日本学術振興会研究拠点形成事業

数理論理学とその応用に関するワークショップ

JSPS Core-to-Core Program

Workshop on Mathematical Logic and its Application

2016 年 9 月 16 日・17 日（金曜日・土曜日）
京都大学、吉田南キャンパス、総合人間学部棟 1401 教室
September 16 - 17, 2016,
Faculty of Integrated Human Studies Building, room 1401
Kyoto University

Time Table

Fri. 16 September	Sat. 17 September
Schwichtenberg (9:10-9:45)	Sato (9:10-9:45)
Li (9:45-10:20)	Akiyoshi (9:45-10:20)
Coffee break	*Coffee break*
Pelupessy (10:50-11:25)	Kimura (10:50-11:25)
Yokoyama (11:25-12:00)	Preining (11:25-12:00)
Lunch break	*Lunch break*
Setzer (13:30-14:05)	U. Berger (13:30-14:05)
de Brecht (14:05-14:40)	Maruyama (14:05-14:40)
Thies (14:40-15:15)	Matsumoto (14:40-15:15)
Coffee break	*Coffee break*
Fujiwara (15:45-16:20)	Kihara (15:45-16:20)
Kawai (16:20-16:55)	Nakazawa (16:20-16:55)
J. Berger (16:55-17:30)	Hirokawa (16:55-17:30)

Friday, 16 September

8:40 – 9:10 Registration and Opening

9:10 – 10:20 Session 1

9:10 Helmut Schwichtenberg

Continuity in constructive analysis

9:45 Wenjuan Li

Determinacy strength of infinite games in ω-languages recognized by variations of pushdown automata

10:20 – 10:50 (Coffee Break)

10:50 – 12:00 Session 2

10:50 Florian Pelupessy

Unprovability and some reverse mathematics which involve ordinals

11:25 Keita Yokoyama

Proof-theoretic strength and indicator arguments

12:00 – 13:30 (Lunch Break)

13:30 – 15:15 Session 3

13:30 Anton Setzer

Programming with objects in theorem provers based on Martin-Löf type theory

14:05 Matthew de Brecht

On the duality of topological Boolean algebras

14:40 Holger Thies

Analytic functions and small complexity classes

15:15 – 15:45 (Coffee Break)

15:45 – 17:30 Session 4

15:45 Makoto Fujiwara

Effective computability and constructive provability for existence sentences

16:20 Tatsuji Kawai

Elimination of binary choice sequences

16:55 Josef Berger

The fan theorem and convexity

Saturday, 17 September

9:10 – 10:20 Session 5

9:10 Masahiko Sato

Proof theory of the λ-calculus

9:45 Ryota Akiyoshi

Strong normalization for the parameter-free polymorphic lambda calculus based on the Ω-rule

10:20 – 10:50 (Coffee Break)

10:50 – 12:00 Session 6

10:50 Daisuke Kimura

Decidability of entailments in separation logic with arrays

11:25 Norbert Preining

Verification in Real computation

12:00 – 13:30 (Lunch Break)

13:30 – 15:15 Session 7

13:30 Ulrich Berger

Extraction of real Gray-code from proofs using non-deterministic implication

14:05 Yoshihiro Maruyama

Harmony, the Curry-Howard correspondence, and higher proof theory

14:40 Kei Matsumoto

Coherence spaces for resource-sensitive computation in analysis

15:15 – 15:45 (Coffee Break)

15:45 – 17:30 Session 8

15:45 Takayuki Kihara

Degrees of unsolovability in topological spaces with countable cs-networks

16:20 Koji Nakazawa

Compositional Z: confluence proofs for permutative conversion

16:55 Nao Hirokawa

Automated normalization analysis for term rewriting

Table of Contents

Strong normalization for the parameter-free polymorphic lambda calculus based on the Ω-rule.

Ryota Akiyoshi[1] and Kazushige Terui[2]

[1] WIAS, Waseda University, 1-6-1 Nishi Waseda, Shinjuku-ku, Tokyo, Japan, `georg.logic@gmail.com`
[2] RIMS, Kyoto University, Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto, Japan, `terui@kurims.kyoto-u.ac.jp`

Following Aehlig [1], we consider a hierarchy $\mathbf{F}^p = \{\mathbf{F}^p_n\}_{n\in\mathbf{N}}$ of parameter-free subsystems of System $\mathbf{F}$, where each $\mathbf{F}^p_n$ corresponds to $\mathbf{ID}_n$, the theory of n-times iterated inductive definitions (thus our $\mathbf{F}^p_n$ corresponds to the $n+1$th system of [1]). We here present two proofs of strong normalization for $\mathbf{F}^p_n$, which are directly formalizable with inductive definitions. The first one, based on the Joachimski-Matthes method [6], can be fully formalized in $\mathbf{ID}_{n+1}$. This provides a tight upper bound on the complexity of the normalization theorem for System $\mathbf{F}^p_n$. The second one, based on the Gödel-Tait method [7], can be locally formalized in $\mathbf{ID}_n$. This provides a direct proof to the known result that the representable functions in $\mathbf{F}^p_n$ are provably total in $\mathbf{ID}_n$. In both cases, Buchholz' Ω-rule ([2], [3], [5]) plays a central role.

References

1. K. Aehlig. Parameter-free polymorphic types. *Annals of Pure and Applied Logic*, 156:3–12, 2008.
2. Wilfried Buchholz. The $\Omega_{\mu+1}$-rule. In [4], pages 188–233, 1981.
3. W. Buchholz. Explaining the Gentzen-Takeuti reduction steps. *Archive for Mathematical Logic*, 40:255–272, 2001.
4. W. Buchholz, S. Feferman, W. Pohlers, and W. Sieg (editors). *Iterated Inductive Definitions and Subsystems of Analysis: Recent Proof-Theoretical Studies*, LNM 897, Springer, 1981.
5. W. Buchholz and K. Schütte. *Proof Theory of Impredicative Subsystems of Analysis*, Bibliopolis, 1988.
6. F. Joachimski and R. Matthes. Short proofs of normalization for the simply-typed lambda-calculus, permutative conversions and Gödel's T. *Archive for Mathematical Logic*, 42:59–87, 2003.
7. W. Tait. Intensional interpretations of functionals of finite type I. *Journal of Symbolic Logic*, 32(2):198–212, 1967.

