Days in Logic 2012: Celebrating Turing

6-8 February, 2012

University of Évora

Preface

The Days in Logic meetings are a biannual event held in Portugal, with the aim of promoting the exchange of knowledge and ideas between researchers with a common interest in Logic research topics.

The 2012 edition, being coincident with the centenary of Alan Turing's birth, will be specially dedicated to celebrate the life and work of one of the scientists with more impact in Computer Science.

The Days in Logic 2012 meeting will consist of four tutorials with three sessions of 60 minutes, by four invited speakers:

Nachum Dershowitz, Universidade de Tel Aviv - *Turing centenary lectures* This tutorial will describe the fundamental work of Alan Turing in the fields of Logic, Mathematics and Computer Science and its consequences. In particular:

1. A proof of the Church-Turing thesis: We will look at the history of the Church-Turing thesis, which states that every effectively computable function is computable in the Turing sense. An axiomatizing of effective computation allows to proof the thesis.

2. Beyond the Church-Turing thesis: We will present arguments for and against hyper-computation, the notion that human beings or structures can compute non-computable functions (in the Turing sense).

3. An extension to the Church-Turing thesis: We will show an extended Church-Turing thesis in the sense that every effective algorithm can be simulated in an effective way by a Turing Machine. In fact, such algorithm is generated by an abstract state machine, which is simulated by a machine of random access with a linear overhead.

Maribel Fernández, King's College, Londres - *Nominal techniques* Nominal logic is a generalization of first-order logic that allows us to deal with syntax involving binding operators in an elegant and practical way. Nominal systems maintain a strict distinction between atoms (variables that may be bound by a special abstraction operation) and meta-variables (or just variables) which cannot be bound, giving the framework a pronounced first-order character since substitution is not capture-avoiding. In nominal syntax, bound entities are explicitly named (rather than using a nameless syntax such as de Bruijn indices), yet we get a formalism that respects alpha-equivalence and can be directly implemented. Nominal unification is decidable (unlike higher-order unification), and efficient unification algorithms are available. Nominal rewriting can be seen as a form of higher-order rewriting with a first-order syntax and built-in alpha-equivalence.

In these lectures, we will introduce the nominal approach to the specification of systems with binding operators, and we will show how good properties of first-order rewriting are inherited by the nominal rewriting framework. We will

describe an efficient matching algorithm that has been used to implement a nominal rewriting tool.

Pedro Quaresma, Universidade de Coimbra - *Automatic theorem proving in Geometry* Proving geometric theorems has been an interesting challenge is automatic theorem provers, ever since the seminal works from Gelernter in 1959 an others, until the current provers based on algebraic methods (Wu 2000, Wang 1995, Kapur 1986, Li 2000) and semi-algebraic (Chou 1996). A particularly important issue is proving theorems that require additional elements to the original construction.

In this tutorial we will present the journey taken by Geometric Automated Theorem Provers (GATP) from the axiomatic systems (that although having the advantage of working over axiomatic geometric systems and producing geometric proofs, are in general very restrictive in the type of geometric construction one can consider) to the algebraic systems. In between we will consider mixed systems, such as the area method, probabilistic proof, among others.

We will also present some of the current challenges of GATPs, in particular concerning the formalization of geometric systems, the iterative and interactive proof of theorems, the generation of proofs understood by geometers and visual proofs and the integration with systems of dynamic geometry.

Guy Wallet, Universidade de La Rochelle - *Nonstandard Type Theory* The aim of these lectures is to introduce to Per Martin-Lf's ideas about a constructive approach of Nonstandard Analysis using the intuitionistic concept of choice sequence reconsidered within Constructive Type Theory. For the first time, these ideas appeared in the article Mathematics of Infinity published in 1989. Although he has published nothing more on this topic, Martin-Lf never stopped his research toward a general Nonstandard Type Theory. Following some recent discussions with him, a more elaborate version of this theory is going to emerge. These lectures will give the state of the art on this subject.

The event's program includes also sessions for contributed talks with a duration of 30 minutes each, where participants of the event will be able to present their work. The abstracts for the contributed talks, are presented in the following pages.

