Electronic Colloquium on Computational Complexity, Report No. 9 (1998)

Parallel Complexity of Integer Coprimality

B. Litow [§]

Abstract

We show that integer coprimality testing is in NC.

AMS classification codes: 68Q15, 68Q22, 68Q25

1 Introduction

The parallel complexity of basic arithmetic operations has been closely investigated since the 1960's. In the case of arithmetic, problem size is usually measured in terms of binary notation for the integer inputs. It is known that addition and multiplication of n-bit integers can be done in NC1, i.e., by logspace computable Boolean circuit families of $O(\log n)$ depth and with $n^{O(1)}$ Boolean gates. Details about these classical results may be found in [12], and information about the parallel complexity class NC may be found in [11, 4]. It is also know that division can be done in the same time and size bounds, but slightly more than logspace is needed to build the requisite Boolean circuits. It is open whether or not division is in NC1. See [2, 5, 7] for more information about division. It is natural to ask about other arithmetic functions. Perhaps the most important function after the basic operations is GCD (greatest common divisor.) Unfortunately, very little is known about the parallel complexity of GCD. In this situation it makes sense to investigate simpler, related arithmetic problems. For this purpose we have selected coprimality testing.

Throughout the paper n will be a positive integer and a and b will be integers in the range $2^{n-1} < a, b < 2^n$. The extended GCD problem (EGCD) is to compute positive integers x and y such that $ax - by = \mathrm{GCD}(a, b)$. Of course, the Euclidean algorithm solves EGCD. a and b are said to be coprime iff $\mathrm{GCD}(a, b) = 1$. If a and b are coprime, then modular inversion (MI) of a w.r.t. b is the computation of a positive integer x such that $ax \equiv 1 \bmod b$. Note that EGCD solves MI. Deciding whether or not a and b are coprime is

[§] Dept. of Computer Science, James Cook University, Townsville, Qld. 4811, Australia
bruce@cs.jcu.edu.au

ISSN 1433-8092

the coprimality problem (CO).

A PRAM algorithm for GCD that runs in $O(\frac{n \log\log n}{\log n})$ time was given by Kannan, Miller and Rudolph [6]. This result was improved to $\frac{n}{\log n}$ by Chor and Goldreich. Adleman and Kompella [1] gave a randomized Boolean circuit algorithm for GCD that requires $O(\log^2 n)$ depth, but $\exp(O(\sqrt{n}\log n))$ gates. Adelman and Kompella ask whether or not GCD is in DSPACE($\sqrt{n}$), which still seems to be an open question. See [1]. It is interesting to note that Reif and Tygar [10] have shown that if MI w.r.t. a prime p is in P - NC, then randomized NC is contained in DSPACE(n^ϵ) for any $\epsilon > 0$. The parallel complexity of MI is also open. In this paper we will prove the following theorem.

Theorem 1 *Integer coprimality testing (CO) is in NC.*

As a corollary we have

Corollary 1 *CO is in polylog space.*

Proof : This follows from Thm. 1 and Theorem 4 of Borodin [3]. □

The paper is in sections. Section 2 is a description of the sieve which is the starting point of our CO algorithm. Section 3 gives the outline of steps of the algorithm and a complexity analysis. Section 4 contains several technical lemmas which are used in the analysis of section 3.

2 The CO sieve

Throughout the paper $s \in [0,1]$, $\iota = \sqrt{-1}$, $\rho = 1/ab$ and $z = \mathbf{e}(s) = \exp(2\pi\iota s)$. The comprimality sieve $S(a,b)$ is defined as

$$S(a,b) = \int_0^1 \frac{ds}{z \cdot (1-(\rho z)^a)(1-(\rho/z)^b)} \tag{1}$$

Lemma 1 *If a and b are coprime, then $S(a,b) > 1/9$, otherwise $S(a,b) = 0$.*

Proof : The integrand of Eq. 1 can be expanded as the geometric series

$$\sum_{p=0}^{\infty}\sum_{q=0}^{\infty} \rho^{ap+bq} \cdot z^{ap-bq-1}$$

Note that $\int_0^1 z^{ap-bq-1} ds$ vanishes, unless $ap - bq - 1 = 0$. If a and b are coprime, then there will be $p < b$ and $q < a$ such that $ap - bq - 1 = 0$. This means $S(a,b) > \rho^{2ab} = (1-1/ab)^{2ab} > 1/9$. If a and b are not coprime, then the integral of every summand in the above expression will vanish. □

The integral in Eq. 1 appears to be a very poor candidate for NC evaluation, but we will show that it can be approximated in NC so that Lem. 1 can be used.

