

**PCC**

**Proof, Computation, Complexity**

**13 - 14 April 2007, Swansea, Wales**

Abstracts

# Control code logic

Jan Bergstra

This is joint work with Kees Middelburg (Amsterdam/Eindhoven). Control code logic (CCL) constitutes an attempt to turn the classical theory of T-diagrams into a conceptual theory of computer programs. Control code is software that can govern machine behavior without being a computer program per se. Working at the abstraction level of control codes one can develop a small amount of theory about executables, assemblers, interpreters and compilers.

The motivation for this work comes about from an involvement in several projects with computer software as a topic but uncommitted to any particular form of it. Themes are software patents and software asset management but also university timetabling organization and systematic budget design.

It will be shown how CCL might provide some common ground for these seemingly very different subjects.

# Content, Consistency and Constructivism

Christopher Broadbent

The so-called ‘crisis in foundations’ at the turn of the last century arose from the ‘discovery’ of problems with unrestricted comprehension principles, in particular Frege’s ‘Basic Law V’. The extent to which people viewed this as a genuine threat to our confidence in mathematical practise is unclear. Cantor was aware of the possibility of ‘inconsistent multiplicities’ and Zermelo was aware of the antinomy usually attributed to Russell prior to Russell; yet neither Zermelo nor Cantor saw this as a big problem.

As Kreisel has pointed out, Basic Law V is far from a paradigm example of a piece of trickery on the part of our ‘mathematical intuition’. It is the result of a confused assimilation of the notions of property, class, set and extension, a confusion unlikely to have been shared by the likes of Cantor who had a better understanding of the structures that he was studying. Today there is little doubt that the standard systems of set theory are consistent and this confidence comes largely from (informal) model theoretic considerations. Indeed our understanding of their ‘subject matter’ gives us confidence to note that they are, in a particularly strong sense, ‘true’. Perhaps the only system for which there is a genuinely open consistency question is Quine’s *New Foundations*, and this is precisely because it is based on the syntactic notion of ‘stratified formulae’ and lacks a clear structure as its subject matter.

Nevertheless, the ‘crisis’ did spawn a number of foundational programmes that seemed to have consistency as at least a partial motivation. The predicative systems of Weyl’s ‘*Das Kontinuum*’ and Russell’s ramified types are examples and to a lesser extent Brouwer’s intuitionism. However, it was Hilbert’s programme that had the idea of ‘consistency proof’ as its central theme and this is arguably where proof theory has its origins.

Hilbert wanted to prove the consistency of a formalised version of mathematical practise using only ‘finitist’ methods. Hilbert certainly spoke of providing a consistency proof by ‘indubitable’ means. Even if it were possible to realise a ‘finitist’ consistency result, it is far from obvious to what extent it would have been any clearer than a result proved from stronger

assumptions. It seems that the far more significant component of Hilbert's programme was a demonstration of the 'eliminability' of his transfinite  $\epsilon$ -symbols, that is a conservation result for arithmetic over his 'finitist' system. By the provable equivalence of  $\Pi_1^0$ -reflection to the consistency sentence for  $PA$  this amounts to the original aim of providing a finitist consistency proof.

Independently of the extent to which it is possible to achieve at least a partial realisation of Hilbert's original goals, it is interesting to ask whether there are any foundational reasons for wanting such a partial realisation. Such a motivation can arise from an attempt to fully understand exactly what the constructivist has in mind. One could perhaps identify three possible antirealist positions that could conceivably force one to a constructivist standpoint: ontological antirealism, denotational antirealism and semantic antirealism. The last was championed by Dummett who argued for the use of constructive (specifically intuitionistic) principles based on the claim that the meaning of all sentences, and in particular those of mathematics, should be given by assertibility conditions. He believed that the semantic antirealist position forced the conclusion independently of one's ontological stance.

I will argue that if semantic antirealism does commit one to constructivism it is likely to be something far closer to Hilbert's finitist position than something akin to Intuitionism or Constructive Recursive Mathematics, as there is a strong sense in which these are no better than classical systems from the perspective of the verificationist. Some elementary cut-elimination results for an infinitary system of first-order arithmetic help to illustrate this point.

# On the Proof Complexity of Deep Inference

Abstract

Paola Bruscoli and Alessio Guglielmi  
University of Bath

Bath BA2 7AY, United Kingdom  
cs.bath.ac.uk/pb/ and alessio.guglielmi.name/res

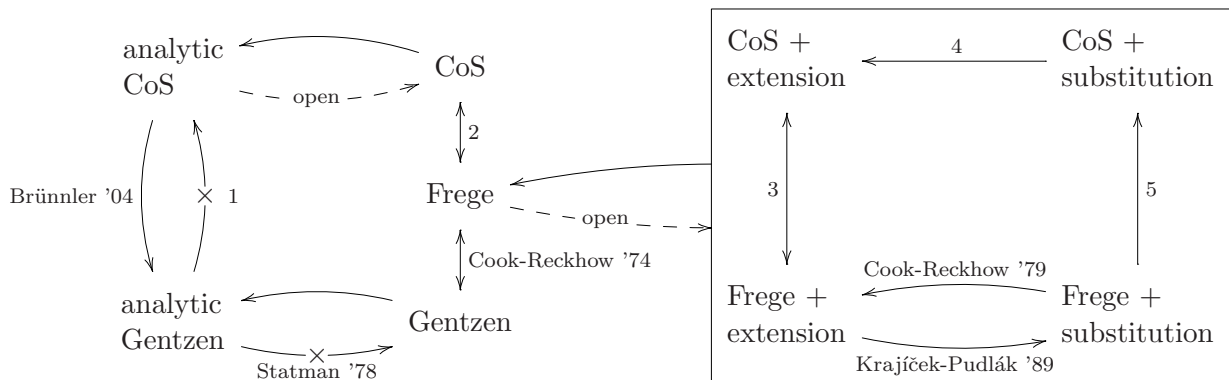
March 3, 2007

*Deep inference* is a relatively new methodology in proof theory, consisting in dealing with deductive system whose inference rules are applicable at any depth inside formulae [4]. We obtain two results about the proof complexity of deep inference:

- regarding proof complexity, deep-inference deductive systems are as powerful as Frege ones, including when extended with Tseitin’s extension rule and with the substitution rule;
- there are analytic deep-inference deductive systems that exhibit an exponential speed-up over analytic Gentzen systems that they polynomially simulate.

These results are established for the *calculus of structures*, or *CoS*, the simplest formalism in deep inference [5], and, in particular, for its deductive system *SKS*, introduced by Brünnler in [1] and extensively studied in the literature (see [4] for references).

Our contributions fit in the following picture.



The notation  $A \rightarrow B$  indicates that formalism  $A$  polynomially simulates formalism  $B$ ; crossed arrows indicate that it is known that this does not happen. Statman proved that analytic Gentzen can prove certain tautologies only with proofs that grow exponentially in their size, while Gentzen (with cut) can prove them with polynomial growth [7]. Cook and Reckhow proved that Frege and Gentzen formalisms are equivalent [2].

In the box at the right of the figure, ‘extension’ refers to Tseitin’s extension rule, and ‘substitution’ to the substitution rule. The works of Cook and Reckhow [3] and Krajíček

and Pudlák [6] established that Frege + extension and Frege + substitution are equivalent. It is immediate to see that these formalisms polynomially simulate Frege and Gentzen, which, in turn, polynomially simulate analytic Gentzen. It is a major open problem to establish whether Frege/Gentzen polynomially simulate Frege + extension/substitution.

In this work, we establish the following results, numbered as in the figure:

1. Analytic Gentzen does not polynomially simulate analytic CoS (in the form of system SKS without cut); in fact, the same class of tautologies studied by Statman in [7] admits polynomial proofs in analytic CoS.
2. CoS and Frege are equivalent; this could be easily inferred from [1], but we establish the correspondence directly.
3. There is a notion of (Tseitin's) extension for CoS, and CoS + extension is equivalent to Frege + extension.
4. There is a very natural notion of substitution for CoS, and CoS + substitution polynomially simulates CoS + extension.
5. Frege + substitution polynomially simulates CoS + substitution; this way, we know that all the extended formalisms are equivalent.

These results stand on a so-called robustness theorem for CoS, stating that all implicationally complete systems in CoS are equivalent. We expect to readily extend the results to different deep-inference formalisms from the calculus of structures.

Establishing whether analytic CoS polynomially simulates CoS is an open problem, and we conjecture that it is not the case.

## References

- [1] Kai Brünnler. *Deep Inference and Symmetry in Classical Proofs*. Logos Verlag, Berlin, 2004. <http://www.iam.unibe.ch/~kai/Papers/phd.pdf>.
- [2] Stephen Cook and Robert Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Proceedings of the 6th annual ACM Symposium on Theory of Computing*, pages 135–148. ACM Press, 1974.
- [3] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.
- [4] Alessio Guglielmi. Deep inference and the calculus of structures. Web site at <http://alessio.guglielmi.name/res/cos>.
- [5] Alessio Guglielmi. A system of interaction and structure. *ACM Transactions on Computational Logic*, 8(1):1–64, 2007. <http://cs.bath.ac.uk/ag/p/SystIntStr.pdf>.
- [6] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic*, 54(3):1063–1079, 1989.
- [7] Richard Statman. Bounds for proof-search and speed-up in the predicate calculus. *Annals of Mathematical Logic*, 15:225–287, 1978.

**Analyzing  $\Pi_4$ -reflection**  
Christoph Duchhardt  
University of Münster, Germany

**Abstract:** We show how to analyze proof-theoretically the theory of  $\Pi_4$ -reflection, which is a natural extension of Kripke-Platek set theory. This is done by iterating the idea of thinning out classes of model candidates.

# A Shoenfield-like bounded functional interpretation

Fernando Ferreira – Universidade de Lisboa

In 1958 [2], K. Gödel defined an interpretation of Peano arithmetic PA into a finite-type quantifier-free calculus  $\mathbb{T}$ , thereby achieving a reduction of the consistency of PA into a quantifier-free calculus of finite-type computable functionals. Gödel’s interpretation introduced a mathematical technique which can be explored in various ways. For instance, Gödel’s methods yield the following conservation result (below,  $\text{AC}_{\text{qf}}^\omega$  is the axiom of choice for quantifier-free matrices in all finite types):

**Theorem.** *If  $\text{PA}^\omega + \text{AC}_{\text{qf}}^\omega \vdash \forall x \exists y A(x, y)$ , where  $A$  is a quantifier-free formula with its variables as shown, then  $\text{PA}^\omega \vdash \forall x \exists y A(x, y)$ .*

Gödel’s original reduction is achieved by means of two steps. Firstly, PA is reduced to Heyting arithmetic HA via a double negation translation. Afterwards, HA is reduced to  $\mathbb{T}$  via an interpretation now known as Gödel’s *Dialectica* interpretation. In his book [3], J. Shoenfield found a direct reduction of the classical theory PA into  $\mathbb{T}$ . This reduction yields a quite straight proof of the above theorem.

Gödel’s two-step interpretation and Shoenfield’s direct reduction are based on a transformation of formulas that preserves set-theoretical truth and whose analysis of  $\forall \exists$ -formulas is given in terms of witnessing functionals. By maintaining Gödel’s functionals but relaxing their witnessing role to that of a mere bound, it is possible to define a Shoenfield-like transformation of formulas which interprets Peano arithmetic strengthened with a very general form of bounded collection. Even though this transformation does not preserve set-theoretical truth any longer, one does have the following “conservation” result:

**Theorem.** *If  $\text{PA}_{\sqsubseteq}^\omega + \text{mAC}_{\text{bd}}^\omega + \text{bC}_{\text{bd}}^\omega + \text{MAJ}^\omega \vdash \forall x \exists y A(x, y)$ , where  $A$  is a bounded formula with its free variables as shown, then one already has  $\text{PA}_{\sqsubseteq}^\omega \vdash \forall a \forall x \sqsubseteq a \exists y A(x, y)$ .*

In the above,  $\sqsubseteq$  is an *intensional* (i.e., rule-governed) version of M. Bezem’s notion of strong majorizability, and the notion of bounded formula appertains to this kind of majorizability. Since in types 0 and 1 every

element is majorizable, in these cases the above theorem indeed provides a conservation result (e.g., for  $\Pi_2^0$ -sentences of first-order arithmetic). The principle  $\text{mAC}_{\text{bd}}^\omega$  is a (monotone) version of choice for bounded matrices whereas  $\text{bC}_{\text{bd}}^\omega$  is the following version of collection for bounded matrices  $A$ ,

$$\forall x \trianglelefteq a \exists y A(x, y) \rightarrow \exists b \forall x \trianglelefteq a \exists y \trianglelefteq b A(x, y).$$

This form of bounded collection may be seen as a higher-order version of first-order bounded collection, as well as of a Brouwerian FAN type principle. The postulate  $\text{MAJ}^\omega$  states that  $\forall x \exists y (x \trianglelefteq y)$ . It should be noted that neither the full set-theoretic structure, nor Bezem's structure of the majorizable functionals, nor the (intensional or extensional) structure of continuous functionals is a model of  $\text{PA}_{\trianglelefteq}^\omega + \text{mAC}_{\text{bd}}^\omega + \text{bC}_{\text{bd}}^\omega + \text{MAJ}^\omega$ . It is difficult to find a model for this theory because its *flattening* – obtained by replacing the intensional  $\trianglelefteq$  by plain majorizability – is an inconsistent theory.