The fan theorem and convexity

Josef Berger and Gregor Svindland

Mathematisches Institut, Ludwig-Maximilians-Universität München
Theresienstraße 39, 80333 München, Germany
jberger@math.lmu.de, svindla@math.lmu.de

The fan theorem is the following statement:

(FAN) Let B be a set of finite binary sequences. Assume that every infinite binary sequence has an initial part that belongs to B. Then there exist an N such that every infinite binary sequence has an initial part of length smaller than N that belongs to B.

This axiom plays an important role in Intuitionism, a philosophy of mathematics that was introduced by the Dutch mathematician L.E.J. Brouwer. We work in constructive mathematics in the tradition of Errett Bishop. Here, the fan theorem is neither provable nor falsifiable. Many theorems of analysis are constructively equivalent to the fan theorem. One example for such a theorem is:

(POS) Every positive-valued uniformly continuous function on the unit interval has positive infimum.

In [1], we have shown that, under the additional condition of convexity of the function, POS is constructively valid; this results has consequences, see [2].

Is there a corresponding constructively valid 'convex fan theorem'?

References

1. Josef Berger and Gregor Svindland, *Convexity and constructive infima*, Archive for Mathematical Logic (2016)
2. Josef Berger and Gregor Svindland, *A separating hyperplane theorem, the fundamental theorem of asset pricing, and Markov's principle*, Annals of Pure and Applied Logic 167 (2016), pp. 1161–1170.

Extraction of real Gray-code from proofs using non-deterministic implication

Ulrich Berger

Department of Computer Science, Swansea University,
Singleton Park, Swansea SA2 8PP, UK,
u.berger@swansea.ac.uk

This is joint work with Hideki Tsuiki.

Gray code for real numbers introduced by Tsuiki [1] requires non-deterministic computation. We introduce an intuitionistic system with a new form of non-deterministic implication that allows for the extraction of real Gray code. We study the logical property of the new connective and sketch the extraction of effective translations between Gray code and signed digit representation.

[1] Hideki Tsuiki: Real Number Computation through Gray Code Embedding. TCS 284(2):467–485, 2002.

On the duality of topological Boolean algebras

Matthew de Brecht

Graduate School of Human and Environmental Studies, Kyoto University, Japan
matthew@i.h.kyoto-u.ac.jp

This talk is an introduction to aspects of Stone duality for Boolean algebras and a result by D. Papert Strauss on topological Boolean algebras. The main results are well known, and our approach is closely related to Hofmann-Mislove-Stralka duality and P. Taylor's Abstract Stone Duality. However, it is our hope that this introduction will make the results more accessible to computer scientists and logicians, and provide guidelines for developing more general dualities involving topological algebra.

We will work within the category of zero-dimensional countably based locally compact Hausdorff spaces, but focus on the subcategory C consisting of the compact spaces and the subcategory D consisting of the discrete spaces.

The two point discrete space 2 defines a contravariant functor $2^{(-)}$ which maps a space X to the space 2^X of clopen subsets of X with the compact-open topology. It is easy to see that $2^{(-)}$ maps D into C, and conversely maps C into D, and that the double exponential functor $2^{2^{(-)}}$ is a monad when restricted to either C or D.

Writing $Bool(D)$ (respectively $Bool(C)$) for the subcategory of D (respectively C) of monad algebras of $2^{2^{(-)}}$ and algebra homomorphisms, one can show that $Bool(D)$ and $Bool(C)$ are precisely the subcategories of topological Boolean algebras within D and C, respectively. Furthermore, every algebra X in $Bool(D)$ (respectively $Bool(C)$) is of the form 2^Y for some space Y in C (respectively D). This forms a dual equivalence between C and $Bool(D)$ and a dual equivalence between D and $Bool(C)$.

Effective computability and constructive provability for existence sentences

Makoto Fujiwara

Waseda Institute for Advanced Study, Waseda University, 1-6-1 Nishi Waseda, Shinjuku-ku, Tokyo 169-8050, JAPAN
makoto_fujiwara@aoni.waseda.jp

Effective provability of existence statements, which motivates the investigation of sequential versions in reverse mathematics, requires an effective procedure to obtain witnesses from instances of the problem. In [1], we have provided an exact formalization of effective provability in systems of (finite-type) arithmetic and have shown that for any existence statement of some syntactical form, it is effectively provable in the base system RCA of reverse mathematics if and only if it is provable in elementary analysis EL, which is the intuitionistic counterpart of RCA. Our formalization of effective provability in RCA roughly states that there is an effective procedure as required and it is verified in RCA. With the aim of illustrating the relationship between provability of existence statements in effective (computable) mathematics and that in constructive mathematics, we consider effective provability verified in a classical system containing arithmetical comprehension axiom ACA and characterize it by (semi-)intuitionistic provability.

References

1. M. Fujiwara, *Intuitionistic provability versus uniform provability in RCA*, CiE 2015 (A. Beckmann, V. Mitrana, and M. Soskova, eds.), Lecture Notes in Computer Science, vol. 9136 (2015), pp. 186–195.

Elimination of Binary Choice Sequences

Tatsuji Kawai

Japan Advanced Institute of Science and Technology
`tatsuji.kawai@jaist.ac.jp`

We define a theory of binary choice sequence BCS which is an extension of Elementary Analysis EL with a new type of objects, i.e. choice sequences. BCS has axioms of analytic data and continuous choices for binary choice sequences which are analogous to the corresponding axioms of the theory of choice sequences CS by Kreisel and Troelstra [2].