3 The algorithm

Throughout the paper, we will use the term 'rational' to mean a quantity $\alpha + \iota\beta$, where α and β are ordinary rational numbers. Let $f(n)$ be a rational valued function on the non-negative integers. We will say that $f(n)$ is *NC-good* iff there is a fixed k such that for each positive c there is an NCk circuit family that computes $g(n)$ such that $|g(n) - f(n)| < 1/2^{n^c}$. We will also say that an approximation algorithm is NC-good if it demonstrates that the quantity being approximated is NC-good. Our task will be to show that $S(a, b)$ is NC-good.

In this section we will give the scheme of approximating $S(a, b)$. Most technical details will be covered here, with the exception of some supporting material. Lemmas for the supporting material will be proved in section 4.

The approach is based on three facts. We will go into each of them in this and the next sections.

- The zeros of an integer polynomial can be isolated to a specified precision in NC. See [9].
- If $h = n^{O(1)}$, w is a complex constant, and $|r + w| > 2^{n^{O(1)}}$ for integers $1 \leq r \leq 2^n$, then sums of the form $\sum_{r=1}^{2^n} 1/(r + w)^h$ are NC-good. We note that w is treated as an indeterminate in actually working out the form of the approximation.
- If $0 \leq \gamma < 1$, β is real, and $|\beta| > 1/2^{n^{O(1)}}$, then $[0, 1]$ can be partitioned into $n^{O(1)}$ subintervals O_i such that for $s \in O_i$
$$\frac{1}{s - \gamma + \beta\iota}$$
has an NC-good approximation which is a polynomial in s with rational expressions in γ and β as coefficients.

We point out that the basic idea in both items two and three above is rescaling. Notice also that item three will permit NC-good approximation of certain integrals over the interval $[0, 1]$.

We proceed to describe the approximation scheme.

Eq. 1 can be written as

$$S(a, b) = \rho^{-(a+b)} \int_0^1 \frac{z^{-1} \cdot ds}{(z^a - 1/\rho^a)(z^{-b} - 1/\rho^b)} \qquad (2)$$

Let $\omega = \mathbf{e}(1/a)$ and $\nu = \mathbf{e}(1/b)$. We obtain the following partial fraction expansion for $S(a,b)$.

$$S(a,b) = \rho^{-(a+b)} \sum_{j=0}^{a-1} \sum_{k=0}^{b-1} \int_0^1 \frac{z^{-1} \cdot ds}{(z\omega^{-j} - 1/\rho)(z^{-1}\nu^{-k} - 1/\rho)} \tag{3}$$

Eq. 3 still appears unpromising, not least because the number of summands is ab.

Define $T_d(w)$ to be the sum of the first $d+1$ terms in the Taylor series for $\exp(w)$. It will be convenient to impose the lower bound of $4n < d$. Define $S_d(a,b)$ as

$$\rho^{-(a+b)} \sum_{j=0}^{a-1} \sum_{k=0}^{b-1} \int_0^1 \frac{T_d(-2\pi\iota s) \cdot ds}{(T_d(2\pi\iota(s - j/a)) - 1/\rho)(T_d(2\pi\iota(-s - k/b)) - 1/\rho)} \tag{4}$$

Lemma 2 *For any $c > 0$ there is a positive integer $d = n^{O(c)}$ such that $|S(a,b) - S_d(a,b)| < 1/2^{n^c}$.*

Proof : Since $ab = 2^{O(n)}$, it suffices to show that the absolute value of the difference of each summand integral in Eq. 3 and the corresponding summand in Eq. 4 is bounded above by $1/2^{n^c}$ for a choice of $d = n^{O(c)}$.

Note that $|z| = |\omega| = |\nu| = 1$, and that

$$|(z\omega^{-j} - 1/\rho)(z^{-1}\nu^{-k} - 1/\rho)| \geq 1/(ab)^2$$

These facts, and the rate of convergence of the Taylor series for $\exp(w)$ establish the lemma. □

By Lem. 2, we will henceforth assume that $d = n^{O(1)}$.

Let $\alpha_1, \ldots, \alpha_r$ be the distinct zeros of $T_d(w) - 1/\rho$. For the sake of notational simplicity, we will assume that these zeros are all simple, so that $r = d$. In fact, we can prove that the 'critical' zeros (to be defined later) are simple, and that simplicity of zeros is not an obstacle to showing that $S(a,b)$ is NC-good.