The above theorem can be also be obtained via a *detour* through intuitionistic logic using results of P. Oliva and the present author in [1].

Classically, weak König's lemma (WKL) is a consequence of  $\text{bC}_{\text{bd}}^\omega$  (for  $x$  of type 1 and  $y$  of type 0). Therefore, if we apply our conservation result to the subsystem  $\text{PRA}_{\trianglelefteq}^\omega$  of  $\text{PA}_{\trianglelefteq}^\omega$  (the former restricts Gödel's functionals to the *predicative* functionals in the sense of Kleene), we immediately get:

**Proposition.** *The theory  $\text{PRA}_{\trianglelefteq}^\omega + \text{WKL}$  is  $\Pi_2^0$ -conservative over  $\text{PRA}_{\trianglelefteq}^\omega$ .*

Using a flattening argument and an internal coding of the finite-type functionals in the sense of Kleene within  $\text{RCA}_0$ , we get H. Friedman's well-known conservation result of  $\text{WKL}_0$  over  $\text{RCA}_0$  (cf. [4]).

## References

- [1] F. Ferreira and P. Oliva. Bounded functional interpretation. *Annals of Pure and Applied Logic*, 135:73–112, 2005.
- [2] K. Gödel. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. *Dialectica*, 12:280–287, 1958. Translated in 1990 in “Kurt Gödel: Collected Works” Vol. II, Oxford University Press.
- [3] J. R. Shoenfield. *Mathematical Logic*. Addison-Wesley Publishing Company, 1967. Republished in 2001 by AK Peters.
- [4] S. G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Mathematical Logic. Springer, Berlin, 1999.

# An explanation for the commuting conversions

Gilda Ferreira  
 gildafer@cii.fc.ul.pt

In the natural deduction calculus, with the aim of obtaining the subformula property in normal proofs, there was the need to introduce some *ad hoc* conversions (connected to the connectives  $\perp$ ,  $\vee$  and  $\exists$ ): the *commuting conversions*.

According to Jean-Yves Girard *et al* (see [3], pages 74 and 80), ‘the elimination rules [of the connectives above] are very bad’ and referring to the commuting conversions ‘one tends to think that natural deduction should be modified to correct such atrocities’.

In 2006, Fernando Ferreira (see [1]) suggested a way of avoiding the *bad* connectives and consequently the commuting conversions in the intuitionistic propositional calculus, embedding it into a calculus with only two connectives: the conditional and a second-order universal quantifier. The latter is only instantiated by atomic formulas.

More recently in a joint work with Fernando Ferreira [2], we showed that the above embedding can be extended to the predicate calculus, i.e. predicate calculus can be embedded into atomic QSOL<sup>i</sup>, a second-order calculus whose connectives are the conditional and the first and second-order universal quantifiers, being the *bad* connectives absent. As a consequence, there are no commuting conversions in the statement of the normalization theorem.

An interesting question may be posed: how are the commuting conversions translated into atomic QSOL<sup>i</sup>? In answering this question, we discovered - in a quite natural way - an explanation for the commuting conversions.

Let us consider the three commuting conversions (c.c.) of the intuitionistic predicate calculus:

1) conversion  $\perp E$

$$\frac{\begin{array}{c} \vdots \\ \frac{\perp}{C} \perp E \\ \hline D \end{array} \quad \begin{array}{c} \vdots \\ r \end{array}}{\quad} \quad \text{c.c.} \quad \rightsquigarrow \quad \frac{\begin{array}{c} \vdots \\ \frac{\perp}{D} \perp E \end{array}}{\quad}$$

2) conversion  $\vee E$

$$\frac{\frac{\frac{\vdots}{A \vee B} \quad \frac{\frac{\vdots}{[A]}{C} \quad \frac{\vdots}{[B]}{C}}{C} \vee E \quad \vdots}{D} r}{c.c.} \rightsquigarrow \frac{\frac{\frac{\vdots}{A \vee B} \quad \frac{\frac{\vdots}{[A]}{C} \quad \frac{\vdots}{[B]}{C}}{D} r \quad \frac{\frac{\vdots}{[B]}{C} \quad \frac{\vdots}{[A]}{C}}{D} r}{D} \vee E}{c.c.} \rightsquigarrow$$

3) conversion  $\exists E$

$$\frac{\frac{\frac{\vdots}{\exists x A} \quad \frac{\frac{\vdots}{[A]}{C}}{C} \exists E \quad \vdots}{D} r}{c.c.} \rightsquigarrow \frac{\frac{\frac{\vdots}{\exists x A} \quad \frac{\frac{\vdots}{[A]}{C} \quad \frac{\vdots}{[A]}{D}}{D} r}{D} \exists E}{c.c.} \rightsquigarrow$$

where r stands for an elimination rule with principal premise  $C$ .

Considering the *redex* of a c.c. as the configuration on the left-hand side, the *contractum* as the configuration on the right-hand side and the formulas  $C$  and  $D$  as, respectively, the principal premise and the conclusion of the c.c., we show the following:

*If one considers the conclusion of a commuting conversion as a block (in a precise sense described in [2]) then from the canonical translation of the redex of the commuting conversion into atomic QSOL<sup>i</sup> we get, through the application of ‘standard conversions’, the canonical translation of the contractum of the commuting conversion.*

#### References

- [1] F. Ferreira, Comments on Predicative Logic. *Journal of Philosophical Logic*, 35, pp. 1-8, 2006.
- [2] G. Ferreira and F. Ferreira, A Study on Commuting Conversions, submitted for publication.
- [3] J.-Y. Girard, Y. Lafont and P. Taylor. *Proofs and Types*. Cambridge University Press, 1989.

# A constructive version of the Mean Ergodic Theorem

Philipp Gerhardy  
Department of Philosophy  
Carnegie Mellon University  
Pittsburgh, USA

March 7, 2007

'Proof mining' is the subfield of mathematical logic is the subfield of mathematical logic that is concerned with the extraction of additional information from proofs – even ineffective proofs! – in mathematics and computer science. Examples of such additional information are (1) computable realizers and bounds, (2) uniformities (i.e. independence of such realizers and bounds from certain parameters of the theorem), and (3) weakening of the premises of the theorem (e.g. elimination of compactness assumptions). In recent years, Kohlenbach et al. have developed very general metatheorems that (1) characterize classes of theorems and proofs for which such extractions can be carried out, (2) a-priorily classify the kind of bounds and uniformities that can be obtained, and (3) describe an actual algorithm to carry out such extractions (see e.g. [4, 3, 1]). Along with developing these metatheorems, Kohlenbach et al. have carried out a number of case studies in functional analysis (see [2] for a survey).

We present a general metatheorem that allows to treat proofs, i.e. extract effective uniform bounds, in the formal system  $\mathcal{A}^\omega[X, \langle \cdot, \cdot \rangle]$ . Here,  $\mathcal{A}^\omega$  is classical analysis in all finite types, i.e.  $\text{PA}^\omega$  (= Peano arithmetic in all finite types) + DC (= the axiom schema of dependent choice).  $[X, \langle \cdot, \cdot \rangle]$  denotes the extension of  $\mathcal{A}^\omega$  with an abstract Hilbert space  $(X, \langle \cdot, \cdot \rangle)$  by adding a new type  $X$ , as well as new constants and axioms that characterize Hilbert spaces. Note, that no separability assumptions are made about the space  $(X, \langle \cdot, \cdot \rangle)$ .

We then sketch an application of this metatheorem to a proof of the Mean Ergodic Theorem. This application is joint work with Jeremy Avigad and Henry Towsner.

Let  $T : X \rightarrow X$  be a linear, nonexpansive map on a Hilbert space  $X$ , and  $f \in X$

any element of that space. Define  $A_n f := \frac{1}{n+1} \sum_{i=0}^{n-1} T^i f$ .

The Mean Ergodic Theorem states the following:

**Theorem 1.**

$$\forall f \in X, T : X \rightarrow X, \varepsilon > 0 \exists n \in \mathbb{N} \forall m \in \mathbb{N} \\ (T \text{ n.e.} \wedge m > n \rightarrow \|A_m f - A_n f\| \leq \varepsilon).$$

It is easy to show that constructively one cannot achieve a full rate of convergence, so we consider the following classically equivalent but constructively weaker version:

**Theorem 2.**

$$\forall f \in X, T : X \rightarrow X, \varepsilon > 0, M : \mathbb{N} \rightarrow \mathbb{N} \exists n \in \mathbb{N} \\ (T \text{ n.e.} \wedge M(n) > n \rightarrow \|A_{M(n)} f - A_n f\| \leq \varepsilon).$$

The function  $M$  is called a counterexample function, so the theorem asserts that there is no counterexample to the convergence of  $A_n f$ , which classically is equivalent to full convergence.

The metatheorem now predicts that one can extract a bound  $N(\varepsilon, b, M)$  on  $n$  not depending on the space  $(X, \langle \cdot, \cdot \rangle)$  and only depending on  $f, T$  via a bound  $b$  on  $\|f\|$ . We will sketch the main ideas of the extraction and present the explicit bounds.

## References

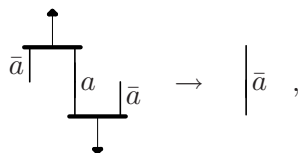
- [1] P. Gerhardy and U. Kohlenbach. General logical metatheorems for functional analysis, 2006. To appear in: *Trans. Am. Math. Soc.*
- [2] U. Kohlenbach. Effective bounds from proofs in abstract functional analysis. In *CiE 2005 New Computational Paradigms: Changing Conceptions of What is Computable*. Springer Publisher, 2005.
- [3] U. Kohlenbach. Some logical metatheorems with applications in functional analysis. *Trans. Amer. Math. Soc.*, 357:89–128, 2005.
- [4] U. Kohlenbach and P. Oliva. Proof mining: a systematic way of analyzing proofs in mathematics. *Proc. Steklov Inst. Math*, 242:136–164, 2003.

# Normalisation Control in Deep Inference Via Atomic Flows

Alessio Guglielmi and Tom Gundersen  
University of Bath  
Bath BA2 7AY, United Kingdom  
<http://alessio.guglielmi.name/res> and  
<http://teg.jklm.no/research>

March 3, 2007

We are interested in the essence of the relation between axioms and cuts. The left part of the following diagram illustrates how an atom  $a$  is produced by an axiom and consumed by a cut below it.

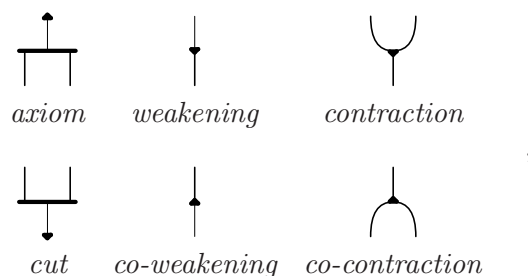


In multiplicative linear logic's proof nets [3], the diagram can be streamlined as on the right, and this forms the basis of normalisation. However, proof nets are not deductive, and multiplicative linear logic is not very expressive; as a matter of fact, the situation is considerably more complicated for richer logics in deductive formalisms like the sequent calculus. The possibly non-multiplicative nature of a logic and the 'bureaucracy' of deductive formalisms conspire against simplicity. In this work we show a technique for designing and proving properties of normalisation procedures that is rather independent of syntax, and, in essence, based only on the 'causality' relation between axioms and cuts, as shown above [4].