We show that BCS is a conservative extension of EL by adapting the method of elimination of choice sequences by Kreisel and Troelstra to the setting of BCS and EL. We relate our method to a sheaf semantics of BCS over the category of sheaves on a site whose underlying category is the monoid of uniformly continuous functions on Cantor space equipped with the open cover topology. Specifically, our translation is a formalisation of the sheaf semantics in EL.

This is analogous to the fact that the elimination of choice sequence by Kreisel and Troelstra is equivalent to the sheaf semantics over the site whose underlying category is the monoid of Brouwer continuous functions (i.e. continuous functions on Baire space which arise from inductively generated neighbourhood functions [3, Chapter 4, Section 8.4]) with the open cover topology as shown by Fourman [1], van der Hoeven and Moerdijk [4].

References

1. M. P. Fourman. Notions of choice sequence. In D. van Dalen and A. Troelstra, editors, *The L.E.J. Brouwer Centenary Symposium*, pages 91–105. North-Holland, 1982.
2. G. Kreisel and A. S. Troelstra. Formal systems for some branches of intuitionistic analysis. *Annals of Mathematical Logic*, 1(3):229–387, 1970.
3. A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics: An Introduction. Volume I*, volume 121 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1988.
4. G. van der Hoeven and I. Moerdijk. Sheaf models for choice sequences. *Annals of Pure and Applied Logic*, 27(1):63–107, 1984.

Analytic Functions and Small Complexity Classes ⋆

Akitoshi Kawamura[1], Florian Steinberg[2], and Holger Thies[1]

[1] Graduate School of Arts and Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan, kawamura@graco.c.u-tokyo.ac.jp, holgerthies@g.ecc.u-tokyo.ac.jp
[2] Department of Mathematics, TU Darmstadt, Schloßgartenstraße 7, 64289 Darmstadt, Germany, steinberg@mathematik.tu-darmstadt.de

Kawamura and Cook's extension to Weihrauch's framework of representations [5] gives a reasonable model to analyze the complexity of operators in analysis [1]. Defining type-2 versions of the complexity classes $\mathcal{P}$, $\mathcal{NP}$ and $\mathcal{PSPACE}$, they generalized many non-uniform hardness results into uniform statements.

Using this model, it can be shown that many important operators are in general hard from the viewpoint of real complexity theory. Nevertheless, restricting to only analytic functions many of these operators can be computed in polynomial time [4]. Using the right representation, those statements can be turned into uniform algorithms [2]. Since applying operators to power series often involves modifications on a large number of coefficients at the same time, it is reasonable to ask which operations on analytic functions can be efficiently parallelized.

In classical complexity theory, efficient parallelization is strongly connected to the complexity classes $\mathcal{L}$ and $\mathcal{NC}$. A generalization of this in the sense of continuous problems was recently done by Kawamura and Ota [3]. Using their framework, we generalize the polynomial time results on analytic functions and investigate which operations are eligible for efficient parallelization and which most likely are not.

References

1. Kawamura, A., Cook, S., *Complexity Theory for Operators in Analysis*, ACM Transactions in Computation Theory, vol. 4 (2012), no. 2, pp. 5:1–5:24.
2. Kawamura, A., Müller, N.T., Rösnick, C., Ziegler, M., *Computational benefit of smoothness: Parameterized bit-complexity of numerical operators on analytic functions and Gevrey's hierarchy*, Journal of Complexity, vol. 31, no. 5, pp. 680–714.
3. Kawamura, A., Ota, H., *Small complexity classes for computable analysis.*, Lecture Notes in Computer Science, vol. 8635, pp. 432–444.
4. Ko, K., Friedman, H. *Computational complexity of real functions*, Theoretical Computer Science, vol. 20 (1982), no. 3, pp. 323–352.
5. Weihrauch, K. *Computable Analysis, an Introduction*, Springer, 2000.

⋆ The authors thank the JSPS Core-to-Core Program (Advanced Research Networks) and Grants-in-Aid for Scientific Research (Kakenhi 24106002 and 26700001) for supporting the research presented here. The second author was supported by the International Research Training Group 1529 Mathematical Fluid Dynamics funded by the DFG and JSPS.

Degrees of unsolvability in topological spaces with countable cs-networks

Takayuki Kihara[1] and Arno Pauly[2]

[1] Department of Mathematics, University of California, Berkeley, USA, kihara@math.berkeley.edu
[2] Département d'Informatique, Université Libre de Bruxelles, Belgium, Arno.M.Pauly@gmail.com

In computability theory, we often think of the degree of unsolvability (the *Turing degree*) of a decision problem as the degree of a point in Cantor space. Similarly, we can think of the degree of enumerability (the *enumeration degree*) of a set of integers as the degree of a point in the Scott domain $\mathcal{P}\mathbb{N}$. More generally, the theory of admissible representation allows us to assign a degree structure to each topological space with a countable cs-network (where "cs" is an abbreviation of "*convergent sequence*"), or equivalently, to each qcb_0 space [3]. This observation enables us to combine degree theory with general topology. For instance, in [1] the authors gave a dimension-theoretic characterization of the Turing degrees: the degree structure of a Polish space is the Turing degrees (up to an oracle) if and only if the space has transfinite inductive dimension.

Moreover, the authors [1] found unexpected applications of the notion of a degree structure of a separable metrizable space in other areas of mathematics which do not involve the notion related to computability theory — they used the notion of the degree structure to solve a preexisting open problem in another branch of mathematics. It is open whether there is such an application of degree theory on nonmetrizable spaces.

In this talk, we focus on degree structures of nonmetrizable spaces. We introduce the notion of quasi-minimality w.r.t. (effective) topological property $\mathcal{P}$. We say that a non-computable point x in a space is *quasi-minimal w.r.t.* $\mathcal{P}$ if x do not have a power to compute a non-computable point in an effective $\mathcal{P}$-space. Of course, if x is quasi-minimal w.r.t. $\mathcal{P}$, then x cannot be a point in an effective $\mathcal{P}$-space. We prove several statements of the following kind.

