# Computability Theory and Foundations of Mathematics

**February, 18th – 20th, 2013**

**Tokyo Institute of Technology, Tokyo, Japan**

http://sendailogic.math.tohoku.ac.jp/CTFM/

東北大学
TOHOKU UNIVERSITY

東京工業大学
Tokyo Institute of Technology

UNIVERSITEIT
GENT

Edited by

Naohi Eguchi and
Kazuyuki Tanaka

Mathematical Institute
Tohoku University
Japan

$\left\{\begin{matrix}\texttt{eguchi}\\ \texttt{tanaka}\end{matrix}\right\}$`@math.tohoku.ac.jp`

**Supporters**

Chiba University
Ghent University
Japan Advanced Institute of Science and Technology
Tohoku University
Tokyo Institute of Technology

**Programme Committee**

Toshiyasu Arai
(Chiba University)
Naohi Eguchi
(Tohoku University)
Hajime Ishihara
(Japan Advanced Institute of Science and Technology)
Ryo Kashima
(Tokyo Institute of Technology)
Sam Sanders
(Ghent University)
Kazuyuki Tanaka (Co-chair)
(Tohoku University)
Andreas Weiermann (Co-chair)
(Ghent University)
Takeshi Yamazaki
(Tohoku University)
Keita Yokoyama
(Tokyo Institute of Technology)

**Local Organising Committee**

Ryo Kashima (Chair)
(Tokyo Institute of Technology)
Keita Yokoyama
(Tokyo Institute of Technology)

**Organising Committee**

Naohi Eguchi
(Tohoku University)
Sam Sanders
(Ghent University)
Kazuyuki Tanaka (Chair)
(Tohoku University)

# Preface

Welcome to CTFM 2013!

Computability Theory and Foundations of Mathematics (CTFM) aims to provide participants with the opportunity to exchange ideas, information and experiences on active and emerging topics in logic, including but not limited to: Computability Theory, Reverse Mathematics, Nonstandard Analysis, Proof Theory, Constructive Mathematics, Theory of Randomness and Computational Complexity Theory. This is a successor to Workshop on Proof Theory and Computability Theory 2012 - Philosophical Frontiers in Reverse Mathematics (February 20 - 23, 2012, Tokyo).

CTFM acknowledges support from Grants-in-Aid for Scientific Research (KAKENHI) No.23340020; the research project "Philosophical Frontiers in Reverse Mathematics" granted by John Templeton Foundation; Joint Research Projects between Tohoku University and Ghent University; JSPS-FWO Bilateral Programs; Tohoku University, Chiba University, Japan Advanced Institute of Science and Technology, and Tokyo Institute of Technology.