We show the power of our technique by adopting it to control normalisation in the calculus of structures, which is a formalism with deep inference, *i.e.*, the ability of performing inference inside formulae. The calculus of structures generalises most deductive formalisms, and normalisation is, consequently, more challenging. We prove a normalisation result that is more general than cut elimination and that entails it. We work on generic derivations, *i.e.*, chains of inference steps from a premiss  $R$  to a conclusion  $T$ , where  $R$  and  $T$  are propositional formulae. We show that we can *streamline* any such derivation, *i.e.*, we can remove all causal dependencies between axioms and cuts of the kind depicted above on the left.

The novelty of our technique is in the use of *atomic flows*, which are diagrams expressing *only* the structural information in derivations, in particular the causality relations between axioms and cuts, which we want to streamline. Atomic flows are made out of the following

six building blocks,



each corresponding to a structural inference rule. In addition to the normal inference rules, we have co-weakening and co-contraction which are the up-down duals of respectively weakening and contraction.

Our diagrams are close relatives of Buss’s flow graphs [2], in their atomic restriction, but we use them more like proof nets and interaction combinators [3, 5]. By establishing soundness properties, which ensure our ability to recover derivations from atomic flows, we can reason exclusively on atomic flows, in a completely syntax-independent way. This ability is crucial to control the intricacies of such a general normalisation theorem. The biggest problem, as expected, comes from contraction, which creates loops and proof complexity.

Atomic flows allow us to design normalisation procedures by providing for convenient induction measures. The bulk of derivation rewriting is performed by an operation of *substitution*, which constitutes in slightly altering a derivation around the matching axiom and cut, and plugging one altered derivation into the other. In principle, this is very similar to normalisation in natural deduction. To the best of our knowledge, this idea has been found by Alwen Tiu and then employed by Brünnler in [1] to prove cut elimination in the calculus of structures. In our case, the idea allows us to dispense entirely with the usual case analysis and permutation of rules, which is the standard (unpleasant) routine in cut elimination proofs in the sequent calculus and elsewhere. At a deeper level, we are led to believe that the success of normalisation stems less than it is usually believed from the mutual ‘harmony’ between logical rules. In fact, in this work, there is no consideration whatsoever for this issue, although the good design of logical rules still plays a role in certain ‘stability’ properties of atomic flows.

## References

- [1] Kai Brünnler. Atomic cut elimination for classical logic. In M. Baaz and J. A. Makowsky, editors, *CSL 2003*, volume 2803 of *Lecture Notes in Computer Science*, pages 86–97. Springer-Verlag, 2003. <http://www.iam.unibe.ch/~kai/Papers/ace.pdf>.
- [2] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53(1):75–102, 1991.
- [3] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.
- [4] Alessio Guglielmi and Tom Gundersen. Normalisation control in deep inference via atomic flows. Submitted. <http://cs.bath.ac.uk/ag/p/NormContrDIAtF1.pdf>, 2007.
- [5] Yves Lafont. Interaction combinators. *Information and Computation*, 137:69–101, 1997.

## **Abstract: $\Pi_2^1$ -comprehension and the property of Ramsey**

We show that a theory of autonomous iterated Ramseyness based on second order arithmetic is proof-theoretically equivalent to  $\Pi_2^1$ -comprehension.

The property of Ramsey is defined as follows. Let  $X$  be a set of real numbers, i.e. a set of infinite sets of natural numbers. We call a set  $H$  of natural numbers homogeneous for  $X$  if either all infinite subsets of  $H$  are in  $X$  or all infinite subsets of  $H$  are not in  $X$ .  $X$  has the property of Ramsey if there exists a set which is homogeneous for  $X$ .

The property of Ramsey is considered in reverse mathematics to compare the strength of subsystems of second order arithmetic.

To characterize the system of  $\Pi_2^1$ -comprehension in terms of Ramseyness we introduce a system of autonomous iterated Ramseyness, called  $R$ -calculus. We augment the language of second order arithmetic with additional set terms (called  $R$ -terms)  $R\vec{x}X\phi(\vec{x}, X)$  for each first order formula  $\phi(\vec{x}, X)$  (where  $\phi$  may contain further  $R$ -terms). The  $R$ -calculus is a system which comprises comprehension for all first order formulas (which may contain  $R$ -terms or other set parameters) and defining axioms for the  $R$ -terms which claim that for each  $\vec{x}$ , we can remove finitely many elements from the set  $R\vec{x}X\phi(\vec{x}, X)$  such that the remaining set is homogeneous for  $\{X \mid \phi(\vec{x}, X)\}$ . We show that the  $R$ -calculus proves the same  $\Pi_1^1$ -sentences as  $\Pi_2^1$ -comprehension.

Christoph Heinatsch

Institut für Mathematische Logik und Grundlagenforschung

Einsteinstr. 62

48149 Münster, Germany

e-mail: heinatc@math.uni-muenster.de

# A way around Luckhardt's elimination of extensionality procedure in the mining of proofs that use the non-standard analytical axiom **F**

Mircea–Dan Hernest

01 March 2007

Let  $\Delta, \Delta' \equiv \{ \forall x^\rho \exists y \leq_\sigma r x \forall z^\tau B^{\text{nc}}(x, y, z) \}$  be two distinct sets of sentences of this particular shape, where  $B^{\text{nc}}$  is a purely-ncm formula, i.e., it may contain only ncm quantifiers. Moreover, the elements of  $\Delta$  are restricted to formulas in which all positively (ncm-)universal and negatively (ncm-)existential quantified variables have type degree at most 2 and also all positively (ncm-)existential and negatively (ncm-)universal quantified variables have type degree at most 1. Hence in particular, the regularly universal quantified variables  $x^\rho$  and  $z^\tau$  have the restriction  $dg(\rho), dg(\tau) \leq 2$ , and also the regularly existential quantified variable  $y^\sigma$  has the restriction  $dg(\sigma) \leq 1$ . Let  $\mathcal{S}^\omega$  denote as usual the full *ZFC* set-theoretic type structure. We further assume that  $\mathcal{S}^\omega \models \Delta_{\text{reg}}$ , where  $\Delta_{\text{reg}} \equiv \{ \forall x^\rho \exists y \leq_\sigma r x \forall z^\tau B(x, y, z) \}$  is the direct regular-quantifier translation of  $\Delta$  (here  $B$  is the usual full regular-quantifier translation of  $B^{\text{nc}}$ , obtained by replacing  $\bar{\forall}$  with  $\forall$  and  $\bar{\exists}$  with  $\exists$ ). Let also  $\mathcal{M}^\omega$  denote Bezem's type structure of all strongly majorizable functionals, as usual. The formulas of  $\Delta'$  are restricted only by  $\mathcal{M}^\omega \models \Delta'_{\text{reg}}$ . Let  $\text{WeZ}_m^\exists, \text{WeZ}_m^{\exists, \text{nc}}, \text{WeZ}_m^{\exists, \text{nc}, \text{c}^+}$  be the classical arithmetics for light monotone Dialectica from Chapter 1 of [1] and also let  $\text{PbZ}, \text{PbZ}^{\text{c}^+}$  be the polynomial classical arithmetics from Chapter 3 of [1]. We further assume that  $\text{WeZ}_m^{\exists, \text{nc}, \text{c}^+}$  and  $\text{PbZ}^{\text{c}^+}$  no longer contain any implicit  $\Delta$ -kind of axiom set and for simplicity also not any kind of  $\Pi$  axiom set<sup>1</sup>.

If instead of a syntactic verifying proof, a simple guarantee that the verification holds in the full set-theoretic type structure  $\mathcal{S}^\omega$  suffices, then the

---

<sup>1</sup>We leave as an easy exercise to the reader that one can add also an axiom set  $\Pi \equiv \{ \forall b B^{\text{nc}}(b) \mid \mathcal{S}^\omega \models \forall b B(b) \}$  to which the same type restrictions as for  $\Delta$  apply, see Section 3.2 of [1] for details.

following extraction theorems can be established in the spirit of Theorem 4.9 of [3].

**Theorem 0.1** Let  $A_1(x^\mu, k^\iota, y^\delta, z^\gamma)$  be a quasi-purely-existential formula of  $\text{WeZ}_m^{\exists, \text{nc}}$  with  $x, k, y, z$  all its free variables, i.e.,  $A_1 \equiv \exists v A^{\text{nc}}(x^\mu, k^\iota, y^\delta, z^\gamma, v^\alpha)$ , and moreover such that  $dg(\delta) \leq 1, dg(\gamma), dg(\alpha) \leq 2$  and further all positively **ncm**-universal and negatively **ncm**-existential quantified variables of  $A^{\text{nc}}$  have type degree at most 1 and also all positively **ncm**-existential and negatively **ncm**-universal quantified variables of  $A^{\text{nc}}$  have type degree at most 2. Let  $s^{(\mu)\iota\delta}$  be a closed term of  $\text{WeZ}_m^{\exists}$ . Let  $\Delta$  and  $\Delta'$  be the explicit sets of axiom sentences defined above (recall that  $\mathcal{S}^\omega \models \Delta_{\text{reg}}$  and  $\mathcal{M}^\omega \models \Delta'_{\text{reg}}$ ). Then there exists an (light monotone Dialectica) algorithm which from a given proof

$$\text{WeZ}_m^{\exists, \text{nc}, \text{c}^+} + \Delta + \Delta' \vdash \forall x^\mu \forall k^\iota \forall y \leq_\delta s x k \exists z^\gamma A_1(x, k, y, z) \quad (1)$$

produces the the closed term  $\mathfrak{t}^{(\mu)\iota\gamma}$  of  $\text{WeZ}_m^{\exists}$  such that

$$\mathcal{S}^\omega \models \forall x^\mu \forall k^\iota \forall y \leq_\delta s x k \exists z \leq_\gamma \mathfrak{t} x k \widetilde{A}_1(x, k, y, z) \quad (2)$$

where  $\widetilde{A}_1(x, k, y, z) \equiv \exists v A(x, k, y, z, v)$  is the regular-quantifier translation of  $A_1$ .

**Proof:** By Theorem 2.35 of [1] one first algorithmically obtains a verifying proof

$$\text{WeZ}_m^{\exists} + \widetilde{\Delta} + \widetilde{\Delta}' \vdash \forall x^\mu \forall k^\iota \forall y \leq_\delta s x k \exists z \leq_\gamma \mathfrak{t} x k \widetilde{A}_1(x, k, y, z) \quad (3)$$

where the sentences in both  $\widetilde{\Delta}$  and  $\widetilde{\Delta}'$  are all of shape  $\exists Y \leq_{\rho\sigma} r \forall x^\rho \forall z^\tau B(x, Yx, z)$ , s.t.  $B$  may use only regular quantifiers, which are the direct regular correspondents of the **ncm** quantifiers which possibly occur in the original  $\forall x^\rho \exists y \leq_\sigma r x \forall z^\tau B^{\text{nc}}(x, y, z)$  sentence. Let **AxBAC** denote the following principle (Axiom) of Bounded Choice:

$$\forall R^{\rho \rightarrow \sigma} [ \forall x^\rho \exists y \leq_\sigma R x C(x, y, R) \rightarrow \exists Y \leq_{\rho \rightarrow \sigma} R \forall x C(x, Yx, R) ]$$

where  $\rho$  and  $\sigma$  are arbitrary types and  $C$  is an arbitrary regular formula of  $\text{WeZ}_m^{\exists}$ , see also Definition 3.2.1 of [3]. For  $R := r$  and  $C(x, y, R) \equiv \forall z B(x, y, z)$  one obtains that

$$\forall x^\rho \exists y \leq_\sigma r x \forall z^\tau B(x, y, z) + \text{AxBAC} \vdash \exists Y \leq_{\rho\sigma} r \forall x^\rho \forall z^\tau B(x, Yx, z)$$

Hence the whole  $\widetilde{\sim}$ -correspondent of a sentence in  $\Delta$  or  $\Delta'$  is a fully regular formula, which can be obtained like in Theorems 3.2.2 - 4.9 of [3] from the

direct regular correspondent of the original sentence and **AxBAC**. In consequence,

$$\Delta_{\text{reg}} + \Delta'_{\text{reg}} + \text{AxBAC} \quad \vdash \quad \widetilde{\Delta} + \widetilde{\Delta}'$$

hence one can also write

$$\text{WeZ}_m^{\exists} + \Delta_{\text{reg}} + \Delta'_{\text{reg}} + \text{AxBAC} \quad \vdash \quad \text{WeZ}_m^{\exists} + \widetilde{\Delta} + \widetilde{\Delta}' \quad (4)$$