By Lem. 2, if we can show that $S_d(a,b)$ is NC-good, then we have shown that $S(a,b)$ is NC-good. The first step in this direction is the following fact.

Lemma 3 *The zeros of $T_d(w) - 1/\rho$ are NC-good.*

Proof : Neff [9] has shown that finding approximations to m bits of all the zeros of a degree d integer coefficient polynomial whose coefficients have absolute value at most 2^k can be computed by NC circuits of $\log^{O(1)}(m + d + k)$ depth and $(m_d + k)^{O(1)}$ size. It is also known [8], Thm. 4.6, that distinct zeros of such a polynomial are separated by at least $d^{-d} \cdot 2^{-2k}$. In our case $m = k = d = n^{O(1)}$. Notice that the multiplicities can be reported correctly by the NC circuit. □

Using partial fraction expansion again, we can rewrite $S_d(a, b)$ as

$$\rho^{-(a+b)} \sum_{j=0}^{a-1} \sum_{k=0}^{b-1} \sum_{p=1}^{d} \sum_{q=1}^{d} \int_0^1 \frac{\mu_{p,q} T_d(-2\pi\iota s) \cdot ds}{(2\pi\iota(s - j/a) - \alpha_p)(2\pi\iota(s - k/b) - \alpha_q)} \tag{5}$$

The $\mu_{p,q}$ are the partial fraction coefficients, which are rational expressions in the zeros.

Referring to Eq. 5, define $A_{j,k,p,q}$ as

$$\int_0^1 \frac{\mu_{p,q} T_d(-2\pi\iota s) \cdot ds}{(2\pi\iota(s - j/a) - \alpha_p)(2\pi\iota(s - k/b) - \alpha_q)} \tag{6}$$

Using Eq. 6, we can write $S_d(a.b)$ as

$$\rho^{-(a+b)} \sum_{j=0}^{a-1} \sum_{k=0}^{b-1} \sum_{p=1}^{d} \sum_{q=1}^{d} A_{j,k,p,q} \tag{7}$$

We now proceed to show that $S_d(a, b)$ is NC-good in two stages. First we will show that each $A_{j,k,p,q}$ is NC-good, then we show that the summation of the approximations according to Eq. 7 is NC-good.

Lemma 4 *For $0 \leq j < a$, $0 \leq k < b$, $1 \leq p, q \leq d$, $A_{j,k,p,q}$ is NC-good. If α_p is critical, then the resulting approximation has the form of*

$$(\ln(1 - k/b - \alpha'_q) - \ln(-k/b - \alpha'_q) \cdot \sum_{i=0}^{\ell} R_i$$

where each R_i is a ratio of polynomials in j, $\alpha'_q = \alpha_q/2\pi$ and all coefficients are independent of either j or k. If α_p is non-critical, then $\sum_{i=0}^{\ell} R_i$ can be replaced by a polynomial in j.

Proof : Note that the numerator of the integrand of Eq. 5 is a polynomial in s of degree $n^{O(1)}$ with coefficients that are rational expressions in $\alpha_1, \ldots, \alpha_d$. This means that it suffices to show that an integral A of the form

$$A = \int_0^1 \frac{s^m ds}{(2\pi\iota(s - j/a) - \alpha_p)(2\pi\iota(s - k/b) - \alpha_q)} \tag{8}$$

is NC-good, where $0 \leq m \leq d$.

By Lem. 3, the integrand of A is NC-good. Using the same kind of argument used to prove Lem. 2, we can continue the proof by working with an approximate integrand of A in which α_p and α_q are replaced by rational approximations. However, we will not further encumber notation by specially indicating this modification. From now on, we will let α_p, etc., stand for the approximations to the zeros.

We proceed to show that A in Eq. 8 is NC-good with the required form. We divide the treatment of A depending on whether or not α_p is critical.

Critical case. By Lem. 8, we know that there are only five possible critical zeros. Using the details from that Lemma, and Eq. 8, we reduce showing that A is NC-good to showing that an integral B of the form

$$B = \int_0^1 \frac{s^m ds}{(s - j/a + g + \beta\iota)(s - k/b - \alpha'_q)}$$

is NC-good. Here $\alpha'_q = \frac{\alpha_q}{2\pi\iota}$, and $\beta = \frac{-\mu}{2\pi}$, where μ is as in Lem. 8. Also note that $g = g'/2\pi$ with g' as in the Lemma. We have neglected the real term of $\nu/2\pi$ since $|\nu| < 2/2^d$, and we take $d > 4n$.