February 2013

Kazuyuki Tanaka

## Conference venue

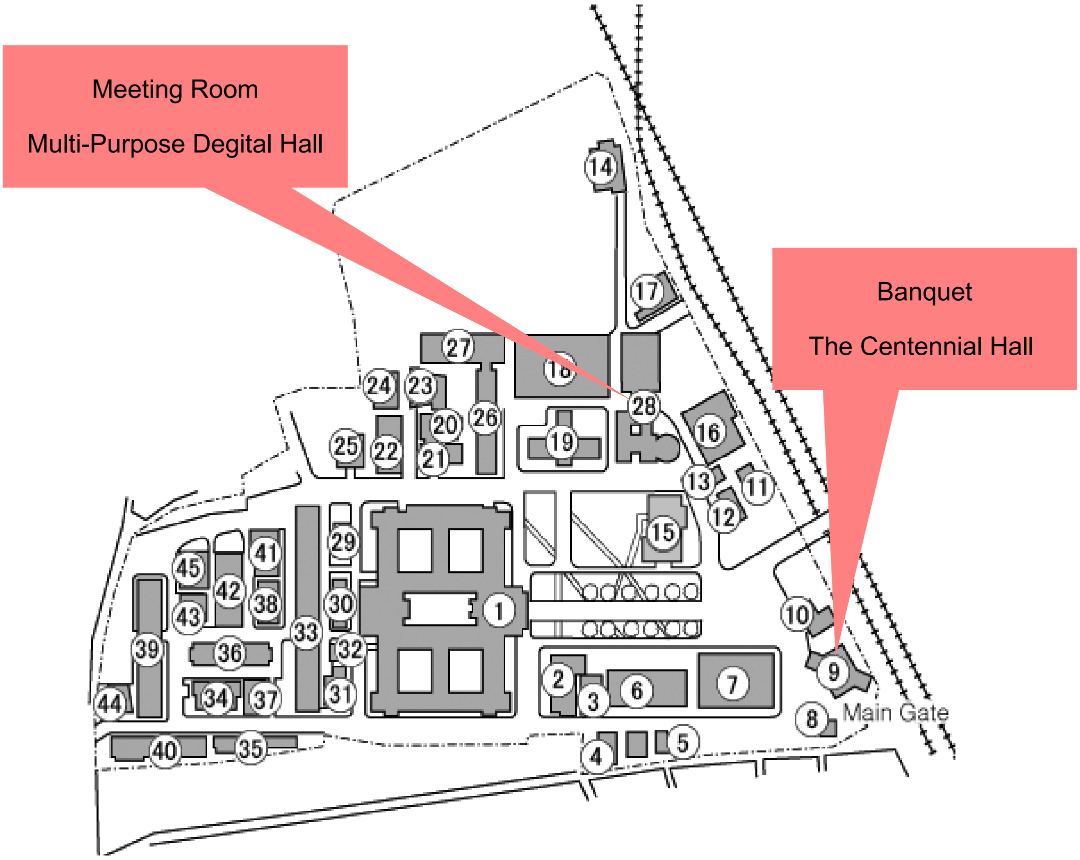
Ookayama campus of Tokyo Institute of Technology, Tokyo, Japan.

## Meeting room

Multi-Purpose Digital Hall (West building 9)

## Banquet

Buffet dinner. February 19th, Tuesday. The Centennial Hall.



## Program

### February 18 (Monday)

9:30. *Reception.*

*Session 1. Reverse Mathematics and Unprovability.* (chair: Keita Yokoyama)

**Contributed talk 1.** 10:00 – 10:30. Takeshi Yamazaki.
Reverse Mathematics and Commutative Ring Theory.

**Contributed talk 2.** 10:30 – 11:00. Florian Pelupessy.
A short proof of two Ramsey like independence results.

11:00 – 11:15. *Short break.*

**Invited talk 1.** 11:15 – 12:00. (chair: Keita Yokoyama) Yang Yue.
Ramsey Theorem for Pairs and Reverse Mathematics.

12:00 – 13:30. *Lunch break.*

**Invited talk 2.** 13:30 – 14:15. (chair: Takeshi Yamazaki) Wu Guohua.
On a theorem of Seetapun on locally noncappable degrees.

14:15 – 14:30. *Short break.*

*Session 2. Degree Theory.* (chair: Takeshi Yamazaki)

**Contributed talk 3.** 14:30 – 15:00. Takayuki Kihara.
An application of Turing degree theory to the $\omega$-decomposability problem on Borel functions.

**Contributed talk 4.** 15:00 – 15:30. Kojiro Higuchi.
The Muchnik degrees of $\Pi^0_1$ and $\Sigma^1_1$ classes.

15:30 – 16:00. *Coffee break.*

*Session 3. Constructive Mathematics.* (chair: Hajime Ishihara)

**Contributed talk 5.** 16:00 – 16:30. Kazuto Yoshimura.
A Categorical Description of Relativization.

**Contributed talk 6.** 16:30 – 17:00. Josef Berger.
Inequality of Reals.

**Contributed talk 7.** 17:00 – 17:30. Sam Sanders.
Reuniting the antipodes, bringing together Nonstandard and Constructive Analysis.

## February 19 (Tuesday)

*Session 4. Proof Theory and Semantics.* (chair: Ryo Kashima)

**Contributed talk 8.** 9:30 – 10:00. Ken-Etsu Fujita.
Decidability for type-related problems of 2nd-order lambda-calculi and negative translations.