Because of the restrictions on the types of the variables in  $\Delta_{\text{reg}}$ , it follows that all these sentences are valid not only in  $\mathcal{S}^\omega$  but also in  $\mathcal{M}^\omega$  (using that  $\mathcal{M}^0 = \mathcal{S}^0$ ,  $\mathcal{M}^1 = \mathcal{S}^1$  and  $\mathcal{M}^2 \subsetneq \mathcal{S}^2$ , see [3]). Since by assumption  $\mathcal{M}^\omega$  is also a model for  $\Delta'_{\text{reg}}$ , it follows that  $\mathcal{M}^\omega$  is generally a model for  $\text{WeZ}_m^{\exists} + \Delta_{\text{reg}} + \Delta'_{\text{reg}} + \text{AxBAC}$  - see also [2, 3] for an indication to the easy proof<sup>2</sup> of  $\mathcal{M}^\omega \models \text{WeZ}_m^{\exists} + \text{AxBAC}$ . Hence from (4) we have that (3) is valid in  $\mathcal{M}^\omega$ . Due to the restriction that the type degree of all positively universal and negatively existential quantified variables of (3) is at most 1 (this includes  $dg(\delta) \leq 1$ ) and also all positively existential and negatively universal quantified variables of (3) have type degree at most 2 (this includes  $dg(\gamma), dg(\alpha) \leq 2$ ) and using  $\mathcal{M}^0 = \mathcal{S}^0$ ,  $\mathcal{M}^1 = \mathcal{S}^1$  and  $\mathcal{M}^2 \subsetneq \mathcal{S}^2$ , in consequence also  $\mathcal{S}^\omega$  is a model of (3), which thus establishes the conclusion (2).  $\square$

It is easy to check that the non-standard (i.e., not valid in  $\mathcal{S}^\omega$ ) analytical axiom

$$\begin{aligned} \mathbf{F}^- &::= \quad \forall \Phi^{\iota(\iota)\iota} \forall x^{\iota\iota} \exists y \leq_{\iota\iota} x \forall k^{\iota} \forall z^{\iota\iota} \forall n^{\iota} \\ &\quad [ \wedge_{i <_{\iota} n} (z i \leq_{\iota} x k i) \rightarrow \Phi k (\lambda k^{\iota}. \text{If}_{\iota}(k <_{\iota} n)(z k) \mathbf{0}) \leq_{\iota} \Phi k (y k) ] \end{aligned}$$

can be included into the axiom set  $\Delta'$ , since  $\mathbf{F}^-$  has the right  $\Delta$ -shape and moreover  $\mathcal{M}^\omega \models \mathbf{F}^-$  (see Remark 4.17 of [3]). On the other hand, although valid in  $\mathcal{M}^\omega$  (see Proposition 4.6 of [3]), the stronger axiom

$$\mathbf{F} \quad ::= \quad \forall \Phi^{\iota(\iota)\iota} \forall x^{\iota\iota} \exists y \leq_{\iota\iota} x \forall k^{\iota} \forall z \leq_{\iota} y k \quad ( \Phi k z \leq_{\iota} \Phi k (y k) )$$

is not directly of  $\Delta$  shape, because of the type- $\iota$  negative universal quantifier expanded from the extensional definition of  $z \leq_{\iota} y k$ . Nevertheless,  $\mathbf{F}$  can be made into a  $\Delta'$  axiom by using an **ncm**-universal quantifier instead of the regular universal quantifier which causes the trouble. Let

$$\mathbf{F}^{\text{nc}} \quad ::= \quad \forall \Phi^{\iota(\iota)\iota} \forall x^{\iota\iota} \exists y \leq_{\iota\iota} x \forall k^{\iota} \forall z^{\iota\iota} [ \bar{\forall}^{\iota} (z l \leq_{\iota} y k l) \rightarrow \Phi k z \leq_{\iota} \Phi k (y k) ]$$

---

<sup>2</sup>The only novelty here, relative to the corresponding proof in [3], appears to be the inclusion of **AxCA** in  $\text{WeZ}_m^{\exists}$ . But both  $\mathcal{S}^\omega$  and  $\mathcal{M}^\omega$  are models of **AxCA**, which thus poses no problem.

be such an **ncm**-variant of  $\mathbf{F}$ , which is easily seen to be a  $\Delta$ -shape axiom. Since moreover  $\mathcal{M}^\omega \models \mathbf{F}$ , which is the direct regular-quantifier translation of  $\mathbf{F}^{\text{nc}}$ , i.e.,  $\mathbf{F} \equiv (\mathbf{F}^{\text{nc}})_{\text{reg}}$ , it follows that  $\mathbf{F}^{\text{nc}}$  is also a  $\Delta'$  axiom. Note that none of  $\mathbf{F}^-$  and  $\mathbf{F}^{\text{nc}}$  is an explicit  $\Delta$  axiom because  $\mathcal{S}^\omega \not\models \mathbf{F}^-$  and also  $\mathcal{S}^\omega \not\models \mathbf{F} \equiv (\mathbf{F}^{\text{nc}})_{\text{reg}}$  (see [3] for indications to the proofs of these). One thus obtains, *without using Luckhardt's elimination-of-extensionality* procedure (in contrast to Theorem 4.9 of [3] which uses it), the following:

**Corollary 0.2 (Full admissibility of  $\mathbf{F}^-$  and  $\mathbf{F}^{\text{nc}}$  to the direct LMD-ext.)**

Theorem 0.1 above holds as well in the variant when the hypothesis (1) is replaced by

$$\text{WeZ}_{\text{m}}^{\exists, \text{nc}, \text{c}^+} + \Delta + \mathbf{F}^- + \mathbf{F}^{\text{nc}} \vdash \forall x^\iota \forall k^\iota \forall y \leq_\delta \text{sxk} \exists z^\gamma A_1(x, k, y, z)$$

**Corollary 0.3 (Polynomial-Feasible case)** Theorem 0.1 and Corollary 0.2 adapt to the extraction of polynomial bounds in the sense of [3] in the following way. Assume that  $A_1$  is a **PbZ** formula and that  $s^{(\iota)\iota\delta}$  is a closed term of **PbZ**. Then there exists an algorithm which from a given proof  $\text{PbZ}^+ + \Delta + \Delta' \vdash \forall x^\iota \forall k^\iota \forall y \leq_\delta \text{sxk} \exists z^\gamma A_1(x, k, y, z)$  produces the syntactic polynomial  $\bar{p}[x^\iota, k^\iota, u^\iota, l^\iota] \in \text{Tm}^-(\text{PbZ})$  such that

$$\mathcal{S}^\omega \models \forall x^\iota \forall k^\iota \forall y \leq_\delta \text{sxk} \exists z \leq_\gamma \lambda u^\iota, l^\iota. \bar{p}[x^M, k, u^M, l] \widetilde{A}_1(x, k, y, z)$$

where  $u$  and  $l$  are (possibly empty) tuples determined by  $\gamma$ . Hence if  $\gamma \equiv \iota$  then  $p$  is a polynomial bound for  $z$  in  $x^M$  and  $k$  which is uniform w.r.t.  $y$ . All the above hold in particular for  $\Delta' \equiv \{\mathbf{F}^-, \mathbf{F}^{\text{nc}}\}$ . See Section 3.2.2 of [1] for terminology and more details.

## References

- [1] M.-D. Hernest. *Feasible programs from (non-constructive) proofs by the light (monotone) Dialectica interpretation*. PhD Thesis, École Polytechnique and University of Munich (LMU), December 2006. Final version available @ <http://www.brics.dk/~danher/teza/>.
- [2] U. Kohlenbach. Pointwise hereditary majorization and some applications. *Archive for Mathematical Logic*, 31:227–241, 1992.
- [3] U. Kohlenbach. Mathematically strong subsystems of analysis with low rate of growth of provably recursive functionals. *Archive for Mathematical Logic*, 36:31–71, 1996.

# Safety Properties Verification for Pfaffian Dynamics

Margarita Korovina<sup>1</sup> and Nicolai Vorobjov<sup>2</sup>

<sup>1</sup> Fachbereich Mathematik, Theoretische Informatik, Universität Siegen, Germany,  
and IIS SB RAS, Novosibirsk, Russia

[korovina@brics.dk](mailto:korovina@brics.dk),

<http://www.brics.dk/~korovina>

<sup>2</sup> Department of Computer Science, University of Bath, Bath BA2 7AY, England

[nv@cs.bath.ac.uk](mailto:nv@cs.bath.ac.uk),

<http://www.bath.ac.uk/~masnvn>

We investigate the behavior of a Pfaffian dynamical system with respect to invariants which formalise safety properties. We study continuous dynamical systems which are called Pfaffian, and first introduced in [5, 6]. These systems are defined by Pfaffian functions, either implicitly (via triangular systems of ordinary differential equations) or explicitly (by means of equations and inequalities involving *Pfaffian functions*). Such functions naturally arise in applications as real analytic solutions of triangular first order partial differential equations with polynomial coefficients, and include polynomials, algebraic functions, exponentials, and trigonometric functions in appropriate domains. Pfaffian functions form the largest natural class of real analytic functions which have a uniform description and an explicit characterisation of complexity of their representations in terms of *formats*.

One of the important problems in the theory of dynamical systems is understanding of the behavior of a dynamical system with respect to safety properties. In other words it would be desirable for a given dynamical system to verify a safety property which states that "something bad does never happen", for examples, the power plant will never blow up, the reactor temperature will never exceed 100° C.

In mathematical settings this problem is formalised in the following way. We consider a continuous dynamical system  $\gamma : G_1 \times T \rightarrow G_2$ , where  $G_1 \subseteq \mathbb{R}^{k_1}$  is a set of control parameters,  $T$  is an interval of time and  $G_2 \subseteq \mathbb{R}^{k_2}$  is a state space. Let  $U$  be a set of control parameters. A safety property is formalised by an invariant. An invariant is given by a condition  $\Phi$  for the states and requires that  $\Phi$  holds for all reachable states under the control  $U$ , i.e.  $\forall \mathbf{x} \in U \forall t \in T \Phi(\gamma_{\mathbf{x}}(t))$ . In this case we say *the subset  $U \subseteq G_1$  satisfies the invariant  $\Phi$* . We assume that dynamical systems and sets we are interested in are semi-Pfaffian. Our goal is to characterise the subsets of control parameter space which satisfy a given invariant. In order to achieve our goal we use encoding trajectories of a Pfaffian dynamical system by finite words [2, 5] and cylindrical cell decomposition for semi-Pfaffian sets [7, 3]. Based on this technique we construct an algorithm for safety properties verification for Pfaffian dynamical systems with an elementary exponential upper bound.

## References

1. S. Basu, R. Pollack and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, Springer, Berlin-Heidelberg, 2003.
2. T. Brihaye, C. Michaux, C. Riviere, C. Troestler, On o-minimal hybrid systems, in: *Hybrid Systems: Computation and Control*, R. Alur, G. J. Pappas, (Eds.), LNCS, **2993**, Springer, Heidelberg, 2004, 219–233.
3. A. Gabrielov, N. Vorobjov, Complexity of computations with Pfaffian and Noetherian functions, in: *Normal Forms, Bifurcations and Finiteness Problems in Differential Equations*, Yu. Ilyashenko et al., (Eds.), NATO Science Series II, **137**, Kluwer, 2004, 211–250.
4. A. Gabrielov, N. Vorobjov, Complexity of cylindrical decompositions of sub-Pfaffian sets, *J. Pure and Appl. Algebra*, **164**, 1–2, 2001, 179–197.
5. M. Korovina and N. Vorobjov, Pfaffian hybrid systems. In *Springer Lecture Notes in Comp. Sci.*, volume 3210 of *Computer Science Logic'04*, 2004, 430–441.
6. M. Korovina and N. Vorobjov, Upper and lower Bounds on Sizes of Finite Bisimulations of Pfaffian Hybrid Systems. In *Proceedings of CiE'06*, invited talk, LNCS 3988, 2006, 235–241.
7. L. van den Dries. *Tame Topology and O-minimal Structures*. Number 248 in London Mathematical Society Lecture Notes Series. Cambridge University Press, Cambridge, 1998.