This event is organized by:

- Sandra Alves, Dept. Computer Science and LIACC, University of Porto;
- Mário Jorge Edmundo, DCeT, University Aberta and CMAF - University of Lisbon;
- Reinhard Kahle, DM, New University of Lisbon and CENTRIA;
- Imme van den Berg, CIMA, University of Évora.

Distinguishing two probability ensembles with one sample from each ensemble

Andreia Teixeira

Faculdade de Ciências da Universidade do Porto and Instituto de Telecomunicações

We study a new method for distinguishing two probability ensembles in which the distinguisher receives as input two samples, one from each ensemble; it will be called the "one from each" method. We prove that there are ensembles distinguishable by this method, but indistinguishable by the *k samples method* previously studied in [1, 2] for any k. We also show that if non-uniform distinguishers (probabilistic circuits) are used, the "one from each" method is not more powerful than the classical one. We moreover obtain that there are classes of ensembles, such that

- any two members of the class are "easily distinguishable" (a definition introduced in this paper) using one sample from each ensemble; the proof uses a variant of Ambainis single message protocol [3] for string equality;
- there are pairs of ensembles in the class that are indistinguishable by the k samples method, for any value of k.

References

[1] O. Goldreich and B. Meyer. Computational indistinguishability: algorithms vs. circuits. *Journal of Theoretical Computer Science*, 191(1-2):215–218, 1998.

[2] O. Goldreich and M. Sudan. Computational Indistinguishability: A Sample Hierarchy. *Electronic Colloquium on Computational Complexity (ECCC)*, 5(17), 1998.

[3] A. Ambainis. Communication Complexity in a 3-Computer Model. *Algorithmica*, 16(3):298–301, 1996.

Individual Zero knowledge

André Souto[1]

Universidade do Porto and Instituto de Telecomunicações

In [2], Goldwasser, Micali and Rackoff introduced the concept of interactive proof systems. In these systems, there is a prover with unlimited computational power, and a verifier running in polynomial time that does not have access to the relevant information. The goal of the prover is to convince the verifier of the validity of some statement, like "$x \in L$", for some language L. The verifier does not trust the prover and only accepts the validity of the assertion at the end if the prover manages to convince him of the validity of the statement. Thus, a natural question arises: *"What knowledge does the verifier gain during the interaction?"*.

The definitions of zero knowledge and witness hiding are based on the existence of simulators or witness extractors. One might raise some questions about such "operational" definitions. For instance, can there be protocols which actually leak no information to the verifier, but which are so obfuscating that there does not exist a simulator? Perhaps there is a more fundamental way to define zero knowledge, and the existence of a simulator would be just a device to prove it. Another concern is that the existence of a simulator might be too weak to guarantee that no information is leaked to the verifier in any instances of the protocol. These questions motivate us to propose a new approach based on Kolmogorov complexity [4, 3, 1], a rigorous measure of the amount of information contained in an object, usually a string, as the size of the smallest program that generates that object. The definition we give is closer to the intuitive idea we have of what it means to be zero knowledge, and is not "operational" in the sense that it does not require the existence of a simulator (or witness extractor for witness hiding) to argue that no knowledge is leaked.

Hence, individual witness hiding proofs are based on the knowledge conveyed on individual communications. The amount of information that any polynomial time verifier can gain from an individual communication is the difference between the time-bounded Kolmogorov complexity of the *"proof"* by itself and the time-bounded Kolmogorov complexity of the *"proof"* given the communication. So, a protocol is individual witness hiding if in all communications, the advantage of the verifier is, at most, a logarithmic term. In this work, we prove that the well-known zero knowledge protocol for the Quadratic residues problem (**QR**) described by [5] is not individual witness hiding and propose an individual witness hiding protocol for the same problem. We also prove that the new protocol is not statistical zero knowledge with respect to the corresponding simulator for **QR**.

[1]andresouto@dcc.fc.up.pt; The authors from U. Porto are partially supported by CSI^2 (PTDC/EIA-CCO/099951/2008). This is a work in progress with Luís Antunes, Sophie Laplante, Paulo Mateus and Andreia Teixeira.