**Contributed talk 9.** 10:00 – 10:30. Gyesik Lee.
Subsystems of arithmetic as type theories with inductive definitions.

**Contributed talk 10.** 10:30 – 11:00. Michele Basaldella.
An interactive semantics for classical proofs.

11:00 – 11:15. *Short break.*

**Invited talk 3.** 11:15 – 12:00. (chair: Ryo Kashima) Helmut Schwichtenberg
Proofs, computations and analysis.

12:00 – 13:30. *Lunch break.*

**Invited talk 4.** 13:30 – 14:15. (chair: Kazushige Terui) Toshiyasu Arai
$\Pi^1_n$-indescribabilities in proof theory.

14:15 – 14:30. *Short break.*

*Session 5. Ordinals and Weak Arithmetic.* (chair: Toshiyasu Arai)

**Contributed talk 11.** 14:30 – 15:00. Jeroen Van der Meeren.
Recursively defined trees and their maximal order types.

**Contributed talk 12.** 15:00 – 15:30. Naohi Eguchi.
Inductive Definitions in Bounded Arithmetic: A New Way to Approach P vs. PSPACE.

**Contributed talk 13.** 15:30 – 16:00. Yoshihiro Horihata.
Theories of concatenation, arithmetic, and undecidability.

16:00 – 16:30. *Coffee break.*

**Invited talk 5.** 16:30 – 17:15. (chair: Kazuyuki Tanaka) Stephen G. Simpson.
A survey of basis theorems.

18:00. *Banquet.*

## February 20 (Wednesday)

*Session 6. Algorithmic Randomness.* (chair: Takayuki Kihara)

**Contributed talk 14.** 9:30 – 10:00. Kenshi Miyabe.
Computably measurable sets and computably measurable functions in terms of algorithmic randomness.

**Contributed talk 15.** 10:00 – 10:30. Ningning Peng.
On the Notions of Relative Randomness.

**Contributed talk 16.** 10:30 – 11:00. Kohtaro Tadaki and Norihisa Doi.
The Generic Group Model and Algorithmic Randomness.

11:00 – 11:15. *Short break.*

**Invited talk 6.** 11:15 – 12:00. (chair: Takayuki Kihara) Chi Tat Chong.
Randomness in the Higher Setting.

12:00 – 13:30. *Lunch break.*

*Session 7. Nonstandard Models.* (chair: Sam Sanders)

**Contributed talk 17.** 13:30 – 14:00. Tin Lok Wong.
Where closure under Turing jumps can replace elementarity between structures.

**Contributed talk 18.** 14:00 – 14:30. Keita Yokoyama.
Several versions of Friedman's self-embedding theorem.

14:30 – 15:00. *Coffee break.*

*Session 8. Complexity and Probability.* (chair: Naohi Eguchi)

**Contributed talk 19.** 15:00 – 15:30. Akitoshi Kawamura, Norbert Müller, Carsten Rösnick and Martin Ziegler.
Parameterized Uniform Complexity in Numerics: from Smooth to Analytic, from NP-hard to Polytime.

**Contributed talk 20.** 15:30 – 16:00. Yoriyuki Yamagata.
Bounded Arithmetic in Free Logic.

**Contributed talk 21.** 16:00 – 16:30. Cameron E. Freer.
Computability and Conditional Probability.

16:30. *Closing.*

# Abstracts

# Contents

# Ramsey Theorem for Pairs and Reverse Mathmetics

Yang Yue

Department of Mathematics, National University of Singapore
Block S17, 10 Lower Kent Ridge Road, Singapore 119076
`matyangy@nus.edu.sg`

Ramsey Theorem is a well-known theorem in combinatorics. However, a special weak form of it (Ramsey Theorem for Pairs) has been a hot topic in Recursion Theory and Reverse Mathematics. In this talk I will give a survey on some recent progresses related to combinatoric principles weaker than Ramsey's Theorem for Pairs. In particular, I will speak about some results obtained by Chitat Chong, Ted Slaman and me.

# On a theorem of Seetapun on locally noncappable degrees

Wu Guohua

Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore
guohua@ntu.edu.sg

In his thesis, Seetapun proved that any nonzero incomplete c.e. degree, a say, can have a c.e. degree c above it, witnessing that a is locally noncappable, i.e. no nonzero c.e. degree below c can form a minimal pair with a. As Seetapun pointed out there, his theorem implies that there is no maximal nonbounding degree (bounding no minimal pairs). In this talk, I will show how to make the degree c in Seetapun's theorem high2, a joint work with Frank Stephan. Our theorem implies that some well-known results of Downey, Lempp and Shore (high2 nonbounding degrees), and Li (high2 plus-cupping degrees), and others.

