Applied Foundations: Proof Mining in Mathematics

Ulrich Kohlenbach

BRICS*
Department of Computer Science
University of Aarhus
Ny Munkegade
DK-8000 Aarhus C, Denmark

A central theme in the foundations of mathematics, dating back to D. Hilbert, can be paraphrased by the following question
'How is it that abstract methods ('ideal elements') can be used to prove 'real' statements e.g. about the natural numbers and is this use necessary in principle?'
Hilbert's aim was to show that the use of such ideal elements can be shown to be consistent by finitistic means ('Hilbert's program'). Hilbert's program turned out to be impossible in the original form by the seminal results of K. Gödel. However, more recent developments show it can be carried out in a partial form in that one can design formal systems $\mathcal{A}$ which are sufficient to formalize substantial parts of mathematics and yet can be reduced proof-theoretically to primitive recursive arithmetic **PRA**, a formal system usually associated with 'finitism'. These systems are based on the so-called binary König's lemma WKL which – in analytic terms – is just the amount of ineffective set theory needed to prove e.g. the Heine-Borel compactness of the unit interval $[0,1]$ which fails to hold in computable analysis (see [22] for a treatment of mathematics based on WKL).
Much larger parts of mathematics can be carried out in systems $\mathcal{A}^*$ which are not quite reducible to **PRA** but to first-order Peano arithmetic **PA**. These systems are based on so-called arithmetical comprehension which is just the amount of ineffective set theory needed to prove the sequential compactness of $[0,1]$ which is ineffective in an even stronger sense than WKL ([22],[6]).
Moreover, one can construct effective transformations of proofs in the systems mentioned into proofs in **PRA** respectively **PA** which preserve certain classes of formulas. Such results suggest to shift emphasis from purely foundational issues to mathematical applications.

*Basic Research in Computer Science, funded by the Danish National Research Foundation.

Already in the 50's G. Kreisel had asked
'What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?'
Kreisel proposed to apply proof theoretic techniques – originally developed for foundational purposes – to concrete proofs in mathematics which mathematicians could not 'unwind' themselves (see e.g. [20]).

Although Kreisel's idea of **unwinding proofs** has been applied e.g. to number theory ([19]), combinatorics ([1]) and algebra ([5]), the area of analysis (and in particular numerical functional analysis) is of particular interest. Here ineffectivity is due not only to the use of non-constructive logical reasoning but at the core of many principles (like compactness arguments) which are used to ensure convergence and which provably rely on the existence of non-computable reals. In mathematical terms this non-computability often is an obstacle to obtain a quantitative stability analysis and rates of convergence.
In recent years the author developed specially designed proof theoretic transformations to unwind proofs in analysis in a systematic way using – among other things – embbedings into systems based on semi-intuitionistic logic and so-called functional interpretations which translate proofs into terms built up out of functionals of finite types ([12],[13]). We call this approach **proof mining** (in analogy to the important area of 'data mining' in computer science). The goal of 'proof mining' is to transform prima facie ineffective proofs into new ones from which certain computational information can be read off which was not visible beforehand. The resulting proof can again be formulated in ordinary mathematical terms without reference to the techniques instrumental in finding it. This new proof, typically, will not and need not be constructive. In fact, only small parts of a given proof usually need to be considered at all. General logical theorems allow one to narrow down those parts which are critical for the computational information in question and provide an extraction algorithm. At the same time these logical theorems single out whole classes of lemmas which simply can be taken as axioms in the process of proof mining.
In applications to concrete proofs, the extraction procedure will not follow step by step the general algorithm provided by these metatheorems, but will use all kinds of mathematical optimizations possible in the situation at hand. Nevertheless, key steps in the analysis will typically correspond to transformations suggested by the logical method used.
We have carried out some case studies of proof mining which yielded not only new quantitative but even new qualitative results in approximation theory and fixed point theory.

These qualitative results are concerned with the independence of certain quantities such as rates of convergence from various parameters of the problem at hand. For instance in the area of metric fixed point theory, complicated functional theoretic embedding techniques have been used for some 20 years to establish certain (partial) uniformity results (see e.g. [8],[7],[10]) on the asymptotic regularity of nonexpansive mappings (see e.g. [9],[2]).

The logical approach not only avoids these techniques but gives qualitatively stronger forms of uniformity ([14],[15]) and easily extends (see recent joint work with Laurenţiu Leuştean [17]) to more general settings (directionally nonexpansive mappings in hyperbolic spaces) for which only rather limited results were known before ([10]).