Theorem 1 ([2]). *If $x \in \mathbb{Z}^{\omega}_{>0}$ is 1-generic w.r.t. the Baire topology on $\mathbb{Z}^{\omega}_{>0}$, then x as a point in $\mathbb{Z}^{\omega}_{>0}$ with the product relatively prime integer topology is quasi-minimal w.r.t. $T_{2\frac{1}{2}}$-spaces with countable cs-networks.*

Theorem 2 ([2]). *Let $\mathcal{A}_1(\omega^\omega)$ be the hyperspace of closed singletons in the Baire space, equipped with the sequentialization of the cs-open topology. Let $x \in \omega^\omega$ be such that $\{x\}$ is not computable as a point in $\mathcal{A}_1(\omega^\omega)$*

1. *We say that $x \in \omega^\omega$ is a* lost melody *if there is $z \in \omega^\omega$ such that $\{x\}$ is a $\Pi^0_1(z)$ singleton in ω^ω, but x is not computable relative to the Turing jump of z. If x is a lost melody, then $\{x\}$ is quasi-minimal w.r.t. second-countable T_0-spaces.*
2. *If $x \in \omega^\omega$ as a function on ω is not dominated by a computable function, then $\{x\}$ is quasi-minimal w.r.t. Hausdorff spaces with countable closed cs-networks. In particular, $\{x\}$ is quasi-minimal w.r.t. regular Hausdorff spaces with countable cs-networks.*
   (Note that a Hausdorff space with countable closed cs-network is not necessarily regular, e.g., the Kleene-Kreisel space $\mathbb{N}^{\mathbb{N}^{\mathbb{N}}}$ [4].)

We will also show similar results concerning the Gandy-Harrington topology, the co-cylinder topology, the lower topology, and so on.

This work was triggered by a private communication with Matthew de Brecht.

References

1. Takayuki Kihara and Arno Pauly, *Point degree spectra of represented spaces*, submitted, 2015.
2. Takayuki Kihara and Arno Pauly, *Notes on point degree spectra of nonmetrizable spaces*, preprint, 2016.
3. Matthias Schröder, *Extended admissibility*, Theoretical Computer Science, vol. 284 (2002), no. 2, pp. 519–538.
4. Matthias Schröder, *The sequential topology on* $\mathbb{N}^{\mathbb{N}^{\mathbb{N}}}$ *is not regular*, Mathematical Structures in Computer Science, vol. 19 (2009), no. 5, pp. 943–957.

Decidability of entailments in separation logic with arrays

Daisuke Kimura[1] and Makoto Tatsuta[2]

[1] Department of Information Science, Toho University, Chiba, Japan kmr@is.sci.toho-u.ac.jp
[2] National Institute of Informatics, Tokyo, Japan

We show decidability of validity of entailments in symbolic-heap fragment of separation logic with arrays, which is designed for verifying array-manipulating imperative programs. Our proof is given by translating entailments into formulas of Presburger Arithmetic, which is known to be decidable. Finally we provide an implementation of our decision procedure, in which Presburger-formulas are decided by an internally called SMT-solver.

References

1. J.Berdine, C.Calcagno, P.W.O'Hearn, *A Decidable Fragment of Separation Logic*, In: Proceedings of the 24th International Conference on Foundations of Software Technology and Theoretical Computer Science (India), LNCS vol. 3328, Springer, 2004, pp. 97–109.
2. J.Berdine, C.Calcagno, P.W.O'Hearn, *Symbolic Execution with Separation Logic*, In: Proceedings of the 3rd Asian Conference on Programming Languages and Systems (Japan), LNCS vol. 3780, Springer, 2005, pp. 52–68.
3. R. Piskac, T. Wies, and D. Zufferey, *Automating Separation Logic Using SMT*, In: Proceedings of the 25th International Conference of Computer Aided Verification (Russia), LNCS vol. 8044, Springer, 2013, pp. 773–789.
4. J.C. Reynolds, *Separation Logic: A Logic for Shared Mutable Data Structures*, In: Proceedings of the 17th Annual IEEE Symposium on Logic in Computer Science (USA), IEEE Computer Society, 2002, pp. 55–74.
5. M.Tatsuta and D.Kimura, *Separation Logic with Monadic Inductive Definitions and Implicit Existentials*, In: Proceedings of the 13th Asian Conference on Programming Languages and Systems (Korea), LNCS vol. 9458, Springer, 2015, pp. 69–89.

Determinacy strength of infinite games in ω-languages recognized by variations of pushdown automata

Wenjuan Li and Kazuyuki Tanaka

Mathematical Institute, Tohoku University,
6-3, Aramaki Aza-Aoba, Aoba-ku, Sendai 980-8578, Japan, sb2m701@math.tohoku.ac.jp

I will report on the progress of our study on determinacy strength of ω-languages recognized by variations of pushdown automata. We downscale Finkel's [1] results on determinacy of context-free ω-languages to lower levels of Borel hierarchy, so that we obtain some reverse mathematical results on determinacy.

We have noticed that infinite games specified by nondeterministic pushdown automata have some resemblance to those by deterministic 2-stack visibly pushdown automata with the same acceptance conditions. So, we first investigate the determinacy of games specified by deterministic 2-stack visibly pushdown automata with various acceptance conditions, e.g., safety, reachability and co-Büchi conditions. Analogue results have obtained for pushdown ω-languages except that the safety case is provable in RCA_0. For instance, we prove that the determinacy of games specified by pushdown automata with a reachability condition is equivalent to the weak König lemma. It is known that determinacy of pushdown ω-languages with a Büchi condition is equivalent to the determinacy of effective analytic games [1], which is independent from ZFC. We here show that for the co-Büchi condition, the determinacy is exactly captured by ATR_0.

References

1. O. Finkel, *The determinacy of context-free games*, The Journal of Symbolic Logic, vol. 78 (2013), no. 4, pp. 1115-1134.