# Complexity Theory and Gödel's $T$

Lars Kristiansen<sup>1,2</sup>

<sup>1</sup> Department of Mathematics, University of Oslo  
larskri@iu.hio.no WWW home page: <http://www.iu.hio.no/~larskri>

<sup>2</sup> Partly joint work with M. Barra (Oslo) and P.J. Voda (Bratislava)

## Two Hierarchies

In [1] and [2] we introduce two hierarchies of unknown ordinal height. Many of the well-known deterministic complexity classes, e.g. LOGSPACE, P, PSPACE, LINSPEACE and EXP, can be found in the hierarchies. These classes are defined by imposing explicit resource bounds on Turing machines, but note that the classes are not uniformly defined as some are defined by imposing *time* bounds, whereas other are defined by imposing *space* bounds. Small subrecursive classes can also be found in our hierarchies, e.g. the relational Grzegorzczuk classes  $\mathcal{E}_*^0$ ,  $\mathcal{E}_*^1$  and  $\mathcal{E}_*^2$ .<sup>3</sup> In contrast to a complexity class, a subrecursive class is defined as the least class containing some initial functions and closed under certain composition and recursion schemes. Some of the schemes might contain explicit bounds, but no machine models are involved.

The two hierarchies are induced by neat and natural fragments of a calculus based on finite types and Gödel's  $T$ ,<sup>4</sup> and all the classes in the hierarchies are uniformly defined without referring to explicit bounds. Thus, one should not expect the hierarchies to capture such a wide variety of classes, that is, both time classes, space classes and subrecursive classes. This indicates that a further investigation of the hierarchies might be rewarding, and perhaps shed light upon some of the notoriously hard open problems involving the classes captured by the hierarchies, e.g. maybe some of these problems turn out to be related in some unexpected way. Moreover, the ingredients of the theoretic framework nourishing the hierarchies are well known and thoroughly studied in the literature, e.g. the ordinal numbers, the typed  $\lambda$ -calculi, cut-elimination, rewriting systems and Gödel's  $T$ . Advanced and well proven techniques of mathematical logic and computability theory will thus be available facilitating the investigations.

In my talk I will carefully define and explain the two hierarchies.

## Nondeterminism

The standard model of nondeterministic computation is the Turing machine. Many of the interesting classes in our hierarchies are typical subrecursive classes and cannot be naturally characterised by Turing machines, and thus, these

---

<sup>3</sup> We expect a wide range of small subrecursive classes to be found in the hierarchies.

<sup>4</sup> The typed  $\lambda$ -calculus extended with numerals and recursors.

classes have no obvious nondeterministic correspondents. When we extend the definition of the terms of Gödel's  $T$  by

- $(M|N)$  is a term of type  $\sigma$  if  $M$  and  $N$  are terms of type  $\sigma$

and add the two rewrite rules  $(M|N) \triangleright M$  and  $(M|N) \triangleright N$ , we obtain a model of nondeterministic computation. This notion of nondeterminism is naïve and straightforward, but still worthy of further investigations since the model yields nondeterministic variants of all the classes occurring in our hierarchies, and thus, a uniform way of defining nondeterministic variants of a wide range of small subrecursive classes.

Our approach begs many questions, and it is not given at the outset that our model of nondeterminism will be robust and fruitful. If time permits, I will survey some recent research along this line.

## References

1. Kristiansen, L.: Complexity-theoretic hierarchies. Beckmann, Berger, Löwe, and Tucker (eds.): CiE'06: Logical Approaches to Computational Barriers, LNCS 3988, pp. 279-288, Springer-Verlag 2006.
2. Kristiansen, L.: Complexity theoretic hierarchies induced by fragments of Gödel's  $T$ . Journal version of [1] (submitted).

# 1 Karl-Heinz Niggl: Improvements on and Optimality of a recent method of certifying polynomial running time and linear/polynomial space

(Joint work with Jan Mehler)

The talk builds on a recent method [4] of certifying polynomial running time and linear/polynomial space for *imperative programs* built from arbitrary basic instructions (BI) by sequencing, if-then-else and for-do statements. Such programs operate on variables  $X_1, \dots, X_n$ , each of which may represent any data structure, provided that it is equipped with a notion of *size* of an object stored in  $X_i$ , denoted by  $|X_i|$ . For example, if  $X_i$  serves as a register, then  $|X_i|$  might be the binary length of the number stored in  $X_i$ .

The method consists in certifying “polynomial size boundedness” under the natural assumption that all basic instructions involved are *polynomial size bounded (psb)*, too. For a program  $P$  in variables  $X_1, \dots, X_n$ , that means there exist polynomials  $p_1, \dots, p_n$  in  $\mathbb{N}[\vec{X}]$ , called *polynomial bound on P*, such that

$$\{s_1 = |X_1|, \dots, s_n = |X_n|\} P \{ |X_i| \leq p_i(s_1, \dots, s_n) \} \text{ for } i = 1, \dots, n.$$

In case of success, the method assigns to  $P$  an  $(n+1) \times (n+1)$  matrix  $M(P)$  over the *forgetting set*  $\mathcal{A} := \{0, 1, \infty\}$  ordered by  $0 < 1 < \infty$ , where for technical reasons the last row is always the  $(n+1)$ -tuple  $0^n 1$ .  $M(P)$  is a *certificate for P* in that there exists a polynomial bound  $p_1, \dots, p_n$  on  $P$  such that for  $i = 1, \dots, n$ , the  $(n+1)$ -tuple  $\langle p_i \rangle$  over  $\mathcal{A}$  satisfies  $\langle p_i \rangle \leq M(P)[i]$ , where the *representation*  $\langle p \rangle$  of a polynomial  $p(\vec{X}) = c_0 + \dots + c_j \cdot X_1^{j_1} \cdot \dots \cdot X_n^{j_n} + \dots$  is defined by

$$(j=1, \dots, n) \quad \langle p \rangle[j] = \begin{cases} 0 & \text{if } p \text{ is a polynomial in } \vec{X} \setminus X_j \\ 1 & \text{if } p = X_j + q \text{ for some polynomial } q \text{ in } \vec{X} \setminus X_j \\ \infty & \text{else} \end{cases}$$

$$\langle p \rangle[n+1] = \begin{cases} c_0 & \text{if } c_0 \leq 1 \\ \infty & \text{else.} \end{cases}$$

For example, a certificate for the assignment statement  $X_i = X_j$  is obtained from the identity matrix  $1_{n+1}$  by replacing row  $i$  with row  $j$ . A certificate for  $X_i = X_i + X_j + 1$  is obtained from  $1_{n+1}$  by replacing row  $i$  with  $1_{n+1}[i] + 0^{j-1} 10^{n-j} 1$ , where  $+$  is the maximum over  $\mathcal{A}$ , except for  $1 + 1 := \infty$ .

The present method strengthens the results for programs of  $\mu$ -measure 0 considered in [2], as the following characterisations are obtained [4].

FPTIME = certified string programs (stack programs, but with any polynomial-time computable BIs)

FLINSPACE = certified general loop programs (loop programs, but with any linear-space computable BIs)

FPSPACE = certified power string programs (string programs, but extended by powerloop statements and any polynomial-space computable BIs)

The improvements over [4] concern the certification of loop statements by generalising the cases “variable/constant assignment” and “push/inc” to the **Additive Case**: Let  $Y$  be the certificate for the body  $Q$  of a loop, then

$$\text{ADD}(Y) := \{i \in \{1, \dots, n\} \mid Y^+[i] \leq 1^n \infty\}$$

denotes the set of *additive  $i$ 's in  $Y$* , where  $Y^+ := \bigsqcup_{k \geq 1} Y^k$  is the component-wise maximum of all positive iterates of  $Y$ .

Writing  $j \rightarrow_Y i$  for  $Y[i][j] \geq 1$  (read  $j$  *controls  $i$  in  $Y$* ), and  $\overset{+}{\rightarrow}_Y, \overset{*}{\rightarrow}_Y$  for the transitive, reflexive and transitive closure of  $\rightarrow_Y$ , respectively, the intuition is that for an additive  $i$  in  $Y$ , the polynomial size bound on  $X_i$  with respect to  $Q$  is of the form  $c_i + \sum_{j \rightarrow_Y i} X_j$  for some constant  $c_i$ .

Suppose that the *psb-criterion* for loop statements holds, i.e.,  $\infty \notin \text{Diag}(\hat{Y}^*)$  (read  $Y$  *contains no control circle*), where  $\hat{Y} := Y \sqcup 1_{n+1}$  and  $Y^* := Y^+ \sqcup 1_{n+1}$ . Then we show that  $\overset{*}{\rightarrow}_Y$  is a partial ordering of  $\{1, \dots, n\}$ , and  $\text{ADD}(Y)$  is closed under control, that is, if  $j \overset{+}{\rightarrow}_Y i$ , and  $i$  is additive in  $Y$ , then so is  $j$ . Thus, the ADD-Case can be treated separately from the “ELSE-Case”, and in fact, we will construct a polynomial size bound on each additive  $i$  in  $Y$  with respect to the given loop statement.

Compared with [4], the additive case admits more certified programs, and leads to better extracted polynomial size bounds — indeed, the present method is available as a Java-applet.

The present method is a major step towards applicability of research in the evolving field of implicit computational complexity to daily programming practice. In [4], this is exemplified by showing that natural implementations of binary ADDITION and MULTIPLICATION, and INSERTION SORT are certified, some of which are considered benchmark algorithms. While the intensional expressive power of such certification methods is often exemplified by certifying benchmark algorithms, the intensional expressive power of our method is substantiated by the following optimality result for so-called core programs.

**Thm (Optimality).** A core program has a certificate iff it is polynomially size bounded.

Similar results have been shown for the class of core programs considered in [2] and [3], where **push** is the only admissible basic instruction. By contrast, the *core programs* here are built from “honestly certified” basic instructions (their certificates satisfy certain conditions) by sequencing and loop statements.

Rounding off, the approach in [1] is strongly related to our method: While the former certifies more loop statements for a loop language where the only admissible basic instructions are assignment statements  $X_i := e$ , the rhs being an expression built from variables and  $+, \cdot$  (no constants!), our method admits any basic instructions (operating on any data structure) that are polynomially size bounded (any polynomial with natural coefficients!). Current research is investigating whether, and if “yes”, how those two methods can be fused to a single new method that preserves the advantages of both approaches.

Karl-Heinz Niggl  
TU Ilmenau, Fakultät für Informatik  
niggl@tu-ilmenau.de  
eiche.theoinf.tu-ilmenau.de/~niggl

## References

- [1] Jones, N.D., Kristiansen, L.: *The flow of data and the complexity of algorithms*. Cooper, Löwe, Torenvliet (eds.): CiE'05, LNCS 3526:263-274, Springer 2005.
- [2] Kristiansen, L., Niggl, K.-H.: *On the computational complexity of imperative programming languages*. TCS, Special issue on Implicit Computational Complexity, Editor J.-Y. Marion, 318(1-2):139–161, Elsevier 2004.
- [3] Kristiansen, L., Niggl, K.-H.: *The Garland Measure and Computational Complexity of Stack Programs*. ENTCS 90 No. 2 (2003),  
URL: <http://elsevier.nl/locate/entcs/volume90.html>, 19 pages
- [4] Niggl, K.-H., Wunderlich, H.: *Certifying polynomial time and linear/polynomial space for imperative programs*. SIAM Journal on Computing, 35(5):1122–1147, published electronically March 3, 2006.

# On the way to NP

Isabel Oitavem

Dept. Matemática da FCT-UNL and CMAF-UL

## Abstract

This talk is based on the recursion-theoretic characterization of Ptime due to Bellantoni and Cook (reformulated over the algebra  $\mathbb{W}$ ) and on the characterization of Pspace which results from the previous one by introducing pointers in the recursion on notation scheme. In this talk we identify a third class of functions  $C$ , such that  $Ptime \subseteq C \subseteq Pspace$ . Any NP decidable language is recognized by some function in  $C$ . In this sense, the class of functions  $C$  is on the way to a recursion-theoretic approach to NP. This is work in progress.