We thank Armando Matos and Sophie Laplante for helpful discussions and suggestions.

References

[1] G. Chaitin. On the Length of Programs for Computing Finite Binary Sequences. *Journal of the ACM*, 13:547–569, 1966.

[2] S. Goldwasser and S. Micali and C. Rackoff. The knowledge complexity of interactive proof-systems *Proceedings of the Symposium on Theory of Computing*, 291–304, 1995.

[3] A. Kolmogorov. Three approaches to the quantitative definition of information. *Problems in Information Transmission*, 1:1–7, 1965.

[4] R. Solomonoff. A formal theory of inductive inference, Part I. *Information and Control*, 7(1):1–22, 1964.

[5] D. Stinson. *Cryptography: Theory and Practice, 1st edition.*, CRC Press. 1995.

PρLog and its Applications

Jorge Coelho[1], Besik Dundua[2], Mário Florido[2], Temur Kutsia[3]and Mircea Marin[4]

PρLog is a system [2] based on ρLog calculus [4] and extends Prolog with strategic conditional transformation rules. These rules define transformation steps on term sequences, also known as *hedges*. Strategy combinators help to combine strategies into more complex ones in a declaratively clear way. Transformations are nondeterministic and may yield several results, which fits very well into the logic programming paradigm. Strategic rewriting separates term traversal control from transformation rules. This allows the basic transformation steps to be defined concisely. The separation of strategies and rules makes rules reusable in different transformations.

PρLog uses four different kinds of variables in one framework, which allows to traverse hedges in single/arbitrary width (with individual and sequence variables) and terms in single/arbitrary depth (with functional and context variables). It facilitates flexibility in matching, providing a possibility to extract an arbitrary subhedge from a hedge, or to extract subterms at arbitrary depth. These capabilities together with strategies enable highly declarative programming style that is expressive enough to support concise implementations for specifying and prototyping deductive systems, solvers for various equational theories, tools for XML querying and transformation, etc.

The talk will be based on the work published in [1, 3].

References

[1] J. Coelho, B. Dundua, M. Florido, and T. Kutsia. A rule-based approach to xml processing and web reasoning. In P. Hitzler and T. Lukasiewicz, editors, *RR*, volume 6333 of *Lecture Notes in Computer Science*, pages 164–172. Springer, 2010.

[2] B. Dundua and T. Kutsia. PρLog. Version 0.9. Available from: `http://www.risc.uni-linz.ac.at/people/tkutsia/software.html`.

[3] B. Dundua, T. Kutsia, and M. Marin. Strategies in PρLog. *EPTCS*, 15:32–43, 2010.

[4] M. Marin and T. Kutsia. Foundations of the rule-based system ρlog. *Journal of Applied Non-Classical Logics*, 16(1-2):151–168, 2006.

[1]ISEP & LIACC, Porto, Portugal, jcoelho@liacc.up.pt
[2]DCC-FC & LIACC, University of Porto, Portugal, fbdundua@dcc.fc.up.pt
[2]DCC-FC & LIACC, University of Porto, Portugal, amf@dcc.fc.up.pt
[3]RISC, Johannes Kepler University, Linz, Austria, kutsia@risc.uni-linz.ac.at
[4]Department of Computer Science, West University of Timisoara, Romania, marmircea@gmail.com

On the Descriptional Complexity of Regular Languages Operations

Eva Maia, Nelma Moreira and Rogério Reis
{emaia,nam,rvr}@dcc.fc.up.pt

CMUP & DCC - FCUP
R. do Campo Alegre 1021/1055, 4169-007 Porto, Portugal

Descriptional complexity studies the measures of complexity of languages and operations. Usually, the descriptional complexity of an object is its shortest description which can be analyzed in the worst or average case. For each measure, it is important to know the size of the smallest representation for a given language and how the size varies when several such representations are combined or transformed. These studies are motivated by the need to have good estimates of the amount of resources required to manipulate those representations. This is crucial in new applied areas where automata and other models of computation are used, for instance, for pattern matching in bioinformatics or network security, or for model checking or security certificates in formal verification systems. In general, having succinct objects will improve our control on software, which may become smaller, more efficient and easier to certify.