Harmony, the Curry-Howard Correspondence, and Higher Proof Theory

Yoshihiro Maruyama

The Hakubi Centre for Advanced Research, Kyoto University

Dummett coined the term "harmony" meaning something like a dual or invertible correspondence between positive and negative inference (e.g., intro. and elim. rules). A motive for requiring harmony was to demarcate genuine logical constants from pseudo-logical ones, in response to Prior's "tonk" problem, which, presumably, tells us not all pairs of rules yield a logical constant. Harmonious pairs of rules alone, Dummett argued, are able to confer meaning on signs. Different conceptions of harmony are proposed in proof-theoretic semantics, a cross-disciplinary enterprise to look into the emergence of meaning in inference.

An intuition underlying proof-theoretic semantics is, presuambly, that harmony ought to warrant proof reduction, which, in turn, should allow us to give type-theoretical or categorical semantics in the sprit of the Curry-Howard correspondence. This intuition shall be further elucidated in this talk, given a precise form in terms of general-elimination harmony and its categorical guise. Here the main tenet is that the harmony principle may be thought of as underpinning the Curry-Howard correspondence, a version of Dummettian verificationist semantics, which, by itself, may count as another conception of harmony.

In passing, it turns out that there is a symmetrical structure between some limit and colimit constructions, so that direct and inverse constructions are united into one and the same concept via the harmony principle. This may be seen as an application of proof-theoretic semantics to category theory, laying a foundation for further interactions between the two fields. The issues of harmony and the Curry-Howard-Lambek correspondence are even relevant to structures in quantum physics through what is called the Abramsky-Coecke correspondence.

The final part of the talk is devoted to developments of higher proof theory, or some sort of higher Curry-Howard correspondence, to shed new light on the logical meaning of higher categories (including a higher-categorical interpretation of proof reduction termination), which is only explicated in a very limited context of a specific type theory thus far. Overall, this is on-going work at quite an early stage, so any comments and suggestions are more than welcome from proof theorists, type theorists, or whoever else knowledgable in this sort of stuff.

References

1. Y. Maruyama Categorical harmony and paradoxes in proof-theoretic semantics, in a Trends in Logic volume *Advances in Proof-Theoretic Semantics*, pp. 95-114, 2016 (open access to the entire volume at the Springer website).
2. Y. Maruyama *Prior's tonk, notions of logic, and levels of inconsistency: vindicating the pluralistic unity of science in the light of categorical logical positivism*, accepted for publication in *Synthese*, 2016 (already available online at the Springer website).

Coherence spaces for resource-sensitive computation in analysis

Kei Matsumoto

RIMS, Kyoto University, Japan, `kmtmt@kurims.kyoto-u.ac.jp`

This is a continuation of our previous works presented at CCA'15 [2] and CCC'15 [3], in which we have proposed a theory of representation based on coherence spaces [1] as an alternative to the type two theory of effectivity (TTE) [6] and the Scott-Ershov domain representations [5], and we have compared these approaches.

In [2], we reported that one can import various concepts from TTE, especially admissibility of representations [4], and provide an admissible representation for the real line and Euclidean spaces, for instance. As a consequence of admissibility, for every real function, it is tracked by a stable map if and only if it is continuous. An entirely new correspondence arises when we consider linear maps as well: a real function is tracked by a linear map if and only if it is uniformly continuous.

In this talk, we plan to report our ongoing work to propose a good criterion for coherent representations named *linear admissibility* which generalizes this phenomenon to a wider class of uniform spaces. We intend this work to be the first step towards understanding the connection between the denotational semantics of linear logic and computation in analysis.

References

1. J.-Y. Girard, *Linear logic*, Theoretical computer science, vol.50, no.1, 1987, pp.1–102.
2. K. Matsumoto, K. Terui, *Coherence spaces for computable analysis*, Proceedings of the Twelfth International Conference on Computability and Complexity in Analysis, 2015, pp.44–46.
3. K. Matsumoto, K. Terui, *Coherence spaces for computable analysis II*, Continuity, Computability, Constructivity: From Logic to Algorithms (CCC2015), 2015.
4. M. Schröder, *Extended admissibility*, Theoretical computer science, vol.248, no.2, 2002, pp.519–538.
5. V. Stoltenberg-Hansen, J. V. Tucker, *Computability on topological spaces via domain representations*, New computational paradigms: Changing conceptions of what is computable (S.B. Cooper, B. Löwe and A. Sorbi, editors), Springer, New York, 2008, pp.153–194.
6. K. Weihrauch, *Computable analysis – An introduction*, Texts in Theoretical Computer Science, Springer-Verlag, 2000.

Compositional Z: confluence proofs for permutative conversion

Koji Nakazawa[1] and Ken-etsu Fujita[2]

[1] Graduate School of Information Science, Nagoya University, knak@is.nagoya-u.ac.jp
[2] Graduate School of Science and Technology, Gunma University, fujita@cs.gunma-u.ac.jp

The permutative conversion was introduced by Prawitz [9] as one of proof normalization processes for the natural deduction with disjunctions and existential quantifiers. It permutes order of applications of elimination rules, and then normal proofs have some nice properties such as the subformula property. In the term representation, the rule of the permutative conversion, or the π-reduction, has the following form:

$$M[x_1.N_1, x_2.N_2]e \to M[x_1.N_1e, x_2.N_2e],$$

where the expression $[x_1.N_1, x_2.N_2]$ denotes a destructor for disjunctions, which can be understood as a case branching, and e denotes either a function argument or another case branching.

This reduction rule is quite simple, but the combination of it with the β-reduction makes confluence proofs much harder if we do not depend on strong normalization, as Ando discussed in [2]. He pointed out that an extension of Parigot's $\lambda\mu$-calculus [8] with permutative conversion brings some big troubles with confluence proofs. Baba et al. [3] also discussed similar problem. They proved confluence of some variants of the $\lambda\mu$-calculus with the so-called renaming reductions. The structural reduction (or the μ-reduction) of the $\lambda\mu$-calculus is a variant of the permutative conversion, and they pointed out that the combination of the structural reduction and the renaming reduction makes a trouble in confluence proofs and it requires a modification of the parallel reduction.