## Ordinal analysis for $\Pi_1^0$ -definable non-monotone inductive definitions

Wolfram Pohlers. Münster

A general (i.e., non-monotone) inductive definition on the natural numbers is just an operator  $\Phi: \text{Pow}(\mathbb{N}) \rightarrow \text{Pow}(\mathbb{N})$ . The *inflationary stages* of an inductive definition  $\Phi$  are defined by

$$\Phi^\alpha := \Phi^{<\alpha} \cup \Phi^{\Phi^{<\alpha}} \quad \text{where} \quad \Phi^{<\alpha} := \bigcup_{\xi < \alpha} \Phi^\xi.$$

Put  $\Phi^\infty := \bigcup_{\xi \in \text{On}} \Phi^\xi$  and call  $\Phi^\infty$  the fixed point of  $\Phi$ . By cardinality reasons there is a countable ordinal  $\sigma$  such that  $\Phi^\sigma = \Phi^{<\sigma}$ . Then  $\Phi^\infty = \Phi^\sigma = \Phi^{<\sigma}$ . An operator is definable if there is a formula  $F$  in the language of number theory such that  $\Phi(X) := \{x \in \mathbb{N} \mid F(x, X)\}$ . It is  $\Pi_1^0$ -definable iff  $F$  is a  $\Pi_1^0$ -formula. A set  $A \subseteq \mathbb{N}$  is inductively  $\Pi_1^0$ -definable over  $\mathbb{N}$  iff there is a  $\Pi_1^0$ -definable operator  $\Phi$  and a natural number  $k$  such that

$$A := \{x \in \mathbb{N} \mid \langle x, k \rangle \in \Phi^\infty\}.$$

We define

$$|n|_\Phi := \begin{cases} \min \{\xi \mid x \in \Phi^\xi\} & \text{for } n \in \Phi^\infty \\ \omega_1 & \text{otherwise} \end{cases}$$

and obtain the pre-wellordering relations

$$m \preceq_\Phi n \quad :\Leftrightarrow \quad m \in \Phi^\infty \wedge |m|_\Phi \leq |n|_\Phi$$

and

$$m \prec_\Phi n \quad :\Leftrightarrow \quad m \in \Phi^\infty \wedge |m|_\Phi < |n|_\Phi \quad \Leftrightarrow \quad |m|_\Phi < |n|_\Phi.$$

Then we get  $\Phi^\infty = \{m \in \mathbb{N} \mid m \preceq_\Phi m\}$ .

To obtain an axiomatization of general inductive definitions we axiomatize the notion of a pre-wellordering.

**0.1 Definition** A prewellordering on a set  $P$  (of natural numbers) is a triple  $(P, \prec, \preceq)$  such that there is a countable ordinal  $\lambda$  and function  $f: A \xrightarrow{\text{onto}} \lambda$  such that

$$m \preceq n \quad \Leftrightarrow \quad m \in A \wedge f(m) \leq f(n)$$

and

$$m \prec n \quad \Leftrightarrow \quad m \in A \wedge f(m) < f(n)$$

where we define  $f(n) := \omega_1$  for  $m \notin A$ .

Then we obtain

**0.2 Theorem** (*Pre-wellordering theorem*) Let  $\Phi$  be an inductive definition. The triple  $(\Phi^\infty, \preceq_\Phi, \prec_\Phi)$  is the uniquely defined pre-wellordering which satisfies

$$m \preceq n \quad \Leftrightarrow \quad m \prec n \vee m \in \Phi(\{x \mid x \prec n\}).$$

**0.3 Theorem** *The triple  $(A, \preceq, \prec)$  is a pre-wellordering iff it satisfies the following conditions*

$$(PW0) \quad x \preceq y \leftrightarrow x \in A \wedge [y \notin A \vee \neg(y \prec x)]$$

$$(PW1) \quad x \prec y \leftrightarrow x \preceq y \wedge \neg(y \preceq x)$$

(PW3)  $\prec$  is well-founded.

It follows from Theorems 0.2 and 0.3 that the theory of inductively definable sets can be axiomatized in a subtheory  $(\Pi_1^0\text{-FXP})$  of second order arithmetic. An ordinal analysis of  $(\Pi_1^0\text{-FXP})$  means to find the least ordinal  $\kappa = \kappa^{(\Pi_1^0\text{-FXP})}$  such that

$$((\Pi_1^0\text{-FXP}) \vdash \underline{n} \in \Phi^\infty) \Rightarrow |n|_\Phi = \kappa,$$

where  $\Phi$  is  $\Pi_1^0$ -definable.

It is known that  $\eta_0$ , the Howard-Bachmann ordinal, is likewise the proof-theoretic ordinal of the theory  $(ID_1)$  of non-iterated positive inductive definitions and that of set theory with absolute separation and  $\Pi_2$ -reflection.

Since the theory  $(ID_1)$  is easily embedded into  $(\Pi_1^1\text{-CA})_0$  which, in turn, is clearly embeddable into  $(\Pi_1^0\text{-FXP})$ , we get  $\eta_0 \leq \kappa^{(\Pi_1^0\text{-FXP})}$ . To get also  $\kappa^{(\Pi_1^0\text{-FXP})} \leq \eta_0$  we show that  $(\Pi_1^0\text{-FXP})$  is embeddable into the set theory with absolute separation and the scheme of  $\Pi_2$ -reflection. such

# Kripke Platek set theory over polynomial time computable arithmetic

Dieter Probst and Thomas Strahm

March 1, 2007

The theory of admissible sets, i.e. Kripke Platek set theory, is one of the most familiar subsystems of Zermelo Fraenkel set theory. Apart from their significance for definability theory, theories for (iterated) admissible sets have long been central to proof theory, see Jäger [4] for a survey or Jäger [5] for a comprehensive monograph.

This work is concerned with systems of Kripke Platek set theory which are proof-theoretically weak. It can be seen as a companion to Jäger's  $\text{KPU}^r$  of Kripke Platek set theory with the natural numbers as urelements, which is a conservative extension of Peano arithmetic  $\text{PA}$ , cf. Jäger [5]. Whereas in  $\text{KPU}^r$  the axioms of admissible sets are stated above the ground theory  $\text{PA}$ , we deal with similar theories above a version of bounded arithmetic, namely Ferreira's polynomial time computable arithmetic  $\text{PCTA}$ , cf. Ferreira [2, 3].

In contrast to the theory  $\text{KPU}^r$ , we no longer claim that the collection of urelements forms a set, since the presence of  $\Delta_0$  separation would immediately yield full unbounded quantification over the urelements. With respect to our urelements  $W$  (the collection of binary words), we study two set existence principles for collections of words, namely:

- (W.0) *The collection of all subwords of a given word forms a set;*
- (W.1) *The collection of all words whose length is less than or equal to the length of a given binary word forms a set.*

We will establish that

- (i)  $\mathbb{A}_0(\text{PTCA})$  is conservative over  $\text{PCTA}$  with respect to  $\forall\exists\Sigma_1^b$  sentences, and,
- (ii)  $\mathbb{A}_1(\text{PTCA})$  is conservative over full bounded arithmetic  $\Sigma_\infty^b\text{-NIA}$  for  $\forall\exists\Sigma_\infty^b$  sentences.

This will yield, in particular, that the  $\Sigma_1^b$  definable functions of  $\mathbb{A}_0(\text{PTCA})$  are the polytime functions, and (ii) the  $\Sigma_\infty^b$  definable functions of  $\mathbb{A}_1(\text{PTCA})$  are the functions in the polynomial time hierarchy.

In order to establish the upper bounds, we embed  $\mathbb{A}_0(\text{PTCA})$  and  $\mathbb{A}_1(\text{PTCA})$  into fixed point theories in the style of  $\text{PA}_\Omega^r$  by Jäger [6], where suitable conservative extensions of  $\text{PTCA}$  and  $\Sigma_\infty^b\text{-NIA}$  take the place of  $\text{PA}$ : In the case of  $\mathbb{A}_0(\text{PTCA})$  we work with a fixed point theory over  $\text{PTCA}$  plus sharp  $\Sigma$  reflection, (cf. Cantini [1]) and in the case of  $\mathbb{A}_1(\text{PTCA})$  a fixed point theory is formulated over

$\Sigma_\infty^b$ -NIA plus  $\Sigma$  reflection (equivalently: bounded collection). A model-theoretic argument is used to show that these theories have the appropriate strength. In the embedding of  $\mathbb{A}_0(\text{PTCA})$  and  $\mathbb{A}_1(\text{PTCA})$  one carefully models initial segments of the constructible hierarchy in the fixed point theories. In verifying the axioms of admissible set theory, crucial use is made of the two principles of sharp and unsharp  $\Sigma$  reflection, respectively.

## References

- [1] CANTINI, A. Asymmetric interpretation for bounded theories. *Mathematical Logic Quarterly* 42 (1996), 270–288.
- [2] FERREIRA, F. *Polynomial Time Computable Arithmetic and Conservative Extensions*. PhD thesis, Pennsylvania State University, 1988.
- [3] FERREIRA, F. Polynomial time computable arithmetic. In *Logic and Computation, Proceedings of a Workshop held at Carnegie Mellon University, 1987*, W. Sieg, Ed., vol. 106 of *Contemporary Mathematics*. American Mathematical Society, Providence, Rhode Island, 1990, pp. 137–156.
- [4] JÄGER, G. Iterating admissibility in proof theory. In *Logic Colloquium '81. Proceedings of the Herbrand Symposium*. North Holland, Amsterdam, 1982.
- [5] JÄGER, G. *Theories for Admissible Sets: A Unifying Approach to Proof Theory*. Bibliopolis, Napoli, 1986.
- [6] JÄGER, G. Fixed points in Peano arithmetic with ordinals. *Annals of Pure and Applied Logic* 60, 2 (1993), 119–132.

## Address

Dieter Probst and Thomas Strahm  
Institut für Informatik und angewandte Mathematik, Universität Bern  
Neubrückstrasse 10, CH-3012 Bern, Switzerland  
Email: `probst@iam.unibe.ch`, `strahm@iam.unibe.ch`

# Searching for Algorithms in Proofs of Existence of Gröbner Bases

Diana Ratiu

We report here the work in progress which investigates the algorithmic potential of classical existence proofs in the theory of Gröbner Bases. Such a proof is that of Dickson's Lemma, which has been investigated in [2] and for which a program has been extracted using the proof assistant Minlog (see [3] for details). An equivalent statement of Dickson's Lemma has been used in [1] to show the existence of the Gröbner Basis of a given ideal. Using the methods of retrieving computational content suggested in [2], we aim at an analysis of this proof and at a comparison with the results of [4], in which the author follows methodically the intellectual process which lead to the invention of Buchberger's Algorithm for the construction of the Gröbner Basis.

## References

- [1] Becker, T. and Weispfenning, V., Gröbner Bases. A computational Approach to Commutative Algebra, 1993, Graduate Texts in Mathematics, Springer-Verlag, New York.
- [2] Berger, U., Buchholz, W. and Schwichtenberg, H., Refined Program Extraction from Classical Proofs, 2002, Annals of Pure and Applied Logic, 3-25
- [3] Berger, U. , Schwichtenberg, H. and Seisenberger, M., The Warshall Algorithm and Dickson's Lemma: Two Examples of Realistic Program Extraction, 2001, Journal of Automated Reasoning, 205-221
- [4] Buchberger B, Towards the Automated Synthesis of a Gröbner Bases Algorithm, 2004, RACSAM (Review of the Spanish Royal Academy of Science), 1-11

# Computational content of indirect existence proofs

Helmut Schwichtenberg

Gödel's Dialectica interpretation assigns to an indirect proof for the existence of an object in a decidable set a direct one. We present an implementation of this proof interpretation, based on a natural deduction formulation of arithmetic in finite types, and discuss some problems connected with it. As a case study, we consider a standard indirect proof (using properties of ideals in the integers) of Euclid's theorem that the gcd of two numbers is a linear combination of the two.

# Representing L-Domains as Information Systems

Dieter Spreen

Theoretische Informatik, Fachbereich Mathematik

Universität Siegen, 57068 Siegen, Germany

*E-mail:* spreen@informatik.uni-siegen.de

## Extended abstract

Information systems have been introduced by Dana Scott as a logic-oriented approach to domain theory: the category of bounded-complete algebraic domains with Scott continuous functions is equivalent to the category of information systems and approximable mappings. An information system typically consists of a set of tokens, say  $A$ , a consistency predicate  $\text{Con}$  on the collection of all finite sets of tokens and an entailment relation  $\vdash$  between consistent sets of tokens and tokens. Structures of this kind have been used to represent various subcategories of algebraic domains. R. Hoofman extended them to the case of bounded-complete continuous domains. In joint work with X. Mao and L. Xu an information-system representation of arbitrary continuous domains has been found.

