Formalizing an analytic proof of the Prime Number Theorem *(extended abstract)*

Dedicated to Mike Gordon on the occasion of his 60th birthday

John Harrison

Intel Corporation, JF1-13
2111 NE 25th Avenue, Hillsboro OR 97124, USA
johnh@ichips.intel.com

1 Formalizing mathematics: pure and applied

I've always been interested in using theorem provers both for "practical" applications in formally verifying computer systems, and for the "pure" formalization of traditional mathematical proofs. I particularly like situations where there is an interplay between the two. For example, in my PhD thesis [5], written under Mike Gordon's supervision, I developed a formalization of some elementary real analysis. This was subsequently used in very practical verification applications [6], where in fact I even needed to formalize *more* pure mathematics, such as power series for the cotangent function and basic theorems about diophantine approximation.

I first joined Mike Gordon's HVG (Hardware Verification Group) to work on an embedding in HOL of the hardware description language ELLA. Mike had already directed several similar research projects, and one concept first clearly articulated as a result of these activities was the now-standard distinction between 'deep' and 'shallow' embeddings of languages [3]. Since I was interested in formalizing real analysis, Mike encouraged me to direct my attention to case studies involving arithmetic, and this was the starting-point for my subsequent research. Right from the beginning, Mike was very enthusiastic about my formalization of the reals from first principles using Dedekind cuts. Mike had been involved in Robin Milner's group developing the original Edinburgh LCF [4], a central feature of which was the idea of extending the logical basis with derived inference rules to preserve soundness. Now that Mike had applied the LCF approach to higher-order logic, suitable as a general foundation for mathematics, it was possible to extend this idea and even develop mathematical concepts themselves in a 'correct by construction' way using definitions. So a definitional construction of the reals fitted in very well with the ideals Mike had for the HOL project, an interest in applications combined with an emphasis on careful foundations that has now become commonplace.

In this paper I want to describe a formalization that was undertaken purely for fun, involving complex analysis [8] and culminating in a proof of the Prime Number Theorem. Nevertheless, it doesn't seem entirely far-fetched to imagine some "practical" applications of this result in the future. For example a weak form of the PNT is implicitly used to justify the termination of the breakthrough AKS primality test [1], and some simpler properties of prime numbers have been used in the verification of arithmetical algorithms by the present author [7]. But I certainly don't need to give any such justification, because Mike Gordon, as well as introducing me to the fascinating world of theorem proving, has always placed a welcome emphasis on doing "research that's fun".

2 Mathematical machinery versus brute force

Formalizing the PNT in itself is not a new accomplishment, since that has already been done very impressively by a team led by Jeremy Avigad [2]. However, that formalization was of the so-called "elementary" Erdös-Selberg proof — elementary in the sense that no higher analysis is used, not in the sense of simplicity. The usual proof in analytic number theory textbooks relies on Cauchy's residue theorem from complex analysis, and the fact that there are no zeros of the Riemann ζ-function for $\Re z \geq 1$. This analytic proof in itself is simpler and clearer than the elementary one, but at the price of requiring much more mathematical "machinery" as a precondition. For this reason, Robert Solovay has suggested an analytic proof of the PNT as a good challenge in the formalization of mathematics [12]. In the full version of this paper we plan to give a more detailed comparison of the elementary and analytic proofs and expand on some of the issues briefly sketched below.

Of course, it might sometimes make sense to play to the particular strengths of computer theorem provers by using a different proof from the one that humans might find appealing; cf. the comments in [13]. For example, see the proof of the Kochen-Specker paradox from quantum mechanics, worked out as an extended example in the present author's HOL Light tutorial. In presenting the proof informally, one would naturally reduce the number of cases by cleverly exploiting symmetry, whereas with a theorem prover it's simpler just to run through the cases by brute force. For a more challenging example, consider proving the associativity of the chord-and-tangent addition operation on elliptic curves. This has been done formally in Coq by Laurent Théry and Guillaume Hanrot [10], with some of the key parts using enormous algebraic computations that were on the edge of feasibility; indeed similar computational issues have obstructed a related project by Joe Hurd. When I mentioned the practical difficulties caused by this example to Dan Grayson, he suggested a more 'human-oriented' proof:

> But why not enter one of the usual human-understandable proofs that + is associative? Too many prerequisites from algebraic geometry? [. . .] The proof I like most is to use the Riemann-Roch theorem to set up a bijection between the rational points of an elliptic curve and the elements of the group of isomorphism classes of invertible sheaves of degree 0. That's a lot of background theory, probably too much for this stage of development, but then the "real" reason for associativity is that tensor product of R-modules is an associative operation up to isomorphism.