From their observation, we can see that the difficulties are caused by the following. First, we cannot naïvely adopt the parallel reduction technique of Tait and Martin-Löf, since a parallel reduction defined in an ordinary way does not have the diamond property. Figure 1 shows a counterexample, where the left bottom arrow consists of two π-steps and the redex of the second step does not occur in M_2. Therefore, Ando generalized the parallel reduction with the notion of the segment trees. Secondly, it is also difficult to adopt Takahashi's technique with complete development [10], and Ando used traditional notion of the residuals [4] to define the complete development.

In this work, we show that we can avoid these troubles by adapting another proof technique for confluence proposed by Dehornoy and van Oostrom [5], called the *Z theorem*: if there is a mapping which satisfies the *Z property*, then the reduction system is confluent. The Z property and its weaker variant are defined as follows.

Definition 1 ((Weak) Z property). *Let $(A, \to)$ be an abstract rewriting system, and $\twoheadrightarrow$ be the reflexive transitive closure of $\to$. Let $\to_{\mathsf{x}}$ be another relation on A, and $\twoheadrightarrow_{\mathsf{x}}$ be its reflexive transitive closure.*

1. A mapping f satisfies the weak Z property for $\to$ by $\to_{\mathsf{x}}$ *if $a \to b$ implies $b \twoheadrightarrow_{\mathsf{x}} f(a) \twoheadrightarrow_{\mathsf{x}} f(b)$ for any $a, b \in A$.*

2. A mapping f satisfies the Z property for $\to$ *if it satisfies the weak Z property by $\to$ itself. When f satisfies the (weak) Z property, we also say that f* is (weakly) Z.

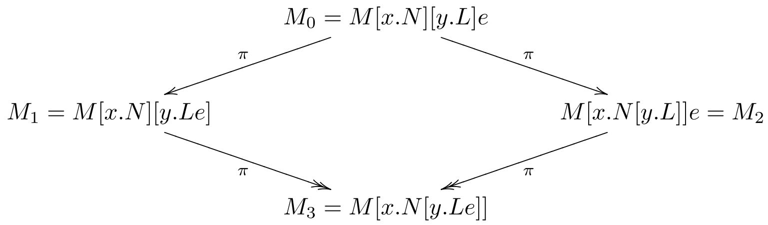


Fig. 1. Critical pair induced by the π-reduction

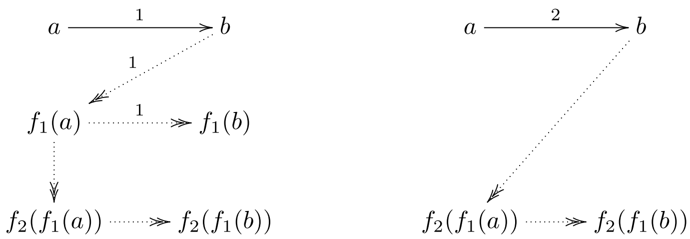
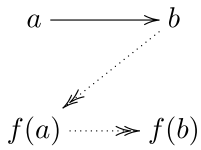


Fig. 2. Proof of Theorem 1

It becomes clear why we call it the Z property when we draw the condition as the following diagram.



A major candidate for the mapping with the Z property is the complete development used in Takahashi's proof, and hence defining such a mapping for calculi with both β and π is still hard.

We extend the Z theorem to compositional functions, called the *compositional Z*, and show that a mapping satisfying the Z property can be easily defined as a composition of two complete developments for the β-reduction and the permutative conversion, respectively. The new theorem can be stated as follows.

Theorem 1 (Compositional Z). *Let* $(A, \to)$ *be an abstract rewriting system, and* $\to$ *be* $\to_1 \cup \to_2$. *If there exist mappings* $f_1, f_2 : A \to A$ *such that*

(a) f_1 *is Z for* $\to_1$

(b) $a \to_1 b$ *implies* $f_2(a) \twoheadrightarrow f_2(b)$

(c) $a \twoheadrightarrow f_2(a)$ *holds for any* $a \in \mathrm{Im}(f_1)$

(d) $f_2 \circ f_1$ *is weakly Z for* $\to_2$ *by* $\to$,

then $f_2 \circ f_1$ *is Z for* $(A, \to)$, *and hence* $(A, \to)$ *is confluent.*

The conditions of the compositional Z can be depicted as Figure 2, which also shows that these conditions imply the conditions of the original Z theorem for $\to_1 \cup \to_2$. One easy example of the compositional Z is a confluence proof for the $\beta\eta$-reduction on the untyped λ-calculus (although it can be directly proved by the Z theorem as in [6]). Let $\to_1 \,=\, \to_\eta$, $\to_2 \,=\, \to_\beta$, and f_1 and f_2 be the usual complete developments of η and β, respectively. Then, it is easy to see the conditions of the compositional Z hold. The point is that we can forget the other reduction in the definition of each complete development.

We can avoid the trouble in the confluence proof for λ- and $\lambda\mu$-calculi with permutative conversion by the compositional Z. Let $\to_1$ be the permutative conversion and $\to_2$ be the β-reduction, then we can introduce the functions f_1 and f_2 satisfying the condition of the theorem. Furthermore, the compositional Z can be adapted to a λ-calculus with explicit substitutions, where we can treat the substitution propagation in a similar way to the permutative conversion.

It should be also interesting that the compositional Z is a generalization of Accattoli and Kesner's *Z property modulo* [1]. For an abstract rewriting system $(A, \to)$ and an equivalence relation $\sim$ on A, the reduction modulo $\sim$, denoted $a \to_{\sim} b$, is defined as $a \sim c \to c' \sim b$ for some c and c'. The Z property modulo says that it is a sufficient condition for the confluence of $\to_{\sim}$ that there exists a mapping which is well-defined on $\sim$ and weakly Z for $\to$ by $\to_{\sim}$. If we consider $\sim$ as the first reduction relation $\to_1$, and define $f_1(a)$ as a fixed representative of the equivalence class including a, then the conditions of the Z property modulo implies the conditions of the compositional Z, since the reflexive transitive closure of $\to \cup \sim$ is $\twoheadrightarrow_{\sim}$.