For any such continuous information system, the collections of its states form a continuous domain with respect to set inclusion. A *state*  $x$  is a set of tokens such that any of its finite subsets is included in a consistent subset of  $x$ ,  $x$  is closed under entailment, and any token in  $x$  is entailed by a consistent subset of  $x$ .

Given a continuous domain  $D$  with basis  $B$ , then by letting  $B$  be the set of tokens, calling a subset  $X$  of  $B$  consistent, if it has a least upper bound in  $D$ , and defining that  $X$  entails  $a$ , if  $a$  is way-below  $\bigsqcup X$ , one obtains a continuous information system which in its turn generates a domain that is isomorphic to  $D$ .

In the talk an extra condition is presented such that the continuous information systems satisfying it generate exactly the continuous L-domains. L-domains have been introduced by A. Jung. Whereas in bounded-complete domains every bounded set has a (global) least upper bound, this is only locally true in the L-domain case: in every principal ideal each subset has a least upper bound.

As said above, consistent subsets of an information system represent existing least upper bounds of base elements. So, the difficulty is to define in the language of information systems when a consistent set of tokens represents a local least upper bound. In the talk we will present such a condition. This will lead to the definition of continuous L-information systems such that the above mentioned equivalence between continuous domains and continuous information systems, when restricted to L-domains, gives the following result.

**Theorem 1** *The category of continuous L-information systems with approximable mappings is equivalent to the category of continuous L-domains with Scott continuous functions.*

Moreover, given continuous L-information systems  $(A_i, \text{Con}_i, \vdash_i)$ , for  $i = 1, 2$ , an information system  $(A_1 \rightarrow A_2, \text{Con}_{\rightarrow}, \vdash_{\rightarrow})$  with the following properties is constructed in a canonical way.

**Theorem 2** 1.  $(A_1 \rightarrow A_2, \text{Con}_{\rightarrow}, \vdash_{\rightarrow})$  is an *L-information system*.

2. *The continuous domain generated by  $(A_1 \rightarrow A_2, \text{Con}_{\rightarrow}, \vdash_{\rightarrow})$  is the continuous L-domain of all approximable mappings between  $A_1$  and  $A_2$  ordered with respect to set inclusion.*

Note that the L-domain of all approximable mappings between  $A_1$  and  $A_2$  is isomorphic to the L-domain of all Scott continuous functions from the domain generated by  $A_1$  into the domain generated by  $A_2$ .

# Infinitary Systems for the Modal $\mu$ -Calculus

Thomas Studer

Our work is concerned with the proof theoretic relationship between two infinitary deductive systems for the propositional modal  $\mu$ -calculus. The  $\mu$ -calculus is defined by the addition of least and greatest fixed point operators to (multi-)modal logic. This results in a great increase in the expressive power: the modal  $\mu$ -calculus includes most of the languages used for program verification. However, it is also much more difficult to present complete deductive systems for the modal  $\mu$ -calculus since its language allows for arbitrary nestings of (possibly interleaved) fixed points.

There are two approaches to define infinitary axiomatizations for the  $\mu$ -calculus. The first approach is to make use of so-called  $\omega$  rules that have infinitely many premises to ensure that a fixed point is a least (or greatest) one.  $\mathbb{T}_{\mu+}^{\omega}$  is such a system studied in [2]. There, completeness of  $\mathbb{T}_{\mu+}^{\omega}$  is established by generalizing standard techniques for modal logics.

A second approach is to define a deductive system  $\mathbb{T}_{\mu}^{\text{pre}}$  such that in a proof search procedure fixed points are simply unfolded (which corresponds to closure of fixed points). This results in a so-called preproof which may have infinitely long branches. A global condition is then added which (roughly) says that in every such an infinite branch, there must be an outermost greatest fixed point unfolded infinitely many often. Such a system is proposed for example in [1].

We show that given a  $\mathbb{T}_{\mu+}^{\omega}$  proof of a formula  $A$  of the  $\mu$ -calculus, one can explicitly construct a  $\mathbb{T}_{\mu}^{\text{pre}}$  proof of  $A$ . This provides:

1. a completeness proof of  $\mathbb{T}_{\mu}^{\text{pre}}$  since  $\mathbb{T}_{\mu+}^{\omega}$  is complete,
2. a soundness proof of  $\mathbb{T}_{\mu+}^{\omega}$  since  $\mathbb{T}_{\mu}^{\text{pre}}$  is sound,
3. a proof-theoretic proof of the finite model property of the  $\mu$ -calculus since the canonical counter model construction for  $\mathbb{T}_{\mu+}^{\omega}$  can now be finitized.

## References

- [1] C. Dax, M. Hofmann, and M. Lange. A proof system for the linear time  $\mu$ -calculus. In *Proc. 26th Conf. on Foundations of Software Technology and Theoretical Computer Science, FSTTCS'06*, volume 4337 of *LNCS*, pages 274–285. Springer, 2006.
- [2] G. Jäger, M. Kretz, and T. Studer. Canonical completeness of infinitary  $\mu$ . Submitted.

### Address

Thomas Studer

Institut für Informatik und angewandte Mathematik, Universität Bern

Neubrückstrasse 10, CH-3012 Bern, Switzerland

tstuder@iam.unibe.ch

## FINDING DIALECTICA REALISERS FOR AXIOMS

TRIFON TRIFONOV

Gödel's functional (*Dialectica*) interpretation [1, 6, 9] was designed to translate a possibly non-constructive system to a constructive quantifier-free system employing the concept of primitive recursive functionals of higher finite type. More precisely, each arithmetic formula  $\varphi$  translates to a formula  $\exists_x \forall_y \varphi_D(x, y)$ , such that  $\varphi$  is provable in the original system if and only if the quantifier-free  $\varphi_D(t, y)$  is provable in the target constructive system, with  $t$  a term (not containing  $y$  freely) called the *realiser* for  $\varphi$ .

The Dialectica interpretation can be naturally used for program extraction from classical proofs, since its soundness proof provides as with an algorithm to convert a classical proof of the original formula to a realiser and a constructive proof of its translation. One of the main disadvantages of Dialectica, compared to other approaches for program extraction (e.g. Friedman's A-translation [5] as well as Berger, Buchholz and Schwichtenberg's refined variant [2]), is that extracted terms tend to become long very fast when the length of the formula increases. The underlying reason for this is that Dialectica was designed to take into account both positive (realising) and negative (challenging) computational content of proofs. There already exist variants of the interpretation, which try to remove some of the unnecessary complexity: Kohlenbach's Monotone Dialectica [8], which looks for bounds of realising terms and Hernest's Light (Monotone) Dialectica [3], which employs non-computational quantifiers to deal with lack of computational relevance. Yet Dialectica remains technically complex, even when applied to relatively short proofs and requires automatic treatment.

In order to fully exploit the potential of Dialectica it is good to strengthen the original system with as many realisable (non-constructive) principles as possible. Such principles are often represented as axiom schemes with free predicate and type variables. Since an axiom does not have a proof in the system it is added to, it is not possible to use the general method to present a realiser for it. However, realisers for axioms are explicitly needed in the extraction process. Usually such a realiser can be given directly, but this can be technically difficult even for short axioms. Moreover, it might be necessary to impose some restrictions on the axiom scheme in order to be able to realise it [1, 3, 8, 9]. Therefore, an automatic way for checking realisability and realising axioms would be desirable.

Unlike the original formulation of Gödel, we consider pair types instead of dealing with variable tuples. For a formula  $\varphi$  we can inductively define inductively the types  $\tau^+(\varphi)$  and  $\tau^-(\varphi)$  of the variables  $x$  and  $y$  in its Dialectica translation  $\exists_x \forall_y \varphi_D(x, y)$ , called the *positive* and the *negative* type of  $\varphi$  respectively. A realiser for an axiom scheme should be a closed term of the positive type.

We have a natural translation of types to propositional formulae with  $\rightarrow$  and  $\wedge$ . Using the Curry-Howard correspondence we can reduce the search for a closed term of the appropriate type to search of a proof in minimal propositional logic of the corresponding formula. An example of such an algorithm can be found in [4, 7]. Since Dialectica translations are quantifier-free, the procedure to check whether a term is a realiser of a formula can be done again via propositional proof search. However, not every closed term of the appropriate type is a realiser for the axiom,

so if the realiser check gives a negative result, the proof search should continue. In case the proof search gives a negative result, we can conclude that a realiser of the axiom should include constants or perhaps canonical inhabitants. While this is the case for example with the induction axiom, it is unlikely to happen for general logical axioms without type constants. In the latter case we should consider a possible restriction on the axiom scheme.

The search for axiom realisers was implemented in the interactive proof system Minlog [10] developed in Munich. The automatic procedure was able to provide realisers for axioms usually used to extend a weak-extensional intuitionistic first-order arithmetic, such as Independence of Premise, Markov's Principle, Axiom of Choice. The realiser search was successful also for some axioms suggested by Hernest in [3] to extend a classical first-order arithmetic, where in addition some refinements of the restrictions imposed in [3] were proved to preserve realisability.

#### REFERENCES

- [1] J. Avigad and S. Feferman. *Gödel's functional ('Dialectica') interpretation*, volume 137 of *Studies in Logic and the Foundations of Mathematics*, pages 337–405. Elsevier, 1998.
- [2] Ulrich Berger, Wilfried Buchholz, and Helmut Schwichtenberg. Refined program extraction from classical proofs. *Ann. Pure Appl. Logic*, 114(1-3):3–25, 2002.
- [3] Mircea Dan-Hernest. *Optimized programs from (non-constructive) proofs by the light (monotone) Dialectica interpretation*. PhD thesis, 2007.
- [4] Roy Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *JSL*, 57:793–807, 1992.
- [5] Harvey Friedman. Classically and intuitionistically provably recursive functions. *Lecture Notes in Mathematics*, 669:21–27, 1978.
- [6] Kurt Gödel. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. *Dialectica*, (12):280–287, 1958.
- [7] Joerg Hudelmaier. Bounds for cut elimination in intuitionistic propositional logic. *AML*, 31:331–354, 1992.
- [8] U. Kohlenbach. Proof interpretations and the computational content of proofs. Lecture course.
- [9] Helmut Schwichtenberg. Lecture notes in proof theory. Summer Semester 2006.
- [10] Helmut Schwichtenberg et al. Interactive proof system MINLOG. <http://www.minlog-system.de/>.

# Ordinal Arithmetic and $\Sigma_2$ -Elementarity

Gunnar Wilken

March 2, 2007

## **Abstract**

Elementary Patterns of Resemblance, introduced by T.J. Carlson as a new approach to ordinal notation systems, are finite sequences of nested trees which satisfy certain simple conditions. Despite their short definition, which essentially involves the notion of elementary substructure, they have a complex combinatorial structure.

In this talk we will illustrate the ordinal arithmetical analysis of Patterns of Resemblance that are based on  $\Sigma_2$ -elementarity.

# Normalisation of $\omega$ -Arithmetic by certain finite means

Ernst Zimmermann, Boeblingen

February 2007

## Abstract

Normalisation of Arithmetic in Natural Deduction with the  $\omega$ -rule is proved with certain finite means only: a mapping of deductions to the universal tree of finite sequences of natural numbers and induction on such trees, which are in fact well founded; an expansion operation for implicative cuts, which separates the bad, complexity increasing, from the good, complexity decreasing part of implicative cuts; and conversions. The inductions involved in normalising a deduction are of order type  $\omega^\omega \cdot \omega$ , if put together.

## 1 Rules for $\Omega$ -Arithmetic

**Definition 1.1** The *language of first order  $\omega$ -arithmetic*  $\Omega A$ . A set  $V$  of countable many *individual variables*:  $x_1, x_2, \dots \in V$ ; *individual constant* 0; a set  $F$  of countable many *function signs*  $f_1, f_2, \dots \in F$  of arbitrary arity, where  $' = f_1$  is a unary function sign. The set of *number terms*  $C$ :  $0 \in C$ ; if  $r \in C$ , then  $r' \in C$ . The set of *terms*  $T$ :  $C \subseteq T, V \subseteq T$ ; if  $r_1, \dots, r_k \in T$  and  $f_m \in F$ , then  $f_m(r_1, \dots, r_k) \in T$ .  $=$  is a binary relation sign,  $\rightarrow, \wedge$  binary connectives,  $\forall$  a quantifier, and  $\perp$  a constant;  $(, )$ , the parantheses, are auxiliar symbols.