Indeed, it seems to the present author that formalizing mathematical machinery on that level is probably still many years away. So it is slightly depressing to reflect that we may be forced to formalize unnatural or 'hacky' proofs because not enough people are working on the systematic development of general mathematical machinery. The work reported in this paper is modest by comparison with the reasoning mentioned in that quotation, but still it represents a small step in the direction of formalizing non-trivial proofs in analytic number theory in the style of a mainstream textbook or research paper.

3 Formalizing Newman's proof of the PNT

There are numerous different analytic proofs of the PNT, but there seems to be a general consensus that an approach developed by Newman, just using Cauchy's integral formula for a simple bounded contour, is the simplest known. We took as our text to formalize the book by Newman himself [9], more specifically the "second proof" on pp. 72-74 using the analytic lemma on pp. 68-70. While Newman writes in a friendly and accessible style, he sometimes assumes quite a lot of background or leaves some non-trivial steps to the reader. The overall PNT proof naturally splits up into five parts, which are presented by Newman in somewhat distinct styles and with widely varying levels of explicitness.

1. The Newman-Ingham "Tauberian" analytical lemma.
2. Basic properties of the Riemann ζ-function and its derivative, including the Euler product.
3. Chebyshev's elementary proof that $\sum_{p\leq n} \frac{\log p}{p} - \log n$ is bounded.
4. Application of analytic lemma to get summability of $\sum_n (\sum_{p\leq n} \frac{\log p}{p} - \log n - c)/n$ for some constant c.
5. Derivation from that summability that $\sum_{p\leq n} \frac{\log p}{p} - \log n$ tends to a limit.
6. Derivation of the PNT from that limit using partial summation.

We have compared the main parts of our formalization against reverse-engineered TeX for corresponding passages in Newman's book (thanks to Freek Wiedijk for composing these!) The *de Bruijn factor* [11], the size ratio of the gzipped formal proof text versus the gzipped TeX (gzipped for a crude approximation to 'information content'), varies widely:

Part of proof	dB factor
1 Analytical lemma	8.2
2 ζ-function	81.3
3 Chebyshev bound	28.2
4 Summability	11.0
5 Limit	5.4
6 PNT	30.4

It is commonly found that the de Bruijn factor for typical formalizations is about 4, so these are very high. However, the really high figures are for parts where Newman is not really giving a proof in any sense. The quotations that follow are the sum total of Newman's text for parts 2, 3 and 6, which take over half of the 4939 lines in the complete HOL Light formalization. In no cases can Newman's passage really be called a proof, so the comparison is hardly fair:

2 Let us begin with the well-known fact about the ζ-function: $(z-1)\zeta(z)$ is analytic and zero free throughout $\Re z \geq 1$.

3 In this section we begin with Tchebyshev's observation that $\sum_{p \leq n} \frac{\log p}{p} - \log n$ is bounded, which he derived in a direct elementary way from the prime factorization on $n!$

6 The point is that the Prime Number Theorem is easily derived from '$\sum_{p \leq n} \frac{\log p}{p} - \log n$ converges to a limit' by a simple summation by parts which we leave to the reader.

If we restrict ourselves to parts 1, 4 and 5, the de Bruijn factor is about 8, still higher than normal, but not outrageously so. And indeed, although the proof did not present any profound difficulties, we found that it took more time to formalize Newman's text than we have grown to expect for other formalizations. This may indicate that Newman's style is fairly terse and leaves much to the reader (this does seem to be the case), or that in this area, we sometimes have to work hard to prove things that are obvious informally (this is certainly true for the winding number of the contour mentioned later). For instance, a simple transformation in part 4, reversing the order of summation in this double series for $\Re z > 1$, needed to be justified by a proof, even if not a very difficult one, whereas it is simply posited without comment by Newman:

$$f(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \Big(\sum_{p \leq n} \frac{\log p}{p} \Big) = \sum_{p} \frac{\log p}{p} \Big[\sum_{n \geq p} \frac{1}{n^z} \Big].$$

To give something of the flavour of the proof, the centerpiece of Newman's approach is the analytical lemma; this is the only part that uses non-trivial facts about the complex numbers and is thus the locus of the analytical 'machinery':

> **Theorem.** *Suppose $|a_n| \leq 1$, and form the series $\sum a_n n^{-z}$ which clearly converges to an analytic function $F(z)$ for $\Re z > 1$. If, in fact, $F(z)$ is analytic throughout $\Re z \geq 1$, then $\sum a_n n^{-z}$ converges throughout $\Re z \geq 1$.*

The proof involves applying Cauchy's integral formula round a contour and then performing some careful estimations of the sizes of the various line integrals involved. The contour we use, traversed counterclockwise, is shown in figure 1; this is slightly different from Newman's (using horizontal straight-line segments rather than continuing the arc of the circle), though only because we found it easier to understand informally, not because of any particular problem of formalization. The place where formalization presents a striking contrast with informal perception is that in order to apply Cauchy's integral formula, one must verify that the winding number of this contour, formally

$$\frac{1}{2\pi i} \int_{\gamma} dz/z$$

is indeed 1, indicating that the curve winds exactly once round the origin counterclockwise. Intuitively this is obvious. When formalized in the right way, it is not difficult, but it needs some systematic general lemmas about winding numbers of composite paths.