By Lem. 6, B has an NC-good approximation B' of the form

$$B' = \sum_{i=0}^{\ell} \int_{O_i} \frac{R_i s^m \cdot ds}{s - k/b - \alpha'_q}$$

By synthetic division, the only contribution to the approximation of B' that requires inspection is

$$\sum_{i=0}^{\ell} \int_{O_i} \frac{ds}{s - k/b - \alpha'_q} = \int_0^1 \frac{ds}{s - k/b - \alpha'_q} = \ln(1 - k/b - \alpha'_q) - \ln(-k/b - \alpha'_q)$$

Non-critical case. We assume that $|\alpha_p| \geq 4\pi$. Since

$$|\frac{2\pi\iota(s - j/a)}{\alpha_p} \leq 1/2$$

we have an NC-good approximation of

$$\frac{1}{2\pi\iota(s - j/a) - \alpha_p}$$

by geometric series expansion in powers of $\frac{2\pi\iota(s-j/a)}{\alpha_p}$. The remaining steps are now as in the critical case.
□

$B_{p,q}$ will designate the approximation to $A_{j,k,p,q}$ guaranteed by Lem. 4. We have suppressed j, k as indices because the form of $B_{p,q}$ depends on p and q but not on j or k.

Lemma 5 *$S_d(a, b)$ is NC-good.*

Proof : Recalling Eq. 7, we now know that

$$|S_d(a,b) - \sum_{p=1}^{d}\sum_{q=1}^{d}\sum_{j=0}^{a-1}\sum_{k=0}^{b-1} B_{p,q}| < 1/2^{n^c}$$

Therefore, it remains to show that

$$\sum_{p=1}^{d}\sum_{q=1}^{d}\sum_{j=0}^{a-1}\sum_{k=0}^{b-1} B_{p,q}$$

is NC-good. Since $p, q = n^{O(1)}$, we must show for each p and q, that the above sum is NC-good. We treat the summations over j, k by cases according to whether or not α_p and α_q are critical.

Both α_p and α_q are non-critical. By Lem. 4, $B_{p,q}$ is the product of a polynomial in j and $\ln(1 - k/b - \alpha'_q) - \ln(-k/b - \alpha'_q)$. The summation over j assumes a closed form as a rational expression in the limits of summation. Recall that the powers of j are bounded above by $n^{O(1)}$. Likewise, $|\alpha'_q| > 2$, and both $|1 - k/b|$ and $|k/b| < 1$, we see that the logarithmic factors are NC-good via Taylor series expansion for the logarithm.

α_p is critical. We will see that summation on k can be handled using the technique for summation on j.

The logarithmic factor does not depend on j. We want to approximate $\sum_{j=0}^{a-1} B_{p,q}$. We have to evaluate

$$\sum_{j=0}^{a-1}\sum_{k=0}^{\ell} R_i$$

with ℓ and R_i as in Lem. 4. The expressions R_i arise in the proof of Lem. 6. If we look at each of the subcases encountered in that proof, we see that except for Case $j \neq 0$, subcases $g = \pm 1$ and regions 1 and 3 of subcase $g = 0$, R_i is a polynomial in j, and summation is straightforward.

In the remaining cases, and noting the two remarks in the proof of Lem. 6, we can apply Lem. 10 to obtain NC-good approximations for the summation on j.

Finally, we can consider summation over k of the logarithmic contribution. If α_q is non-critical, then the logarithms have NC-good approximation via straightforward expansion of the Taylor series as previously described. If α_q is critical, then the range of summation can be broken into $n^{O(1)}$ octaves and an appropriate rescaling in each octave allows one to get an NC-good approximation via the Taylor series again. This is very similar to the strategy for summation over j in the α_p critical cases above.

□

We are now able to prove Thm. 1.

Proof : By Lem. 2 and Lem. 5, $S(a, b)$ is NC-good. The theorem follows from Lem. 1. □

4 Technical lemmas

4.1 The main approximation lemmas

The following lemma is the main approximation and is a precise reformulation of item 3 discussed at the start of section 3.