In approximation theory proof mining resulted in quantitative bounds on strong unicity in Chebycheff approximation ([11]) as well as recently (joint work with Paulo Oliva) in L_1-approximation. In the latter case, the first explicit and effective (in all parameters) rate of strong unicity for best L_1-approximations of $f \in C[0,1]$ by polynomials of degree $\leq n$ was obtained ([16]) improving previously known ineffective results ([3],[18]). Using this result Oliva obtained the first complexity upper bound for the sequence of best L_1-approximations by polynomials ([21]).
We hope that these applications will convince the reader of the potential relevance of this project of 'applied foundations'.

References

[1] Bellin, G., Ramsey interpreted: a parametric version of Ramsey's theorem. In: Logic and computation (Pittsburgh, PA, 1987), pp. 17-37, Contemp. Math., 106, Amer. Math. Soc., Providence, RI, (1990).

[2] Borwein, J., Reich, S., Shafrir, I., Krasnoselski-Mann iterations in normed spaces. Canad. Math. Bull. **35**, pp. 21-28 (1992).

[3] Björnestål, B.O., Continuity of the metric projection operator I-III. The preprint series of Department of Mathematics. Royal Institute of Technology. Stockholm, TRITA-MAT **17** (1974), **20** (1974), **12** (1975).

[4] Cheney, E.W., Approximation Theory. AMS Chelsea Publishing, x+259 pp., 1966.

[5] Delzell, C., Kreisel's unwinding of Artin's proof-Part I. In: Odifreddi, P., Kreiseliana, 113-246, A K Peters, Wellesley, MA, 1996.

[6] Feferman, S., In the Light of Logic. Oxford University Press, 340 pp. (1998).

[7] Goebel, K., Kirk, W.A., Iteration processes for nonexpansive mappings. In: Singh, S.P., Thomeier, S., Watson, B., eds., Topological Methods in Nonlinear Functional Analysis. Contemporary Mathematics **21**, AMS, pp. 115-123 (1983).

[8] Edelstein, M., O'Brien, R.C., Nonexpansive mappings, asymptotic regularity and successive approximations. J. London Math. Soc. **17**, pp. 547-554 (1978).

[9] Ishikawa, S., Fixed points and iterations of a nonexpansive mapping in a Banach space. Proc. Amer. Math. Soc. **59**, pp. 65-71 (1976).

[10] Kirk, W.A., Nonexpansive mappings and asymptotic regularity. Nonlinear Anal. **40**, Ser. A: Theory Methods, pp. 323-332 (2001).

[11] Kohlenbach, U., New effective moduli of uniqueness and uniform a–priori estimates for constants of strong unicity by logical

analysis of known proofs in best approximation theory. Numer. Funct. Anal. and Optimiz. **14**, pp. 581–606 (1993).

[12] Kohlenbach, U., Analysing proofs in analysis. In: W. Hodges, M. Hyland, C. Steinhorn, J. Truss, editors, *Logic: from Foundations to Applications. European Logic Colloquium* (Keele, 1993), pp. 225–260, Oxford University Press (1996).

[13] Kohlenbach, U., Arithmetizing proofs in analysis. In: Larrazabal, J.M., Lascar, D., Mints, G. (eds.), Logic Colloquium '96, Springer Lecture Notes in Logic **12**, pp. 115-158 (1998)

[14] Kohlenbach, U., A quantitative version of a theorem due to Borwein-Reich-Shafrir. Numer. Funct. Anal. and Optimiz. **22**, pp. 641-656 (2001).

[15] Kohlenbach, U., Uniform asymptotic regularity for Mann iterates. Preprint 17pp., submitted (2002).

[16] Kohlenbach, U., Oliva, P., Proof mining in L_1-approximation. Preprint 35pp., to appear in: Ann. Pure Applied Logic.

[17] Kohlenbach, U., Leuştean, L., Mann iterates of directionally nonexpansive mappings in hyperbolic spaces. Preprint 32 pp. (2002).

[18] Kroó, A., On the continuity of best approximations in the space of integrable functions. Acta Mathematica Academiae Scientiarum Hungaricae **32**, pp. 331-348 (1978).

[19] Luckhardt, H., Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. J. Symbolic Logic **54**, pp. 234-263 (1989).

[20] Luckhardt, H., Bounds extracted by Kreisel from ineffective proofs. In: Odifreddi, P., Kreiseliana, 289–300, A K Peters, Wellesley, MA, 1996.

[21] Oliva, P., On the computational complexity of L_1-approximation. To appear in: Math. Logic Quaterly.

[22] Simpson, S.G., Subsystems of Second Order Arithmetic. Perspectives in Mathematical Logic. Springer-Verlag. xiv+445 pp. 1999.