# Proofs, computations and analysis

Helmut Schwichtenberg

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

Algorithms are viewed as one aspect of proofs in (constructive) analysis. Data for such algorithms are finite or infinite lists of signed digits -1, 0, 1 (i.e., reals as streams), or possibly non well-founded labelled (by lists of signed digits -1, 0, 1) ternary trees (representing uniformly continuous functions). A theory of computable functionals (TCF) suitable for this setting is described. The main tools are (i) a distiction between computationally relevant and irrelevant logical connectives and (ii) simultaneous inductively/coinductively defined predicates. A realizability interpretation of proofs in TCF can be given, and a soundness theorem holds.

# $\Pi^1_n$-indescribabilities in proof theory

Toshiyasu Arai

Graduate School of Science, Chiba University, Japan
tosarai@faculty.chiba-u.jp

It is well known that the least $\Pi^1_1$-indescribable cardinal(weakly compact cardinal) $\kappa$ is much bigger than the least weakly Mahlo cardinal: the set of Mahlo cardinals below $\kappa$ is stationary in $\kappa$. Moreover for any stationary subset $S$ of $\kappa$, there exists an inaccessible cardinal $\lambda < \kappa$ such that $S \cap \lambda$ is stationary in $\lambda$. For inaccessible cardinals $\lambda < \kappa$, let $\lambda \in M(S)$ iff $S \cap \lambda$ is stationary in $\lambda$. Then if $S$ is stationary in $\kappa$, then so is $M(S)$. This means that in $\Pi^1_1$-indescribable cardinal $\kappa$ one can iterate the Mahlo operation $M$. How far can one iterate $M$ in $\kappa$?

It is shown that over $\mathsf{ZF} + (V = L)$, the existence of a $\Pi^1_1$-indescribable cardinal is proof-theoretically reducible to iterations of Mostowski collapsings and Mahlo operations. The same holds for $\Pi^1_{n+1}$-indescribable cardinals and $\Pi^1_n$-indescribabilities.

# A survey of basis theorems

Stephen G. Simpson

Department of Mathematics, Pennsylvania State University
http://www.math.psu.edu/simpson/
simpson@math.psu.edu

This is my abstract for the Workshop on Computability Theory and Foundations of Mathematics, to be held in Tokyo, February 18–20, 2013.

A *basis theorem* is a theorem of the form "Every nonempty effectively closed set in an effectively compact metric space contains at least one point which is, in some specific sense, close to being computable." Some well known basis theorems are the Low Basis Theorem, the Hyperimmune-Free Basis Theorem, the R.E. Basis Theorem, the Cone Avoidance Basis Theorem, and the Randomness Preservation Basis Theorem. Less well known is a recent basis theorem due to Higuchi/Hudelson/Simpson/Yokoyama concerning preservation of partial randomness. In this talk we shall state these basis theorems, sketch some of their proofs, and discuss the possibilities for combining them in various ways. We shall present some new results and open problems.

# Randomness in the Higher Setting

Chi Tat Chong

Department of Mathematics, National University of Singapore, Singapore 119076
chongct@math.nus.edu.sg

The study of algorithmic randomness in first-order arithmetic is an active area of current research in recursion theory. There is a natural extension of ideas and notions of randomness to higher order arithmetic, known as *Higher randomness*.

In this talk we give a survey of some of the work done in higher randomness by various authors, and discuss several open problems.

# Reverse Mathematics and Commutative Ring Theory

Takeshi Yamazaki
Mathematical Institute, Tohoku University

**Abstract.**

The goal of Reverse Mathematics is to classify specific mathematical theorems according to which set existence axioms are needed to prove them. In this talk, we will introduce some new reverse mathematical results on countable commutative ring theory, including some fields which have not been treated as far, such as modules, tensor product, p-adic number theory and so on.