Lemma 6 *Let a be an n-bit integer, j an integer in the range $0 \leq j < a$, $g \in \{0, 1, -1\}$, and $1/2^{2n} < |\beta| < 1/2^{2n-1}$. Let $\ell = 2n$. The interval $[0, 1]$ can be partitioned into subintervals, $O_0, \ldots, O_\ell$ such that for any given $c > 0$ there is a polynomial $R_i \in \mathbb{Q}[s]$ such that over $s \in O_i$*

$$|\frac{1}{s - j/a + g + \beta\iota} - R_i(s)| < 1/2^{n^c}$$

The coefficients of R_i are independent of j. The subintervals O_i and polynomials R_i can be computed in NC2, although the degree of the polynomial governing circuit size will depend on c.

Proof : We point out to the reader that at two places we will make remarks that will be used in the final steps of the proof of Thm. 1, but are only observations in the context of this proof.

We divide the construction of the subintervals and polynomials into cases. In each case we will make an appeal to Lem. 9.

Case $j = 0$. We consider the subcases depending on g.
Subcase $g = 1$. Note that

$$1 + \beta^2 \leq |s + 1 + \beta\iota|^2 \leq 4 + \beta^2 \leq 4(1 + \beta^2)$$

This means that we can apply Lem. 9 without using octaves.

Subcase $g = 0$. $O_0 = [0, 1/2^\ell]$, and if $0 < i \leq \ell$, then $O_i = [1/2^{\ell-i+1}, 1/2^{\ell-i}]$. For $s \in O_i$ it is clear that the minimum of $|s + \beta\iota|^2$ occurs at $s = 1/2^{\ell-i+1}$, and the maximum occurs at $s = 1/2^{\ell-i}$. It is easy to check that the maximum is not more than twice the minimum, so we can apply Lem. 9.

Subcase $g = -1$. This is essentially subcase $g = 0$ under the change of variable $s' = s - 1$.

Case $j \neq 0$. Again, we consider three subcases depending on g. The $g = \pm 1$ subcases are relatively simple, so we dispose of them first. Now, we also must observe how j occurs in the approximation. This is necessary because j will enter into the scaling factor per Lem. 9.

Subcase $g = -1$. We use the change of variable $t = -s + 1 + j/a$. We have $s - 1 - j/a + \beta\iota = -(t - \beta\iota)$. Note that $t \in [j/a, j/a + 1]$. $O_0 = [j/a, j/a + 1/2^\ell]$, and if $0 < i \leq \ell$, then $O_i = [j/a + 1/2^{\ell-i+1}, j/a + 1/2^{\ell-i}]$. For $0 \leq i \leq \ell$, the minimum of $|t - \beta\iota|^2$ in O_i occurs at the low end of the subinterval, and the maximum occurs at the high end. It is easy to check that the maximum is not more than twice the minimum so we can apply Lem. 9. The scaling factor will involve $(j/a)^2 + \beta^2$ for O_0 and $(j/a + 1/2^{\ell-i+1})^2 + \beta^2$ for O_i, $i > 0$.

Remark We remark that the reciprocals of the two scaling factors above can be decomposed in partial fractions to expressions of the form $\frac{1}{j+w}$ such that the real part of w is non-negative. This allows application of Lem. 10 to summation of j from $j = 1$ to $a - 1$.

Subcase $g = 1$. Let $t = s + 1 - j/a$, and observe that $t \in [1 - j/a, 2 - j/a]$. This subcase can be treated in the same manner as $g = -1$.

Subcase $g = 0$. We first deal with the subinterval O_0. We partition $[0, 1]$ into three intervals that we will call regions.

Region 1 $s \in [0, j/a - |\beta|]$

Region 2 $s \in [j/a - |\beta|, j/a + |\beta|]$

Region 3 $s \in [j/a + |\beta|, 1]$

We first treat region 2. It is clear that the minimum of $|s - j/a + \beta\iota|$ is $|\beta|$ and the maximum is $\sqrt{2}|\beta|$. Lemma 9 applies here, and the resulting approximation is a polynomial in j/a.

Region 3 can be transformed into Region 1 via the change of variable $t = s - j/a - |\beta|$, so we concentrate on Region 1. Region 1 is partitioned into $\ell + 1$ subintervals $O_0, \ldots, O_\ell$ as follows. We start at the high end of the region and define $O_0 = [(1 - 1/2^\ell)(j/a - |\beta|), j/a - |\beta|]$. If $i \neq 0$, then $O_i = [(1 - 1/2^{\ell-i})(j/a - |\beta|), (1 - 1/2^{\ell-i+1})(j/a - |\beta|)]$. For $0 \leq i \leq \ell$, let g_i be the minimum of $|s - j/a + \beta\iota|^2$ over O_i, and G_i the maximum.