Among formal languages, regular languages are fundamental structures in Computer Science. One of the most studied complexity measures for regular languages is the number of states of its minimal (complete) deterministic finite automaton (state complexity of the language). The state complexity of an operation over languages is the complexity of the resulting language as a function of the complexities of its arguments [4]. Both concepts can be extended to other models of computation (nondeterministic automata, regular expressions, etc.), other measures (number of transitions, number of symbols, etc.), and other subclasses of regular languages [3, 2].

In this talk we survey some results on operational state complexity of regular languages and present recent work on the operational transition complexity of incomplete deterministic finite automata, a subject that only very recently has been investigated [1].

References

[1] Yuan Gao, Kai Salomaa, and Sheng Yu. Transition complexity of incomplete dfas. *Fundam. Inform.*, 110(1-4):143–158, 2011.

[2] Markus Holzer and Martin Kutrib. Nondeterministic finite automata - recent results on the descriptional and computational complexity. *Int. J. Found. Comput. Sci.*, 20(4):563–580, 2009.

[3] Sheng Yu. State complexity: Recent results and open problems. *Fundam. Inform.*, 64(1-4):471–480, 2005.

[4] Sheng Yu, Qingyu Zhuang, and Kai Salomaa. The state complexities of some basic operations on regular languages. *Theor. Comput. Sci.*, 125(2):315–328, 1994.

A note on Spector's consistency proof of analysis

Fernando Ferreira
Universidade de Lisboa

In 1962, Clifford Spector gave a consistency proof of analysis using so-called bar recursors. His paper extends an interpretation of arithmetic given by Kurt Godel in 1958. Spector's proof relies crucially on the interpretation of the so-called (numerical) double negation shift principle. The argument for the interpretation is ad hoc. On the other hand, William Howard gave in 1968 a very natural interpretation of bar induction by bar recursion. We show directly that, within the framework of Godel's interpretation, (numerical) double negation shift is a consequence of bar induction.

A unified view over the bounded functional interpretations

Gilda Ferreira
CMAF - Universidade de Lisboa and NIM - Universidade Lusófona

Bounded functional interpretations are variants of functional interpretations where bounds (rather than precise witnesses) are extracted from proofs. These have been particularly useful in computationally interpreting non-computational principles such as weak König's lemma. In this talk we present a family of bounded functional interpretations – in the form of a parametrised interpretation – of both intuitionistic logic and (a fragment of) intuitionistic linear logic. We show how three different instantiations of the parameters give rise to three known bounded interpretations whose bounds occur at the level of the interpretation of formulas: the bounded functional interpretation [6], bounded modified realizability [5] and confined modified realizability [2].

The present unified view over the bounded interpretations was inspired in a previous (well-succeeded) unification effort concerning the well-known functional interpretations of intuitionistic logic such as Gödel's dialectica interpretation [7], Diller-Nahm interpretation [1] and Kreisel's modified realizability [8] (see [9], [11], [10] and [3]).

This is joint work with Paulo Oliva and is available in [4].

References

[1] J. Diller and W. Nahm. Eine Variant zur Dialectica interpretation der Heyting Arithmetik endlicher Typen}.Arch. Math. Logik Grundlagenforsch , 16:49–66, 1974.

[2] G. Ferreira and P. Oliva, Confined modified realizability}. Mathematical Logic Quarterly, 56(1):13–28, 2010.

[3] G. Ferreira and P. Oliva. Functional interpretations of intuitionistic linear logic. In *Logical Methods in Computer Science*, 7(1):1–22, 2011.

[4] G. Ferreira and P. Oliva. on bounded functional interpretations. In *Annals of Pure and Applied Logic*. In Press, available online 4 January 2012.

[5] F. Ferreira and A. Nunes. Bounded modified realizability.The Journal of Symbolic Logic, 71:329–346, 2006.

[6] F. Ferreira and P. Oliva. Bounded functional interpretation, Annals of Pure and Applied Logic, 135:73–112, 2005.

[7] K. Gödel. Ueber eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. Dialectica, 12:280–287, 1958.