## References

[1] H. M. Friedman, S. G. Simpson, R. L. Smith, Countable algebra and set existence axioms, Ann. Pure Appl. Logic 25 (1983), 141–181.

[2] K. Hatzikiriakou, Algebraic disguises of $\Sigma^0_1$ induction, Archives of Mathematical Logic 29, pp.47–51, 1989.

[3] Stephen G. Simpson, *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1999.

[4] Dodney G. Downey, Steffen Lempp and Joseph R. Mileti, Ideals In Computable Rings, J. Algebra 314 (2007), 872–887.

# A short proof of two Ramsey like independence results.

Florian Pelupessy
pelupessy@cage.ugent.be

Department of Mathematics, Ghent University

This is joint work with Harvey Friedman. We will examine two Ramsey like independence results. The first one is Friedman's adjacent Ramsey theorem (AR) from [1] and the second one is the Paris–Harrington theorem (PH) from [2]. In [1] Friedman proves that an infinite version of AR implies the well-ordering of $\varepsilon_0$. We adapt this proof to show that AR with fixed $k$ is unprovable in $\mathrm{I}\Sigma_k$. We use the tools from this proof to also show PH with fixed dimension $d+1$ is unprovable in $\mathrm{I}\Sigma_d$. The remarkable feature of these proofs is that they are much less complicated than earlier proofs of independence of Ramsey like theorems.

For $r$-tuples we use $\leq$ to indicate the coordinatewise order. A multivariate function $C\colon \{0,\dots,R\}^k \to \mathbb{N}^r$ is limited if $\max C(x) \leq \max x$.

**Theorem 1 (adjacent Ramsey,** AR**).** *For every $k, r$ there exists $R$ such that for every limited function $C\colon \{0,\dots,R\}^k \to \mathbb{N}^r$ there are $x_1 < \ldots < x_{k+1} < R$ with $C(x_1,\dots,x_k) \leq C(x_2,\dots,x_{k+1})$.*

We use $[X]^k$ to denote the set of $k$-element subsets of $X$, $[a,b]^k$ to denote the set of $k$-element subsets of the interval $[a,b]$. We call sets $H$ for which colouring $C$ limited to $[H]^d$ is constant homogeneous for $C$.

**Theorem 2 (Paris–Harrington,** PH**).** *For every $d, c, m$ there exists an $R$ such that for every colouring $C\colon [m,R]^d \to [0,c]$ there exists an $H \subseteq [m,R]$ of size* $\min H$ *which is homogeneous for $C$.*

## References

1. Friedman, H. Adjacent Ramsey theory,
http://www.math.osu.edu/∼friedman.8/pdf/PA%20incomp082910.pdf
2. Paris, J. and Harrington, L. A Mathematical Incompleteness in Peano Arithmetic. In Handbook for Mathematical Logic (Ed. J. Barwise). Amsterdam, Netherlands: North-Holland, 1977.

# An Application of Turing Degree Theory to the $\omega$-Decomposability Problem on Borel Functions

Takayuki Kihara

Japan Advanced Institute of Science and Technology, Ishikawa 923-1292, Japan
kihara.takayuki.logic@gmail.com

Almost 100 years ago, Nikolai Luzin asked whether every Borel function on $\mathbb{R}$ can be decomposed into countably many continuous functions. Nowadays the Luzin problem is known to be negative. But then, *which Borel functions are decomposable into countably many continuous functions?* Jayne and Rogers [3] proved that, for every function from an analytic space into a separable metric space, the preimage of each $F_\sigma$ set under it is again $F_\sigma$ if and only if it is decomposable into countably many continuous functions with closed domains (in real analysis, such a real-valued function is also extensively studied under the name of a *Baire star one* function). Subsequently, a number of set-theoretic results on the decomposability problem have also been established, e.g., [2, 6, 8, 9], and several authors [1, 4, 5] have conjectured that the Jayne-Rogers Theorem can be generalized to all finite levels of Borel functions.

In this talk, by using the Shore-Slaman Join Theorem [7] on the Turing degrees, we show the following variant of the Jayne-Rogers Theorem, which can be viewed as a partial solution to the generalization conjecture [1, 4, 5].