We claim that

$$|s - j/a + \beta\iota|^2 = (s - j/a)^2 + \beta^2$$

is monotone increasing as s goes from $j/a - |\beta|$ to 0. This is clear if we write $s = \mu(j/a - |\beta|)$, where $0 \leq \mu \leq 1$. Note that

$$|s - j/a - \beta\iota|^2 = ((1-\mu)j/a + \mu|\beta|)^2 + \beta^2$$

and that the derivative of $(1-\mu)j/a + \mu|\beta|$ is $-j/a + |\beta|$ which is negative because $j > 0$, and $1/a > |\beta|$.

We carry out a detailed analysis of g_i and G_i for $i \neq 0$. The case $i = 0$ is simpler. Let $x = 2^{i-1}j/a$. We have

$$g_i/\beta^2 = (Cx + 1 - \frac{1}{2^{\ell-i+1}})^2 + 1$$

and

$$G_i/\beta^2 = (2Cx + 1 - \frac{2}{2^{\ell-i+1}})^2 + 1$$

Now

$$x(C - \frac{1}{2^{\ell-i+1} \cdot x}) > x(C - a/2^\ell) > xC/2$$

This last inequality is far from sharp since $a < 2^n$ and $2^{2n-2} < 1/|\beta| < 2^\ell$. In any event, we get

$$g_i/\beta^2 > C^2x^2/4 + Cx + 2$$

We can overestimate G_i/β^2 by

$$(2Cx + 1)^2 + 1 = 4C^2x^2 + 4Cx + 1$$

We get

$$16G_i < g_i$$

We apply Lem. 9 with the scaling factor γ^2 for O_i of

$$\gamma^2 = (C^2x^2/4 + Cx + 2)\beta^2 = \frac{2^{2i-2}}{2^{2\ell}} \cdot (j/a + \frac{(1-\iota)2^\ell\beta}{2^{i-1}})(j/a + \frac{(1+\iota)2^\ell\beta}{2^{\ell-i}})$$

Remark The above scaling factors for each octave can be expressed by partial fractions in terms of ratios of the form $\frac{1}{j+w}$ such that $|j + w| > 1/2^{n^{O(1)}}$ (in fact, a $\Omega(1)$ lower bound holds.) This means that Lem. 10 can be applied to summation of these ratios over j from $j = 1$ to $a - 1$. □

4.2 The zeros of $T_d(w) - 1/\rho$

Lemma 7 *If w is a multiple zero of $T_d(w) - 1/\rho$, then $|w| = \Theta(d)$.*

Proof : w is a multiple zero iff $T_d(w) - \rho = 0$ and $T_d'(w) = 0$, where $T_d'(w)$ is the derivative of $T_d(w)$. These two equations imply that $w^d/d! = 1/\rho$, and Stirling's approximation implies that $|w|$ must be very close to D/e. □

Lemma 8 *If $d > \max\{32e, 2n+2\}$, $T_d(w) - 1/\rho = 0$, and $|w| < 4\pi$, then w has the following form*

$$w = \mu + (g'\pi + \nu)\iota$$

where μ and ν are real, $\mu = -1/ab + O(1/2^{4n})$, $|\nu| < 2/2^d$, and $g' \in \{0, \pm 2\}$. In addition, w is simple.

Proof : That w is simple follows from Lemma 7.

We need the following fact. If $|w| < 4\pi$, then

$$|T_d(w) - \exp(w)| < 1/2^d \tag{9}$$

If $d > 32e$, then Stirling's approximation gives for $k \geq d$,

$$|w|^k/k! \leq e^k(4\pi)^k/k! < (16e/k)^k < 1/2^k$$

and Eq. 9 clearly follows from this.