[8] G. Kreisel. Interpretation of analysis by means of constructive functionals of finite types. In A. Heyting, editor, *Constructivity in Mathematics*, pages 101–128. North Holland, Amsterdam, 1959.

[9] P. Oliva. Unifying Functional Interpretations. Notre Dame Journal of Formal Logic, 47(2):263–290, 2006.

[10] P. Oliva. Modified realizability interpretation of classical linear logic. In *Proc. of the Twenty Second Annual IEEE Symposium on Logic in Computer Science LICS'07*. IEEE Press, 2007.

[11] P. Oliva. Computational interpretations of classical linear logic. In *Proceedings of WoLLIC'07, LNCS 4576*, pp. 285–296. Springer, 2007.

P, NP and Pspace

Isabel Oitavem

CMAF-UL and FCT-UNL

We give a characterization of NP using a recursion scheme with tier 0 pointers. This extends the Bellantoni-Cook characterization of Ptime and, simultaneously, it is a restriction of a recursion-theoretic characterization of Pspace.

References

[1] S. Bellantoni and S. Cook, A new recursion-theoretic characterization of Polytime functions, Computational Complexity, vol. 2, 1992, pp. 97-110.

[2] I. Oitavem, Characterizing Pspace with pointers, Mathematical Logic Quarterly 54, N.3, 2008, pp.317-323.

[3] I. Oitavem, A recursion-theoretic approach to NP, Annals of Pure and Applied Logic 162/8, 2011, pp.661-666.

1 On invertibility of linear finite automata and Cryptography

Ivone Amorim, António Machiavelo and Rogério Reis
ivone.amorim@dcc.fc.up.pt

The concept of public key criptography was introduced by Diffie, Hellman and Merkle in 1976, and in 1978, Rivest, Shamir and Aldeman presented the first public key cryptosystem, called RSA. The RSA system and most of the public key cryptosystems created in the following years were based in complexity assumptions related to number theory problems. This kind of cryptosystems are computationally expensive in time as well as in space, and their security relies on a very small set of problems. The cryptographic schemes based on finite automata (named FAPKC) seem to be a good alternative to classical systems, since they are computationally attractive and seem suitable for application on devices with very limited computational resources [1].

The first FAPKC system was proposed in 1985, by R. Tao and S. Chen (an English description of it can be found in [2]). Some variants of this system were proposed in the following years, by R. Tao and some other researchers in China. The FAPKC schemes are based on invertibility theory of finite automata, and their security relies on the difficulty of inversion of nonlinear finite automata and of factoring matrix polynomials over $\mathbb{F}_q$ [1].

One of the big challenges of finite automata based cryptography is having an efficient method to generate finite automata with the required conditions for cryptographic purposes. The techniques to construct such automata came from the study of the invertibility theory of finite automata.

In this talk we intend to describe a general FAPKC scheme, and to present some recent results on the invertibility theory of linear finite automata [3]. These results give a new condition to verify if a linear finite automata with memory is weakly invertible with delay τ, which uses the Smith's normal form of a polynomial matrix, and give a new way to construct a weak inverse with delay τ of an invertible linear finite automata.

References

[1] Renji Tao. *Finite Automata and Application to Cryptography.* Springer Publishing Company, Incorporated, 2009.

[2] Renji Tao and Shihua Chen. Two varieties of finite automaton public key cryptosystem and digital signatures. *Journal of Computer Science and Technology.*, 1(1):9-18, 1986.

[3] Ivone Amorim, António Machiavelo and Rogério Reis. On Linear Finite Automata and Cryptography. Technical report, Centro de Matemática da Universidade do Porto, Faculdade de Ciências, Universidade do Porto, 2011.

Applying logic to Hillam's theorem on fixed point iterations

Jaime Gaspar

www.jaimegaspar.com, mail@jaimegaspar.com

Hillam's theorem is a charming little result characterising the convergence of fixed point iterations x_n of continuous functions from $[0,1]$ to $[0,1]$:

$$x_n \text{ converges if and only if } x_{n+1} - x_n \to 0.$$

On the analytical side, we present a quantitative version of Hillam's theorem that relates "finitary" rates of convergence of x_n and "finitary" rates of convergence of $x_{n+1} - x_n$.

