Referee Report of SICOMP submission Electronic Colloquium on Computational Complexity, Comment 3 on Report No. 009 (1998)

Parallel Complexity of Integer Coprimality

B. Litow

1 Summary

The author attempts to construct an NC algorithm for deciding whether two given integers a and b are relatively prime.

2 Recommendation

The paper is not acceptable for publication. The algorithm contains a flaw I believe to be fatal. In fact, I do not think that the author's approach, though innovative and promising at first sight, is viable.

The manuscript also has major stylistic deficiencies, which by themselves preclude it from journal publication: numerous little errors, bad use of notation, lack of overall structure, and poor writing in general.

2.1 The flaw in the algorithm

The fatal error occurs in Lemma 10. The list of forms the terms of $F_{j,k,p,q,g,h,i}$ can take is incomplete. In particular, the the argument of the first logarithm in the statement of the lemma can also take the form $(j/a-k/b+c-\alpha/2\pi\iota)$, where c is some easily computable rational constant depending on the term. Similarly, the argument of the second logarithm can have this form.

The reason is the following. The logarithmic terms come from the integrals

$$\int_{O_i} \frac{ds}{s-k/b-\alpha/2\pi\iota},$$

where O_i is one of the intervals defined in Lemma 7. Some of the intervals are independent of j but others (in fact, most of them) have end points of the form $j/a+c$. The latter leads to the logarithm of the above arguments after integration.

The correction in Lemma 10 fatally complicates the summation of the terms $F_{j,k,p,q,g,h,i}$ over j and k as needed in Lemma 11. It necessitates the evaluation of sums of the form

$$\sum_{j=0}^{a-1}\sum_{k=0}^{b-1} r(j)\cdot\ln(j/a-k/b+c-\alpha/2\pi\iota),$$

where r is a rational function of the form (31). Lemma 9 computes NC approximations to sums of that type that do not contain j/a in the argument of the logarithm. It uses rational approximations to the logarithm function in order to do so. Because of the essential singularity at zero, different rational expressions are needed for different ranges of the argument. This dependency becomes problematic when j/a appears in the argument. Which rational expressions we have to use now depends on the interval in which $j/a-k/b+c-\alpha/2\pi\iota$ falls.

In particular, if $c \ll 2^{-2n}$ there is an expression E which we should use for precisely those pairs (j,k) for which $j/a=k/b$. Note that the situation $c \ll 2^{-2n}$ does happen, and that the contribution of E to the approximation is actually large, so this case cannot be ignored. The pair $(0,0)$ always satisfies the condition $j/a=k/b$; there are other pairs (j,k) satisfying it iff a and b have a factor in common. Thus, computing the contribution of E in NC seems to entail deciding in NC whether a and b are relatively prime. The strategy becomes circular, to say the least.

ISSN 1433-8092

2.2 The failure of the approach

Variants of the author's approach seem to have the same problem. For example, approximating the integrand term $1/(s-k/b-\alpha/2\pi\iota)$ as in step 4 on page 15 instead of approximating the resulting integral, or computing the components of the integral (26) exactly and then approximating the resulting expression. In fact, I think the problem is inherent to the approach. The following explains why. It is a more general view of the above argument.

Given the positive integers a and b, the author considers the complex contour integral

$$\oint_{|z|=1} \phi_a(z)\phi_b(1/z)/z^2 dz.$$

He shows that its value is positive and bounded away from zero in case a and b are relatively prime, and that if vanishes otherwise. The idea is to approximate the value of the integral in NC closely enough so that the two cases can be distinguished.

The integrand contains the product of two functions, $\phi_a(z)$ and $\phi_b(1/z)$, where $\phi_d(z)$ is a rational function with poles on the regular d-gon centered at the origin, at distance about 2^{-2n} from the unit circle, and intersecting the positive real axis. All poles of $\phi_d(z)$ are of first order. The fact that the poles are that close to the unit circle makes that the integral is bounded away from zero in case a and b are relatively prime.

The author tries to approximate the integrand analytically. Because of the presence of the poles, there is no single analytic approximation that will work on the entire unit circle. In particular, at the points closest to the poles the radius of convergence will only be about 2^{-2n}. This implies that an exponential number of different approximations are necessary. The hope is that this exponential number of contributions has enough structure so that they can be summed in NC. This would be the case if only $\phi_a(z)$ or only $\phi_b(1/z)$ occurred in the integrand since the terms are periodic with period a or b respectively. However, the terms in the product of $\phi_a(z) \cdot \phi_b(1/z)$ have period $ab/\gcd(a,b)$. Summing them in NC seems to require computing $\gcd(a,b)$ in NC, a problem which is at least as hard as deciding whether a and b are relatively prime.

3 Final Comments

Although I am very sceptic, I am willing to referee new attempts to solve the problem. I do request, though, that the author discusses in detail how he tackles the issue I raised above.

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