Write $w = u + v\iota$, where u, v are real. If w is a zero, then by Eq. 9 we have

$$|\rho - \exp(u) \cdot \exp(v\iota)| < 1/2^d \tag{10}$$

Let $\delta = \rho - \exp(u)\cos(v)$, and $\delta' = \exp(u)\sin(v)$. Separating real and imaginary parts in eq. 10, we get $|\delta'| < 1/2^d$ and $|\delta| < 1/2^d$. Since $\cos^2(u) + \sin^2(v) = 1$, we get

$$\exp(2u) = \rho^2 - 2\delta'\rho + \delta^2 + \delta'^2$$

From this we can conclude that

$$|\exp(2u) - \rho^2| < 3/2^d < 1/2^{2n} < 1/2^{4n}$$

Taking logarithms, we get

$$2u = \ln(1 - \delta'')$$

where $\delta'' = 2/ab \pm O(1/2^{4n})$. The claim for u is immediate from this and we set $\mu = u$.

We now know that $\exp(u) = 1 - 1/ab \pm O(1/2^{4n})$. This and $|\delta'| = |\exp(u)\sin(v)| < 1/2^d$ and $|\alpha_i| < 4\pi$ tell us that $v = g\pi + \nu$ such that $g' \in \{0, \pm 1, \pm 2\}$, and $|\nu| < 2/2^d$. However, $g' = \pm 1$ is ruled out, since then $|\delta| = |\rho - \exp(u)\cos(v)| > \rho$, which is impossible, and the lemma is proved. □

4.3 Octave rescaling

Lemma 9 *If w is a complex quantity, $\gamma > 1/2^{n^c}$ for some $c > 0$, and for some $C = n^{O(1)}$, $\gamma \leq |w| \leq C\gamma$, then $1/w$ has an NC-good approximation consisting of a sum of nonnegative powers of*

$$1 - \frac{|w|^2}{(C^2+1)\gamma^2}$$

Proof : We have (the bar designates complex conjugation)

$$\frac{1}{w} = \frac{\bar{w}}{|w|^2} = \frac{\bar{w}}{(C^2+1)\gamma^2(1-(1-\frac{|w|^2}{(C^2+1)\gamma^2})}$$

If $\gamma > 1/2^{n^c}$ for some $c > 0$, then since

$$1 - \frac{C^2}{C^2+1} \leq 1 - \frac{|w|^2}{(C^2+1)\gamma^2} \leq 1 - \frac{1}{C^2+1}$$

we have shown that $1/w$ is NC-good via an aproximation by a truncated geometric series in powers of $1 - \frac{|w|^2}{(C^2+1)\gamma^2}$. □

We will refer to $(C^2+1)\gamma^2$ as the scaling factor.

4.4 Summation by octaves

Lemma 10 *Let $N > 1$ be an integer, $n = \log N$, $c = n^{O(1)}$ and w a complex number. If $|k+w| > 1/2^{n^{O(1)}}$ for integers $1 \leq k \leq N$, then*

$$\sum_{k=1}^{N} \frac{1}{(k+w)^c}$$

is NC-good in terms of n.

Proof : Write $w = u + \iota v$, where u and v are real. We treat the case $u < 0$ in detail. The case $u \geq 0$ is simpler and can be treated in a similar manner.

Note since $|\frac{1}{k+w}| < 2^{n^d}$ for some $d > 0$, and $c = n^{O(1)}$ that we can apply Lem. 11 and assume that $c = 1$.

We start with

$$|k+w|^2 = (k+u)^2 + v^2 \tag{11}$$

Let k_0 be the integer in the summation range for which $|k+w|$ is minimum. Actually, if $-u$ is halfway between two integers there will be two such values of k. However, this is an inessential complication, so we will assume a unique k_0. If $k \geq k_0 + 1$ and $0 \leq x < y$, then certainly by Eq. 11, $|k+x|^2 < |k+y|^2$

and $|k+2y|^2 < 4|k+y|^2$. Likewise, if $k \leq k_0 - 1$, then $|k-x|^2 < |k-y|^2$ and $|k-2y|^2 < 4|k-y|^2$.

Partition the summation range into 'octaves'. $O_{+,i}$ will be the range from $k_0 + 2^{i-1}$ to $k_0 + 2^i - 1$, and $O_{-,i}$ will be the range from $k_0 - 2^{i-1}$ to $k_0 - 2^i + 1$. The outermost octaves may have fringes, but that won't affect the argument. Within any octave $O_{\pm,i}$, we know by Lem. 9 that $\frac{1}{k+w}$ can be approximated to within $1/2^{n^{O(1)}}$ using the sum of the first $n^{O(1)}$ terms of the geometric series in

$$1 - \frac{|k+w|^2}{17 \cdot |k_0 \pm 2^{i-1} + w|^2}$$

Now, each octave sum involving these powers can be expressed in closed form as a rational form in 2^i and w. These evaluations can clearly be done in NC, and the summation of these results for all octaves is also in NC, since $i = O(n)$. □

The next lemma is really included for completeness. It is often assumed in various forms in the practice of polynomial size approximations.