On the logical side, we explain why we have to content ourselves with "finitary" rates of convergence instead of full rates of convergence, and how the relation between the rates is obtained by logical tools.

On combined connectives

João Rasga

Dep. Matemática, Instituto Superior Técnico, Universidade Técnica de Lisboa,
SQIG, Instituto de Telecomunicações, Portugal

Combined connectives arise in combined logics. In fibrings, such combined connectives are known as shared connectives and inherit the logical properties of each component. A new way of combining connectives (and other language constructors of propositional nature) is proposed by inheriting only the common logical properties of the components. A sound and complete calculus is provided for reasoning about the latter. The calculus is shown to be a conservative extension of the original calculus. Examples are provided contributing to a better understanding of what are the common properties of any two constructors, say disjunction and conjunction. This talk reports on: *A. Sernadas, C. Sernadas, and J. Rasga. On combined connectives. Logica Universalis, 5:205–224, 2011.*

Stratified Semantics in First-Order Logic

José Roquette,

Departamento de Matemática

Instituto Superior Técnico, Lisbon, Portugal

jroquet@math.ist.utl.pt

The ontology underlying this work is *realism*: mathematical objects do exist, independently of the human mind. So, our semantics starts with them. But the various nature of the mathematical objects in what concerns their complexity, our knowledge of them or the possibility to make them explicit (for example, innitesimal or ilimited real numbers in *nonstandard analysis*) is a strong motivation to consider their distribution into levels or strata. The *stratification* depends on the selected property (or properties) of the mathematical objects that are the subject-matter of our study.

We begin by considering a first-order language, $\mathcal{L}$, with equality, no constant symbols and no function symbols, like the language of *ZFC* , or even the languages of *IST (Nelson's internal set theory)*, or *HST (Hrbaček's set theory)*, theories that are largely used in *nonstandard analysis*. Then we add to $\mathcal{L}$ a new constant symbol, $\mathbf{0}$, intended to denote a chosen mathematical object at the *ground level*, and a new binary relation symbol of *precedence of level*, $\sqsubseteq$, thus defining a new language, $\mathcal{L}_*$. To each level, we associate a set of mathematical objects and a set of basic truths about them, formulated in $\mathcal{L}_*$ enriched with a constant symbol for each mathematical object associated with the level. Together, the level and the associated sets of mathematical objects and basic truths determine a *context*. Contexts depend on the choice of the stratification and determine a classical structure.

A sentence φ of the union of all enriched languages, $(\mathcal{L}_*)_+$, has a *meaning*, and consequently a *truth-value*, only within a context where we may interpret all the *closed terms* of φ as elements of the respective set of mathematical objects. Since contexts depend on the mathematician's choice of the stratification, we do not have *realism in truth-value* for the sentences of $(\mathcal{L}_*)_+$, nor do we have *structural realism* for the above mentioned classical structures. In more *down-to-earth* (and less interesting) language: we introduce *stratification* in first-order logic (for languages like $\mathcal{L}$); then we discuss *soundness*, *conservativeness* and *completeness*.

Cramer's Rule applied to flexible systems of linear equations

Júlia Justino

EST Setubal, Departamento de Matemática.

We study systems of linear equations with coefficients of first and/or second member having uncertainties of type $o(.)$ or $O(.)$; in fact, we do not use this functional form of neglecting but an alternative formulation within nonstandard analysis using sets of infinitesimals. We call this kind of systems flexible systems of linear equations.

In some cases an exact solution may not exist but we present a general theorem that guarantees the existence of an admissable solution, in terms of inclusion. This admissible solution is produced by Cramer's Rule; depending on the size of the uncertainties appearing in the matrix of coefficients and the second member some adaptations may be needed.

Monadic translation of classical sequent calculus and strong normalisation

Luís Pinto

Centro de Matemática - Universidade do Minho

Classical logic gives a meaningful way to extend the basic setting of functional programming provided by lambda-calculus and intuitionistic logic, where control operators like call-cc acquire a logical foundation. In particular, its formulation in the sequent calculus format has been successfully used, for example, to account for dualities in computation.

