications*, **9** (1983), 311–316.

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

[25] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.

[26] I. E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser, 1999.

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

[28] Jonathan Sorenson, 'Two Fast GCD Algorithms', *Journal of Algorithms* **16** (1994), 110–144.

[29] 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).

[30] Kenneth Weber, 'Parallel Implementation of the Accelerated Integer GCD Algorithm', *Journal of Symbolic Computation* **21** (1996), 457–466.

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

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