**Theorem 1.** *Assume $\xi \leq \zeta < \xi \cdot 2 < \omega_1$. For any function $F : \mathcal{X} \to \mathcal{Y}$ with $\mathcal{X}$ and $\mathcal{Y}$ Polish, the following conditions are equivalent:*

1. *From any Borel code of each $\mathbf{\Sigma}^0_{\xi+1}$ set $S \subseteq \mathcal{Y}$, one can continuously find a Borel code of its $\mathbf{\Sigma}^0_{\zeta+1}$ preimage $F^{-1}(S) \subseteq \mathcal{X}$.*
2. *$F$ is decomposable into a collection $\{F_n\}_{n\in\omega}$ of $\mathbf{\Sigma}^0_{\eta(n)+1}$-measurable functions with $\mathbf{\Pi}^0_\zeta$ domains, for some ordinals $\{\eta(n)\}_{n\in\omega}$ with $\eta(n) + \xi \leq \zeta$.*

*Further, even if $\zeta \geq \xi \cdot 2$, the implication (2)⇒(1)⇒(2') always holds, where*
*2'. $F$ is decomposable into $\mathbf{\Sigma}^0_{\eta(n)+1}$-measurable functions with $\eta(n) + \xi \leq \zeta$.*

**Keywords:** Descriptive Set Theory, Real Analysis, Turing degrees

## References

1. A. Andretta. in *Foundations of the formal sciences V.* 1–38, 2007.
2. J. Cichoń, et al., *J. Symb. Log.* 56: 1273–1283, 1991.
3. J. E. Jayne and C. A. Rogers. *J. Math. Pure Appl.*, 61:177–205, 1982.
4. L. Motto Ros. 2012. preprint.
5. J. Pawlikowskia and M. Sabok. *Ann. Pure Appl. Log.*, 163:1748–1764, 2012.
6. S. Shelah and J. Steprāns. *Fund. Math.*, 145:171–180, 1994.
7. R. A. Shore and T. A. Slaman. *Math. Res. Lett.*, 6:711–722, 1999.
8. S. Solecki. *J. Amer. Math. Soc.*, 11:521–550, 1998.
9. J. Zapletal, *Descriptive Set Theory and Definable Forcing*, 2004.

# The Muchnik degrees of $\Pi^0_1$ and $\Sigma^1_1$ classes

Kojiro Higuchi

Tohoku University

**Abstract.** In this talk, we investigate the Muchnik degree structures of $\Pi^0_1$ subsets of Cantor space. It is demonstrated that the Muchnik degrees of $\Sigma^1_1$ subsets of Cantor space or Baire space play an important role when we study the Muchnik degrees of $\Pi^0_1$ sets. In particular, we see that an open interval between two Muchnik degrees of nonempty $\Pi^0_1$ sets contains the Muchnik degree of a $\Pi^0_1$ set if and only if it contains the Muchnik degree of a $\Sigma^1_1$ set.

# A Categorical Description of Relativization

Kazuto Yoshimura

k.yoshimura@jaist.ac.jp
Japan Advanced Institute of Science and Technology

The aim of this research is to give an effectivity-independent foundation for computable analysis. In *type-2 theory of effectivity* [Wei00], a framework of computable analysis, each computational structure is understood as compatible with a topological structure. As a fragment of our reasoning for such cognition, it is well-known that for every subset of a given computable topological space, oracle co-r.e. closedness is coinside with topological closedness.

Recently, a categorical foundation for general topology, known as *a functional approach to general topology*, came up [PT03]. On that foundation, even though many analogous results to general topology can be obtained, we can treat not only usual topological structures, but also other types of structures, for example, computational one.

Using this, we give a pure categorical description of "relativization to oracles" and generalize that well-known fact showing an equivalence between oracle co-r.e. closedness and topological closedness. As a result, we obtain a generalized statement which doesn't depend on a particular effectivity concept e.g. computability.