Cps (continuation-passing style) translations have their origin as a compilation technique for functional programs, but are related to double-negation translations in logic. It is known that monads are an useful concept to factor cps translation of lambda-calculus. Specifically, Moggi's monadic meta-language can be used to factor traditional cps translations of lambda-calculus into a monadic translation followed by an instantiation to the continuations-monad.

We adapted this methodology in order to obtain modular and syntactic proofs of strong normalisation for the call-by-name (cbn) and the call-by-value (cbv) fragments of the classical sequent calculus $\overline{\lambda}\mu\tilde{\mu}$ by Curien and Herbelin. Additionally, we guaranteed that our translations strictly simulate reduction (i.e. one step in the source calculus implies one or more steps in the target), so that strong normalisation of the target can be inherited by the source.

This led us:

- to the definition of a meta-language for classical logic, which is a monadic reworking of Parigot's $\lambda\mu$-calculus, and whose intuitionistic restriction is a variant of Moggi's meta-language;
- to the definition of monadic translations of the cbn and the cbv fragments of $\overline{\lambda}\mu\tilde{\mu}$ into the new monadic meta-language;
- to cps translations into simply-typed lambda-calculus, obtained by composition of the monadic translations with the instantiation to the continuations-monad.

The results readily extend to second-order logic, with polymorphic lambda-calculus as target, giving new strong normalisation results.

(Joint work with José Espírito Santo (Centro de Matemática, Univ. Minho), Ralph Matthes (IRIT- CNRS and Univ. Toulouse III) and Koji Nakazawa (School of Informatics, Univ. Kyoto).)

The Application of Lindenbaum's Theorem

René Gazzari

Centria, FCT, Universidade Nova de Lisboa

David W. Miller raises in his article *"Some Lindenbaum Theorems Equivalent to the Axiom of Choice"* the problem to re-prove the well known equivalences of some variants of Lindenbaum's Theorem for deductive systems (each equivalent to the Axiom of Choice) *without an application* of the Axiom of Choice.[1] At first glance, this demand seems to be quite clear, but trying to formulate a satisfactory criterion unveils the underlying problematic.

Providing such a criterion involves several problems. The relationship between informal mathematical language and its formalisation has to be discussed. For having an appropriate formalisation, close to informal language, we have to enrich our formal language and extend the possibilities of the calculus. Furthermore, we have to know, which formulas are applied in a given proof, we have to identify the problematic applications and decide, if a version of Lindenbaum's Theorem is applied there or another formula forbidden by our demands. This certainly involves, on the one hand, the distinction between logically equivalent formulas (as the Axiom of Choice and Lindenbaum's Theorem) and, on the other hand, the identification of formulas not being logically equivalent (there are several important, but not equivalent versions of Lindenbaum's Theorem).

Our final aim is to provide an appropriate formal criterion, whether a formalisation of a proof, given in informal language, qualifies for being a proof of the equivalence of some versions of Lindenbaum's Theorem respecting our demands. This goal is strongly related to the philosophical problem of pure proofs not using notions extraneous to them. The Axiom of Choice and other variants, as the Well Ordering Theorem, are extraneous to the set theoretical theory of deductive systems and their Lindenbaum's Theorems. By defining the notion of a version of Lindenbaum's Theorem in contrast to other variants of the Axiom of Choice, we transfer this problem of pureness to formulas. Conversely, any satisfactory criterion for our demands seems to be at least a necessary condition of pureness.

In our talk we first give a brief introduction to deductive systems and the problem raised by Miller. We also mention the general strategy, used by him in his article and also in my diploma thesis, to provide some (partial) solutions to the problem. Subsequently, we discuss our demands in some more details to clarify the underlying problematic of defining an adequate formal criterion. If there is time left, we also sketch some ideas, how to catch formally the notion of a version of Lindenbaum's Theorem and how to find proofs satisfying our demands.

[1] David W. Miller: Some Lindenbaum Theorems Equivalent to the Axiom of Choice, *Logica Universalis* **1**, 2007, pp. 183–199.