Lemma 11 *If a, b are complex numbers such that $3^{k+1} \cdot |a|^{2^{k+1}-1} \cdot |b| < 1$, then for $2^k \leq n < 2^{k+1}$,*

$$|a^n - (a+b)^n| < 3^{k+1} \cdot |a|^{2^{k+1}-1} \cdot |b|$$

Proof : First we will prove by induction on $1 \leq j \leq k$ that

$$|a^{2^j} - (a+b)^{2^j}| < 3^j \cdot |a|^{2^j - 1} \cdot |b|$$

By the triangle inequality, $|(a+b)^2 - a^2| \leq 2|ab| + |b|^2 < 3|ab|$. This takes care of $j = 1$. The induction argument essentially replicates this. Assume the result for $j < k$. Note that

$$(a+b)^{2^{j+1}} = (a^{2^j} + b_j)^2$$

where by induction hypothesis,

$$|b_j| < 3^j \cdot |a|^{2^j - 1} \cdot |b|$$

From this and the triangle inequality, we get

$$|a^{2^{j+1}} - (a+b)^{2^{j+1}}| < 2 \cdot 3^j \cdot |a|^{2^j} \cdot |a|^{2^j - 1} \cdot |b| + |b_j|^2$$

By assumption $|b_j| < 1$, so

$$|a^{2^{j+1}} - (a+b)^{2^{j+1}}| < 3 \cdot 3^j \cdot |a|^{2^{j+1}-1} \cdot |b|$$

which completes the induction.

In general, if $2^j < n < 2^{j+1}$, for $j \leq k$, then write $n = 2^j + q$, where $q < 2^j$. We use induction on j. Write $(a+b)^{2^j} = a^{2^j} + b_j$ and $(a+b)^q = a^q + b_q$. Using the triangle inequality, we get

$$|a^n - (a+b)^n| \leq |a|^q |b_j| + |a|^{2^j} |b_q| + |b_q||b_j|$$

From this, $|b_q|, |b_j| < 3^j \cdot |a|^{2^j - 1} \cdot |b| < 1$, and the induction hypothsis, we get the lemma by replacing each of the three right hand terms by the overestimate, $|a|^{2^j} \cdot 3^j \cdot |a|^{2^j - 1} \cdot b$. □

5 Open problems

The obvious question is whether or not the method of this paper extends to MI. There appears to be a serious technical complication in attempts made by the author to go beyond the decision problem CO. In effect, for MI the numerator of Eq. 1 will involve an 'entanglement' of a and b, and this leads to a breakdown in the approximation approach.

It may also be the case that the integral approximation by octaves has other applications in computer science.

References

[1] L. Adleman and K. Kompella. Using smoothness to achieve parallelism. In *Proc. 20th ACM STOC*, pages 528–538, 1988.

[2] P. Beame, S. Cook, and H. Hoover. Log depth circuits for division and related problems. *SIAM J. Comp.*, 15,4:994–1003, 1986.

[3] A. Borodin. On relating time and space to size and depth. *SIAM J. Comp.*, 6:733–744, 1977.

[4] S. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64:2–22, 1985.

[5] G. Davida and B. Litow. Fast parallel arithmetic via modular representation. *SIAM J. Comp.*, 20,4:756–765, 1991.

[6] R. Kannan, G. Miller, and L. Rudolph. Sublinear parallel algorithms for the greatest common divisor of two integers. In *Proc. 25th IEEE FOCS*, pages 7–11, 1984.

[7] B. Litow. On iterated integer product. *Inf. Proc. Lett.*, 42,5:269–272, 1992.

[8] M. Mignotte. *Mathematics for Computer Algebra.* Springer, 1992.

[9] C. Neff. Specified precision polynomial root isolation is in NC. *JCSS*, 48:429–463, 1994.

[10] J. Reif and J. Tygar. Efficient parallel pseudorandom number generation. *SIAM J. Comp.*, 17(2):404–411, 1988.

[11] W. Ruzzo. On uniform circuit complexity. *Journal of Computer and System Sciences*, 22:365–383, 1981.

[12] I. Wegener. *The Complexity of Boolean Functions.* Wiley-Teubner, 1987.