PROJECTS FOR "COMPUTATIONAL CONTENT OF PROOFS"

HELMUT SCHWICHTENBERG

Hilbert-Bernays Summer School, Göttingen, July 2016

Some of the projects below involve use the proof assistant Minlog (see `www.minlog-system.de` or Schwichtenberg (2006)). To download it execute `git clone http://www.math.lmu.de/˜minlogit/git/minlog.git`. Part of the distribution is a tutorial.

1. Constructive logic

Minimal logic for $\to, \forall$ when presented in natural deduction style is essentially a lambda-calculus, with formulas viewed as types (Curry-Howard correspondence). Classical logic can be naturally embedded. Constructive logic is obtained by adding a (proper, or strong) existential quantifier $\exists_x A$ (as opposed to the classical one defined by $\tilde{\exists}_x A := \neg\forall_x \neg A$)

Tasks, to be done informally and/or with Minlog, based on the lecture notes `www.math.lmu.de/~schwicht/lectures/logic/ss16/ml.pdf`:

(a) Properties of $\neg$, interaction of $\neg$ with $\to, \forall$.
(b) Interaction of $\exists$ with $\to, \forall$.
(c) Embedding classical logic: stability, interaction of $\tilde{\exists}$ with $\to, \forall$, drinker formula, Gödel-Gentzen translation.

2. Infinity of primes

Often in mathematics existence proofs are indirect, i.e., assuming that there is no solution of a problem one derives a contradiction. An example is Fürstenberg's (1955) topological proof of the infinity of primes; it is the fifth of "Six proofs of the infinity of primes" in Aigner and Ziegler's "Proofs from THE BOOK" (2004, Problem 1). Call a set X of natural numbers *open* if every $x \in X$ starts an arithmetic progression contained in X, i.e., $\forall_{x \in X} \exists_{b>0} \forall_n (x+bn \in X)$. Clearly arbitrary unions and finite intersections of open sets are open, i.e., we have a topology. Let Np be the set of multiples of a positive number p. Then Np is not only open but also closed, since it is the complement is a finite union of open sets. The only thing we assume on primes is that every number > 1 has a prime divisor. Now assume that there would be only finitely many primes $p_0, p_1, \dots, p_{m-1}$. Since $\bigcup_{l<m} Np_l$ is closed, its complement is open and therefore infinite, a contradiction.

Clearly such proofs only implicitly provide a solution, and it is a challenge to access the hidden computational content. In the present example this can be done by slightly modifying the argument. Call X *uniformly open* if $\exists_{b>0}\forall_{x\in X}\forall_n(x + bn \in X)$; the number b is a *witness* of uniform openness. Again arbitrary unions and finite intersections of uniformly open sets are uniformly open; witnesses in the latter case are finite products of the given witnesses. Since $\bigcup_{l<m} Np_l$ is uniformly closed with witness $b := \prod_{l<m} p_l$, its complement is uniformly open, and since it contains 1, it also contains $1 + b$. — This is the standard constructive proof of the infinity of primes.

Tasks.

(a) Present the informal proofs, both the original one and the one for uniform openness.
(b) Formalization (in `projfuerst.scm`) with the necessary background.
(c) Program extraction and discussion of the informal algorithm.

3. Modulus of continuity

It is shown that there is no (continuous) modulus-operator M assigning to every G of type two (i.e., $(\mathbf{N} \to \mathbf{N}) \to \mathbf{N}$) a modulus of continuity for G. The moral is that in constructive mathematics one has to careful when defining concepts: a continuous type two function has to be given together with its modulus of continuity. — The example is originally due to Kreisel, and has been worked on by Troelstra (1977) and Escardó and Xu (2015).

Tasks.

(a) Present the informal argument, based on Escardó and Xu (2015, p.4–5).
(b) Formalization (in `projmod.scm`) with the necessary background.

4. List reversal and decoration

This is an example of “program development by proof transformation”, based on what is done in the course. The standard proof of list reversal has as its computational content a quadratic algorithm. The decoration algorithm applied to the formalization of this proof transforms a universal quantifier $\forall_{v_1}$ into a “non-computational” one $\forall^{\mathrm{nc}}_{v_1}$. The new proof has as its content the well-known linear algorithm for list reversal, with its use of an accumulator.

Tasks.

(a) Formalization in Minlog, including `decorate`.
(b) Extraction, before and after decoration.
(c) Understanding and running the extracted terms.

References

Martin Aigner and Günter M. Ziegler. *Proofs from THE BOOK*. Springer Verlag, Berlin, Heidelberg, New York, 3rd edition, 2004.

Martin H. Escardó and Chuangjie Xu. The inconsistency of a Brouwerian continuity principle with the Curry-Howard interpretation. In T. Altenkirch, editor, *Proceedings TLCA 2015*, Leibniz International Proc. in Informatics, pages 1–12, 2015.

Harry Fürstenberg. On the infinitude of primes. *Amer. Math. Monthly*, 62: 353, 1955.

Helmut Schwichtenberg. Minlog. In F. Wiedijk, editor, *The Seventeen Provers of the World*, volume 3600 of *LNAI*, pages 151–157. Springer Verlag, Berlin, Heidelberg, New York, 2006.

Anna S. Troelstra. A note on non-extensional operations in connection with continuity and recursiveness. *Indag. Math.*, 39(5):455–462, 1977.

Mathematisches Institut der LMU, München, Germany