The full version of this work can be found in [7].

References

1. B. Accattoli and D. Kesner, *The permutative λ-calculus*, Proceedings of the International Conference on Logic Programming and Automated Reasoning (LPAR 2012), vol. 7180 of Lecture Notes in Computer Science, pp. 15–22, 2012.
2. Y. Ando, *Church-Rosser property of a simple reduction for full first-order classical natural deduction*, Annals of Pure and Applied Logic, vol. 119 (2003), pp. 225–237.
3. K. Baba, S. Hirokawa, and K. Fujita, *Parallel reduction in type free $\lambda\mu$-calculus*, Electronic Notes in Theoretical Computer Science, vol. 42 (2001), pp. 52–66.
4. A. Church and J.B. Rosser, *Some properties of conversion*, Transactions of ASM, vol. 29 (1936), no. 3, pp. 472–482.
5. P. Dehornoy and V. van Oostrom, *Z, proving confluence by monotonic single-step upperbound functions*, Logical Models of Reasoning and Computation (LMRC-08), 2008.
6. Y. Komori, N. Matsuda, and F. Yamakawa, *A simplified proof of the Church-Rosser theorem*, Studia Logica, vol. 102 (2013), no. 1, pp. 175–183.
7. K. Nakazawa and K. Fujita, *Compositional Z: confluence proofs for permutative conversion*, Studia Logica, to appear.
8. M. Parigot, *$\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction*, Proceedings of the International Conference on Logic Programming and Automated Reasoning (LPAR '92), vol. 624 of Lecture Notes in Computer Science, Springer, 1992, pp. 190–201.
9. D. Prawitz, *Natural deduction: a proof theoretical study*, Dover, 2006.
10. M. Takahashi, *Parallel reduction in λ-calculus*, Information and Computation, vol. 118 (1995), pp. 120–127.

Verification in Real computation

Norbert Müller[1], Sewon Park[2], Norbert Preining[3], and Martin Ziegler[2]

[1] Trier University, Universitätsring 15, 54296 Trier, Germany, mueller@uni-trier.d
[2] KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, Korea, swelite@kaist.ac.kr, ziegler@cs.kaist.ac.kr
[3] Accelia Inc., Chiyoda-ku, 102-0083 Tokyo, Japan and JAIST, 1-1 Asahidai, 923-1292 Nomi, Japan, norbert@preining.info

Recursive Analysis provides a sound foundation of computation over real numbers, functions, and compact subsets by approximation up to guaranteed error bounds; and has been generalized to metric spaces. Moreover huge strides have been made from computability theory to bit-complexity However the underlying Turing machine model, operating on sequences of approximations from a fixed countable dense subset, is awkward to program in practice; while the intuitive algebraic model ignores rounding errors and in fact exhibits superrecursive power. Reconciliating and combining the best of both worlds, a model of imperative computation over the reals had been suggested and implemented as abstract data type `REAL` in the object-oriented programming language `C++`. It maintains the perspective of real numbers as entities by assigning to inequality tests a modified, namely multivalued (aka non-extensional aka fuzzy aka soft) semantics well-known inherent to real computation.

In this work we present and formally prove the correctness of algorithms for three simple but natural multivalued example problems: truncated binary logarithm

$$\mathrm{ilog}_2 : (0;\infty) \ \ni \ x \ \mapsto \ \{k \in \mathbb{Z} : 2^{k-1} < x < 2^{k+1}\} \ , \tag{1}$$

1D simple root finding, and nontrivially solving a given homogeneous system of linear equations $A \cdot \boldsymbol{x} = \mathbf{0}$. Lacking tests for equality, the latter requires, in addition to continuous $A \in \mathbb{R}^{m\times n}$, the discrete input of $\mathrm{rank}(A) \in \{0, 1, \ldots, \min(n, m) - 1\}$, employed in a non-trivial refinement of classical Gaussian Elimination worthwhile verifying.

Our symbolic proofs presume the underlying arithmetic primitives and multivalued tests to be correct, implemented for instance using multiple precision interval computations, and thus complement current research on the verification of floating-point arithmetic. The long-term goal is to extend Floyd-Hoare Logic to more general classes of hybrid algorithms, operating on both discrete and continuous abstract data types such as Sobolev spaces $H^k(\Omega)$.

Unprovability and some reverse mathematics which involve ordinals

Florian Pelupessy

Mathematical Insutitute, Tohoku University, Sendai
florian.pelupessy@operamail.com

The techniques from proof theory which are used for showing properties of weak incompleteness phenomena are rather suitable for classifying their relativised versions in the reverse mathematics setting. The implication is that these relativised versions are not classified into the "Big Five", but equivalent to the well-foundedness of the corresponding proof theoretic ordinal.

We will examine some cases of this observation.

Proof theory of the λ-calculus

Masahiko Sato

Graduate School of Informatics, Kyoto University
masahiko@kuis.kyoto-u.ac.jp

We develop a proof theory of the λ-calculus where we study the set of closed lambda terms by inductively defining the set as a free algebra.

The novelty of the approach is that we construct and study λ-calculus without using the notions of variables and alpha-equivalence. In this approach we can study λ-terms as combinators and can have a clean proof of the Church-Rosser Theorem in the Minlog proof assistant.

This is a joint work with Helmut Schwichtenberg and Takafumi Sakurai.