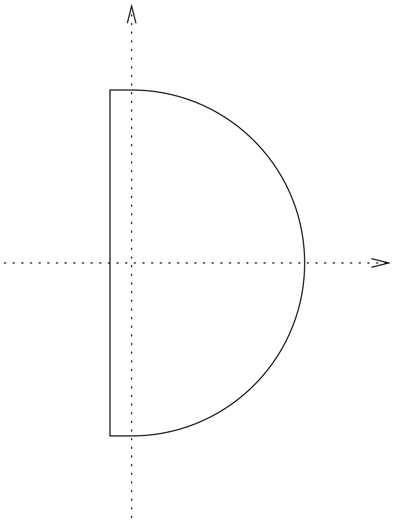

Fig. 1. Contour used in application of Cauchy's integral theorem

Nevertheless, despite these reservations, the proof presents no fundamental problems and we finally derive the Prime Number Theorem. The usual informal statement is that $\pi(n) \sim n/\log(n)$, where $\pi(x)$ denotes the number of prime numbers $\leq x$ and '$\sim$' indicates that the ratio of the two sides tends to 1 as $n \rightarrow \infty$. In our HOL formalization we do not use the auxiliary concepts $\pi(x)$ and '$\sim$' (though we easily could), but spell things out, where '&' is the type cast $\mathbb{N} \rightarrow \mathbb{R}$:

```
|- ((\n. &(CARD {p | prime p /\ p <= n}) / (&n / log(&n)))
     ---> &1) sequentially
```

References

1. M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.
2. J. Avigad, K. Donnelly, D. Gray, and P. Raff. A formally verified proof of the prime number theorem. *ACM Transactions on Computational Logic*, 2007.
3. R. Boulton, A. Gordon, M. Gordon, J. Harrison, J. Herbert, and J. Van Tassel. Experience with embedding hardware description languages in HOL. In V. Stavridou, T. F. Melham, and R. T. Boute, editors, *Proceedings of the IFIP TC10/WG 10.2 International Conference on Theorem Provers in Circuit Design: Theory, Practice and Experience*, volume A-10 of *IFIP Transactions A: Computer Science and Technology*, pages 129–156, Nijmegen, The Netherlands, 1993. North-Holland.
4. M. J. C. Gordon, R. Milner, and C. P. Wadsworth. *Edinburgh LCF: A Mechanised Logic of Computation*, volume 78 of *Lecture Notes in Computer Science*. Springer-Verlag, 1979.
5. J. Harrison. *Theorem Proving with the Real Numbers*. Springer-Verlag, 1998. Revised version of author's PhD thesis.

6. J. Harrison. Formal verification of floating point trigonometric functions. In W. A. Hunt and S. D. Johnson, editors, *Formal Methods in Computer-Aided Design: Third International Conference FMCAD 2000*, volume 1954 of *Lecture Notes in Computer Science*, pages 217–233. Springer-Verlag, 2000.
7. J. Harrison. Isolating critical cases for reciprocals using integer factorization. In J.-C. Bajard and M. Schulte, editors, *Proceedings, 16th IEEE Symposium on Computer Arithmetic*, pages 148–157, Santiago de Compostela, Spain, 2003. IEEE Computer Society. Currently available from symposium Web site at `http://www.dec.usc.es/arith16/papers/paper-150.pdf`.
8. J. Harrison. Formalizing basic complex analysis. In R. Matuszewski and A. Zalewska, editors, *From Insight to Proof: Festschrift in Honour of Andrzej Trybulec*, volume 10(23) of *Studies in Logic, Grammar and Rhetoric*, pages 151–165. University of Białystok, 2007.
9. D. J. Newman. *Analytic Number Theory*, volume 177 of *Graduate Texts in Mathematics*. Springer-Verlag, 1998.
10. L. Théry and G. Hanrot. Primality proving with elliptic curves. In K. Schneider and J. Brandt, editors, *Proceedings of the 20th International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2007*, volume 4732 of *Lecture Notes in Computer Science*, pages 319–333, Kaiserslautern, Germany, 2007. Springer-Verlag.
11. F. Wiedijk. The de Bruijn factor. See `http://www.cs.ru.nl/~freek/factor/`, 2000.
12. F. Wiedijk. *The Seventeen Provers of the World*, volume 3600 of *Lecture Notes in Computer Science*. Springer-Verlag, 2006.
13. L. Wos and G. W. Pieper. *A Fascinating Country in the World of Computing: Your Guide to Automated Reasoning*. World Scientific, 1999.