The set of *well formed formulas wff* of  $\Omega A$  is:  $r = s \in wff$ , if  $r, s \in T$ ;  $\perp \in wff$ ;  $(A \rightarrow B), (A \wedge B), (\forall x A) \in wff$ , if  $A, B \in wff, x \in V$ . Parentheses, especially outer ones, are often missing.  $\neg A \leftrightarrow_{df} A \rightarrow \perp$ .

$X(s/t)$  has the meaning, that in expression  $X$ , term, formula or deduction, term  $s$  is substituted at all occurences through term  $t$ .

**Definition 1.2** The *rules* of  $\Omega A$  are:  $AX, BR, \rightarrow E, \rightarrow I, \wedge E, \perp R, \forall E, \forall I$ .

$AX$  states any arithmetic equality  $A$  without free variables, calculated by primitive recursive means, as axiom;  $BR$  states any arbitrary formula  $A$  without free variables as assumption;  $\rightarrow E, \rightarrow I, \wedge E, \wedge I, \perp R$  are as usual;  $\forall I$  has infinitely many premises;  $\forall E$  is restricted to substitution of number terms.

$$\begin{array}{c}
 \vdots \quad \vdots \\
 \frac{A \quad A \rightarrow B}{B} \rightarrow E \qquad \frac{[A]^u \quad B}{A \rightarrow B} \rightarrow Iu \\
 \\
 \vdots \qquad \qquad \qquad \vdots \quad \vdots \\
 \frac{\forall x A}{A(x/k)} \forall E \text{ if } k \in C \qquad \frac{A(x/0) \quad A(x/0') \quad \dots}{\forall x A} \forall I
 \end{array}$$

Concepts like premise, conclusion, major premise, minor premise, assumption, path, height of a formula occurrence, cut, degree of a formula, are defined as usual.

**Lemma 1.3 Paths of deductions are of finite length.**

Proved by induction on the length of a path in a deduction.

As a consequence of this lemma the deduction trees of  $\Omega A$  are well-founded, although they may branch infinitely, the paths or branches themselves are finite.

**Definition 1.4** To every formula occurrence of a given deduction a finite sequence of natural numbers  $\langle a_1, \dots, a_n \rangle$  for  $a_1, \dots, a_n \in \omega$  is assigned via recursive function  $\pi$ :

if  $\frac{\vdots}{B}$ , then  $\pi(B) = \langle \rangle$ ;

( $B$  is the conclusion of a given deduction;)

if  $\frac{\dots \frac{A_k}{A} \dots}{A}$  and  $\pi(A) = \langle b_1, \dots, b_m \rangle$ , then  $\pi(A_k) = \langle b_1, \dots, b_m, k \rangle$  for  $0 \leq k$ .

( $A_k$  is the  $k$ -th premise of an application of a rule with conclusion  $A$ .)

On  $\mathcal{O}$ , the set of all finite sequences of natural numbers, for short *sequence numbers*, including the empty sequence  $\langle \rangle$ , the natural *lexicographical order*  $\prec$  is defined: for  $\langle a_1, \dots, a_k \rangle, \langle b_1, \dots, b_m \rangle \in \mathcal{O}$ :  $\langle a_1, \dots, a_k \rangle \prec \langle b_1, \dots, b_m \rangle$  iff  $k < m$  or ( $k = m$  and  $a_1 < b_1$ ) or ... or ( $k = m$  and  $a_1 = b_1$  and ... and  $a_{k-1} = b_{m-1}$  and  $a_k < b_m$ ).

**Lemma 1.5  $\pi$  is an injection: for any  $A, B$  of any  $\mathcal{D}$ :  $\pi(A) \neq \pi(B)$ , if  $A \neq B$ .** Proof by induction on the height of  $A$ .

## 2 Normalisation

The idea of the normalisation proof is as follows: first expand the implicative cuts of largest degree, then convert the cuts of largest degree of a given deduction. Expansions are done first, because they are the bad, complexity increasing part of implicative conversions. Only implicative conversions have such bad parts.

**Definition 2.1** An *expansion* puts the subdeduction leading to minor premise  $A$  of  $\rightarrow E$  applied on implicative cut  $A \rightarrow B$  on top of every assumption  $[A]$  discharged by  $\rightarrow I$ , which introduces implicative cut  $A \rightarrow B$ .

$$\frac{\frac{[A]^u \quad \vdots}{\vdots} \quad \frac{A \quad \frac{B}{A \rightarrow B} \rightarrow I}{B} \rightarrow E}{\vdots} \text{ expands to } \frac{\frac{\vdots \quad \frac{B}{A \rightarrow B} \rightarrow I}{A \quad \frac{B}{A \rightarrow B} \rightarrow I} \rightarrow E}{B} \rightarrow E$$

A implicative cut  $A \rightarrow B$  is *expanded*, if the subdeduction leading to the minor premise  $A$  is put on top of every discharged assumption  $[A]$ . A implicative cut  $A \rightarrow B$  is *free* iff it is not expanded and it is of largest degree in a given deduction and there is no other unexpanded implicative cut of largest degree in the subdeduction leading to minor premise  $A$  of cut  $A \rightarrow B$ .

**Lemma 2.2** Single Expansion of a free cut

**If in deduction  $\mathcal{D}$  is one free cut  $C \rightarrow D$  of largest degree  $k$  an expansion of  $C \rightarrow D$  gives a deduction  $\mathcal{D}^*$  s.t. at most one free cut  $A \rightarrow B$  of largest degree  $k$  is in  $\mathcal{D}^*$  and height of  $A \rightarrow B$  is lower than height of  $C \rightarrow D$ .**

Proof by inspection of expansion of free cuts. Consider the deduction at the left immediately above and assume cut  $A \rightarrow B$  to be of largest degree. Assume further a free cut  $C \rightarrow D$  of largest degree to be located in the subdeduction leading to minor premise  $A$ , and assume cut  $A \rightarrow B$  to become free by expansion of  $C \rightarrow D$ . A further cut  $E \rightarrow F$  of largest degree, which would become free by expansion of  $C \rightarrow D$ , must be located in the subdeduction leading to minor premise  $A$ . But if  $E \rightarrow F$  is in subdeduction of  $A$  and becomes free by expansion of  $C \rightarrow D$ ,  $A \rightarrow B$  cannot become free by expansion of  $C \rightarrow D$ ; in this case  $A \rightarrow B$  could become free at most by expansion of  $E \rightarrow F$ . So, a cut like  $E \rightarrow F$  can not exist.

**Lemma 2.3** Expansion of a free cut

**If in deduction  $\mathcal{D}$  is one free cut  $A \rightarrow B$  of largest degree  $k$ ,  $\mathcal{D}$  can be expanded to a deduction  $\mathcal{D}^*$  with no free cut  $C \rightarrow D$  of largest degree  $k$ .**

Proof with the last lemma and an induction on the height of formulas in deduction trees. Expansion of  $A \rightarrow B$  with height  $m$  in  $\mathcal{D}$  gives a deduction  $\mathcal{D}^1$  with the last lemma s.t. at most one free cut  $C_1 \rightarrow D_1$  of height  $m - (k + 1)$  is in  $\mathcal{D}^1$ ; repeating this argument gives finally a deduction  $\mathcal{D}^*$  with no free cut of largest degree.

**Lemma 2.4** Observation on Expansions

**Paths of deductions remain of finite length under expansion.**

By inspection on expansions it is clear that paths of deductions may grow under expansion, but they remain finite.

**Lemma 2.5** Transfinite expansions of cuts

**All free cuts of largest degree  $k$  of a given deduction  $\mathcal{D}$  can be expanded s.t. a deduction  $\mathcal{D}^*$  results with no free cuts of largest degree  $k$ .**

Proof by induction on the sequence numbers of free cuts in  $\mathcal{D}$  with use of the lemma on expansions.

**Definition 2.6** *Conversions* for  $\rightarrow, \wedge, \forall, \perp$  are as usual; two are exemplified.

$$\begin{array}{ccc} \vdots & & \vdots \\ \vdots & \frac{B}{A \rightarrow B} \rightarrow I & \vdots \\ \frac{A \rightarrow B}{B} \rightarrow E & \text{converts to} & B \\ \vdots & & \vdots \end{array}$$

Conversions of implicative cuts  $A \rightarrow B$  will be applied only in cases where  $\rightarrow I$  does not discharge assumptions  $A$ .

$$\begin{array}{ccc} \vdots & \vdots & \\ \frac{A(x/0) \quad A(x/0') \quad \dots}{\forall x A} \forall I & \text{converts to} & \vdots \\ \frac{\forall x A}{A(x/k)} \forall E & & A(x/k) \\ \vdots & & \vdots \end{array}$$

**Definition 2.7** In the sequel a certain configuration of cuts, i.e. a tower of cuts, is used. Immediately below is a simple example of a tower of cuts, presupposed cuts  $A \wedge B$  and  $C \rightarrow B$  have the same, largest degree of the given deduction:

$$\begin{array}{c}
 \vdots \quad \vdots \\
 \frac{A \quad B}{A \wedge B} \wedge I \\
 \vdots \quad \frac{B}{C \rightarrow B} \rightarrow I \\
 \frac{C \quad C \rightarrow B}{B} \rightarrow E \\
 \vdots
 \end{array}$$

So, a *tower of cuts* is a finite sequence of cuts  $\langle A_1, \dots, A_m \rangle$  of the same, largest degree in a given deduction, where the conclusion of the elimination rule applied on cut  $A_{k+1}$  is the main premise of the introduction rule applied on cut  $A_k$  for  $k < m$ . The *length* of a tower of cuts is the number of cuts in the sequence. A tower of cuts is *expanded* iff its implicative cuts are expanded.

**Lemma 2.8** Conversion of an expanded tower of cuts

**Given a deduction  $\mathcal{D}$  with one tower of cuts  $\langle A_1, \dots, A_n \rangle$  of largest degree  $k$  and all cuts expanded, this tower can be converted leading to a deduction  $\mathcal{D}^*$  with no cut of largest degree  $k$ .**

Proof. Convert the tower of cuts  $\langle A_1, \dots, A_n \rangle$  from below by induction on its length.

**Lemma 2.9** Transfinite conversions of expanded towers of cuts

**Given a deduction  $\mathcal{D}$ , where every cut of largest degree  $k$  is expanded,  $\mathcal{D}$  can be converted to a deduction  $\mathcal{D}^*$  with largest degree below  $k$ .**

Proof by induction on the sequence numbers of  $\mathcal{D}$  with the preceding lemma.

**Theorem 2.10** Normalisation of any  $\Omega A$  deduction

**Any deduction in  $\Omega A$  can be normalised.**

Proof. Assume a deduction  $\mathcal{D}$  of  $\Omega A$  with largest cut degree  $k$ . First expand the implicative cuts of largest degree  $k$ , than convert all cuts, i.e. towers of cuts of largest degree  $k$  with the preceding lemmata. Repeat this process  $k$  times.

Finally put the inductions together: expansion of implicative cuts of largest degree is done within  $\omega \cdot \omega^\omega = \omega^\omega$ , and conversion of towers of cuts of largest degree again is done in  $\omega \cdot \omega^\omega = \omega^\omega$ . This has to be repeated at most  $\omega$  times, so the complete induction is in  $\omega^\omega \cdot 2 \cdot \omega = \omega^\omega \cdot \omega$ .

### 3 References

- G. Gentzen, 1936, Die Widerspruchsfreiheit der reinen Zahlentheorie. In: Mathematische Annalen, 112, p.493-565.
- G. Mints, 1975, Finite Investigations of infinite derivations (Russian). English Translation in: Journal of Soviet Mathematics, 10, 1978, p.548-596.
- D. Prawitz, 1971, Ideas and Results in Proof Theory. In: J.E. Fenstad, Ed., Proceedings of the Second Scandinavian Logic Symposium, p.237-309.
- K. Schuette, 1950, Beweistheoretische Erfassung der unendlichen Induktion. In: Mathematische Annalen, 122, p.47-65.