Continuity in constructive analysis

Helmut Schwichtenberg

Mathematisches Institut der Universität München, Theresienstraße 39, Germany
schwicht@math.lmu.de

We aim at doing constructive analysis in such a way that its constructions correspond to good algorithms, which can then be extracted from the formalized proofs (by the realizability interpretation). To obtain such proofs we use locatedness in the form

$$\forall_{v \in V}(c \leq \rho(u, v)) \vee \exists_{v \in V}(\rho(u, v) \leq d),$$

and avoid total boundedness (i.e., the existence of ε-nets). Generally, we (1) view constructive analysis as an extension of (rather than an alternative to) classical analysis, (2) formalize proofs in TCF (a theory of acomptable funcionals, based on the Scott-Ershov model of partial continuous functionals), and (3) use low type levels whenever possible, for instance by viewing a continuous function on the reals as determined by its values on the rationals. As examples we treat the intermediate value theorem, and the attainment of infima for convex real functions.

Programming with Objects in Theorem Provers based on Martin Löf Type Theory

Anton Setzer

Dept of Computer Science, Swansea University, Singleton Park, Swansea, UK, a.g.setzer@swan.ac.uk

In programming, the main programming paradigm used is object-orientation. The reason is that it supports well the hiding of implementation details from the outside and the change of implementations details of units without affecting the whole code. The question is whether it is possible to apply a similar approach in the area of proofs, and get similar benefits. Interactive proofs typically use a huge amount of lemmas and definitions, and techniques from programming might help to organise them in a better way.

One way of addressing this question is by looking at Martin-Löf type theory (MLTT), where proofs and programs are the same. This allows it to transfer concepts between programming and proving in a direct way.

As a first step we will look at how to represent the notion of an object in MLTT, extended by coinductively defined sets [AAS16]. We follow the approach described in [Set12,APTS13], where coinductively defined sets will be given by their observations or elimination rules. An object is essentially determined by its methods‘, and therefore one can represent objects as elements of coalgebras.

We will introduce a notion of extending an object. A novelty in the context of MLTT is that we obtain indexed state-dependent coalgebras, and correspondingly state dependent objects. In state dependent objects, the methods available change after applying method calls. An example is a safe stack, for which the the pop method is only available if the stack is non-empty. We will as well combine objects with state-dependent interactive programs.

If time permits we will introduce related research on representing processes in MLTT [IS16] (joint work with Bashar Igried). Processes will be again represented coalgebraically as non-well-founded trees, with branching over the transitions a process can make.

References

[AAS16] Andreas Abel, Stephan Adelsberger, and Anton Setzer. *Interactive programming in Agda – objects and graphical user interfaces.* To appear in Journal of Functional Programming. Preprint available at http://www.cs.swan.ac.uk/∼csetzer/articles/ooAgda.pdf, 2016.

[APTS13] Andreas Abel, Brigitte Pientka, David Thibodeau, and Anton Setzer. *Copatterns: Programming infinite structures by observations.* In Roberto Giacobazzi and Radhia Cousot, editors, Proceedings of the 40th annual ACM SIGPLAN-SIGACT Symposium on Principles of programming languages, POPL '13, ACM, New York, USA, 2013, pp. 27–38.

[IS16] Bashar Igried and Anton Setzer. *Programming with monadic CSP-style processes in dependent type theory.* To appear in proceedings of TyDe 2016, Type-driven Development, preprint available from http://www.cs.swan.ac.uk/∼csetzer/articles/TyDe2016.pdf, 2016.

[Set12] Anton Setzer. *Coalgebras as types determined by their elimination rules.* In P. Dybjer, Sten Lindström, Erik Palmgren, and G. Sundholm, editors, Epistemology versus Ontology, volume 27 of Logic, Epistemology, and the Unity of Science, Springer, Dordrecht, Heidelberg, New York, London, 2012, pp. 351–369.

Automated normalization analysis for term rewriting

Ryoko Watanabe[1] and Nao Hirokawa[1]

School of Information Science, JAIST, 1-1 Asahidai, Nomi, Japan, {s1510061,hirokawa}@jaist.ac.jp

Term rewriting is a simple but powerful computational model, which underlies declarative programming and theorem proving. *Normalization*, a property to ensure existence of computational results, is of fundamental importance in reasoning formal systems written in rewriting. However, unlike termination where a number of powerful termination provers have been developed, so far automating normalization analysis has received little attention. In this talk we present a fully automatic tool for proving or disproving normalization of term rewrite systems. Our approach is to combine several normalization proving methods, exploiting modularity results [1, 2]. Experiments show effectiveness of the approach.

References

1. Jaco van de Pol, *Modularity in many-sorted term rewriting systems,* Master's thesis, Utrecht University, 1992.
2. Enno Ohlebusch, *Modular properties of composable term rewriting systems,* Journal of Symbolic Computation, vol. 20 (1995), no. 1, pp. 1–41.

Proof-theoretic strength and indicator arguments

Keita Yokoyama[1]

Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi, Ishikawa 923-1292 Japan,
`y-keita@jaist.ac.jp`

The indicator argument is a model-theoretic approach to investigate the provably total functions of systems of arithmetic. The original form of the indicator argument is introduced by Kirby and Paris [1] for the study of the strength of infinitary combinatorial principles. Kaye [2] gave a general definition of indicators and developed its frame work in models of first-order arithmetic. Recently, indicator arguments are used to analyze the proof-theoretic strength of Ramsey's theorem for pairs [3, 4]. In this talk, I will give a brief introduction to indicator arguments, and then consider a slight generalization for subsystems of second-order arithmetic.

References

1. L. A. S. Kirby and J. B. Paris, *Initial segments of models of Peano's axioms*, Set theory and hierarchy theory, V (Proc. Third Conf., Bierutowice, 1976), Lecture Notes in Mathematics, Vol. 619, Springer, Berlin, 1977, pp. 211–226.
2. Richard Kaye, *Models of Peano Arithmetic*, Oxford University Press, 1991.
3. Andrey Bovykin and Andreas Weiermann, *The strength of infinitary Ramseyan principles can be accessed by their densities*, accepted for publication in Annals of Pure Appllied Logic, avairable at http: //logic.pdmi.ras.ru/ andrey/research.html, 2005.
4. Ludovic Patey and Keita Yokoyama, *The proof-theoretic strength of Ramsey's theorem for pairs and two colors*, available at http://arxiv.org/abs/1601.00050.