Report on the paper
Deterministic Methods to Find Primes
of "D.H.J. Polymath"

This paper studies the problem of finding a prime number in the interval $[n, 2n]$ in time poly$(\log n)$. Note that by the prime number theorem a $(1/\log n)$ fraction of the numbers are prime and hence there is an easy randomized test: Pick a random $x \in [n, 2n]$ and check it for primality. The open question is whether we could derandomize this algorithm? The paper focuses on a decision version of this search question. Given an interval $[a, b] \subset [n, 2n]$ of size at most $n^{0.5+c}$ (where $c > 0$ is a constant), could we check whether there is a prime in $[a, b]$ in deterministic $n^{0.5-c}$ time? If we assume Cramer's conjecture then this decision problem is trivial. But even assuming the Riemann hypothesis an answer to this question is open. Thus, this decision problem could be considered at the frontier of known analytic number theory techniques.

The authors show how to check whether there are an odd number of primes in $[a, b]$ in determinisitic $n^{0.5-c}$ time. I find this result very interesting. This is a small but positive step towards the original decision problem. This seems to be the first positive development towards deterministically finding primes. As a bonus the authors could generalize their techniques to prove that the *prime polynomial* $P(t) := \sum_{\text{prime } p \in [a,b]} t^p$ modulo 2 has *circuit complexity* $n^{0.5-c}$.

I would like to accept this paper as it deals with a fundamental problem, identifies its natural restricted versions and makes interesting progress. The paper however needs several modifications. At some places the calculations are too dense, it would help if the gaps in the proofs are smoothened. The paper uses older techniques or results but does not cite clear references eg. "Dirichlet hyperbola method" and "Bezout's theorem". Finally, the paper does not clearly say who the authors are! It does refer to a website detailing the *Polymath project* but, I think, a list of names who contributed to the work should be given somehow.

Changes along the above lines and the following suggestions should be made.

1. abstract, last para: ''run time' to 'runtime'.

2. pg 2, para 2, line 2: 'Using the sieve...' to 'The sieve...'.

3. pg 3, para 4, line 4: You do not need 'at most' with the O-notation.

4. ... next line: remove the extra 'is'.

5. ... 3rd line: remove the extra 'that'.

6. ... next line: replace ‘using $O(\ldots)$ units of time’ by ‘in $O(\ldots)$ time’. Make this usage of ‘time’ consistent in the whole paper. Sometimes you use ‘work’; that should be changed to ‘time’ too.

7. Conjecture 1.1: replace ‘work’ by ‘time’. Make this change everywhere else.

8. pg 4, line 2: remove the extra ‘by’.

9. after defining $P_{a,b}$: you use P sometimes. It is better to explicitly define $P = P_{a,b}$ then.

10. Thm 1.3: replace ‘quantity’ by ‘polynomial’.

11. pg 5, line 3: the notation mod $2, g$ looks confusing in the text. Everywhere use either $(\mathrm{mod}\ 2, g)$ or mod $(2, g)$.

12. pg 5, para 2: The arguments here are quite dense. If you want to discuss this then do it more slowly. Also, replace ‘mod 2 and $g(t)$’ by (as remarked before) ‘mod $(2, g(t))$’.

13. pg 5, Sec 2: Give a proper definition of μ. Also, define $\omega(1) = 0$.

14. pg 6, first Eqn: This is mod 4, it will look better if you use $\equiv$ instead of $=$ and parenthesize mod 4.

15. ... 2nd line: correct to ‘so the RHS summand with $j \in [2, \infty)$ can be ...’. Add a space between ‘algorithm[1]’.

16. pg 6, 2nd last para, last line: replace c by c_0. Also give the calculation ‘Summing in d ...’.

17. ... next para: RHS of the equation should have x instead of n.

18. pg 7, para 1: give a reference for this version of ‘Dirichlet hyperbola method’.

19. pg 7, last line: ‘second term’ is actually ‘third term’ and ‘third’ is ‘fourth’.

20. pg 8, para 1: The line invoking ‘Bezout’s theorem’/‘level set’ is too dense. Give a reference and explain more.

21. Remark 2.3: It is too big and dense for a remark. Shouldn’t you make it a subsection or the last section? Also, what is ‘dyadic decomposition’?

22. pg 10, para 2: Shouldn’t ‘inhomogeneous quadratic forms’ be simply called ‘quadratic polynomials’?

23. ... next para: Add space between ‘algorithm[11]’.

24. Pf of Prop 3.2, line 2: replace ‘also’ by ‘as well’.

25. ... 3rd line: Add a space before ‘A brief ...’ and after the full-stop.

26. pg 11, the eqn before Eqn (3.2): Explain the ‘hyperbola method’ and how you get these double sums in t.

27. ... last para: ‘Proposition 2.2’ should be ‘3.2’.

28. pg 12: Give reference for ‘Holder’s inequality’ you use.

29. ... pf of Thm 1.3, first eqn: this is mod 4, it will look better if you use $\equiv$ instead of $=$ and parenthesize mod 4.

30. ... after this equation: Give a short calculation showing how $b - a = O(N^{0.5+c})$ implies $\sqrt{b} - \sqrt{a} = O(N^{c+o(1)})$.

31. pg 12, 2nd last para: Instead of ‘circuit complexity of $O(\ldots)$ using $O(\ldots)$ work.’ you should just say ‘circuit complexity of $O(N^{0.27+c+o(1)})$.’ and justify why there is a 0.27.

32. ... next para: What is x? you meant N? Add ‘... of the inner sum in Eqn. (3.3)’. The calculation of ‘Summing in d’ should be convincingly done.

33. references, [2]: author-names spelling and pg numbers.