We work on a well-powered large category $\mathbb{E}$ with an equipped proper factorization system $(\mathscr{S}, \mathscr{T})$. Assume that $\mathbb{E}$ is finitely complete, $\mathscr{S}$ is stable under pullback and $\mathbb{E}$ has $\mathscr{T}$-intersection. A subclass of $\mathscr{T}$ is said to be a fundamental class if it contains all isomorphisms, is closed under composition and is stable under pullback. Each fundamental class can be thought as defining a topology-like structure on $\mathbb{E}$. Each object $\alpha \in \mathbb{E}$ is said to be an imaginary if the unique morphism from $\alpha$ to a terminal object is monic and belongs to $\mathscr{S}$. For each fundamental class $\mathscr{F}$, we denote by $\mathscr{L}\mathscr{F}$ the smallest intersection closed fundamental class containing $\mathscr{F}$, and define $\mathscr{I}\mathscr{F} = \{t \in \mathscr{T} : {}^{\exists}\alpha\text{: imaginary s.t. } \mathrm{id}_\alpha \times t \in \mathscr{F}\}$.

Our main result is stated as follows. For every fundamental class $\mathscr{F}$, the following two statements are equivalent: (i) $\mathscr{I}\mathscr{F} \subseteq \mathscr{L}\mathscr{F}$; (ii) all imaginaries are $\mathscr{L}\mathscr{F}$-compact. Statement (i) corresponds to say "oracle co-r.e. closedness implies topological closedness" if we suitably define $\mathbb{E}$, $\mathscr{S}$, $\mathscr{T}$ and $\mathscr{F}$. One can see that statement (ii), and thus also statement (i), always holds when $\mathbb{E}$ satisfies an additional condition. The other direction of inclusion $\mathscr{L}\mathscr{F} \subseteq \mathscr{I}\mathscr{F}$ can also be shown under a sufficiently strong assumption.

## References

[Wei00] K. Weihrauch. Computable Analysis. Springer. 2000.

[PT03] M.C. Pedicchio and W. Tholen. Categorical Foundations: Special Topics in Order, Topology, Algebra, and Sheaf Theory. Cambridge University Press. 2003.

# Inequality of Reals

Josef Berger

Ernst Moritz Arndt Universität Greifswald
Institut für Mathematik und Informatik
Walther-Rathenau-Straße 47
17487 Greifswald, Germany
bergerj@uni-greifswald.de

Working in the intuitionistic formal system *Elementary Analysis*, we show that the following statements are equivalent:

- $\forall x, y, z \in \mathbf{R}\,(x \neq y \to x \neq z \,\vee\, y \neq z)$
- $\forall x, y \in \mathbf{R}\,(x \neq y \to x \leq y \,\vee\, y \leq x)$
- The De Morgan law for $\varPi^0_1$-statements

$\mathbf{R}$ is the set of Cauchy reals. A Cauchy real is a sequence $(x_n)$ of rationals such that

$$\forall m, n \left(|x_m - x_n| \leq m^{-1} + n^{-1}\right).$$

The De Morgan law for $\varPi^0_1$-statements is the following axiom: For all $\varPi^0_1$-formulas $\varPhi$ and $\varPsi$, $\neg\,(\varPhi \wedge \varPsi) \Rightarrow \neg\varPhi \vee \neg\varPsi$ . A formula $\varPhi$ is called a $\varPi^0_1$*-formula* if there exists a binary sequence $\alpha$ such that

$$\varPhi \Leftrightarrow \forall n\,(\alpha n = 0)\,.$$

# REUNITING THE ANTIPODES: BRINGING TOGETHER NONSTANDARD ANALYSIS AND CONSTRUCTIVE ANALYSIS

SAM SANDERS

ABSTRACT. Recently, Sanders introduced an interpretation of Errett Bishop's *Constructive Analysis* (BISH) inside a particular system of classical Nonstandard Analysis called $\mathbb{NSA}$ ([7, 9]). The role of 'algorithm' is played by the notion $\Omega$-*invariance* ([6–9]); Intuitively, an object is $\Omega$-invariant if it does not depend on the *choice* of infinitesimal used in its definition. The role of 'proof' is played by the *Transfer Principle* of Nonstandard Analysis ([4, 5]) as follows: In the same way as the *Brouwer-Heyting-Kolmogorov*-interpretation is limited to provable formulas, we only consider formulas $A$ such that $A \leftrightarrow {}^*A$ in $\mathbb{NSA}$, i.e. formulas which 'satisfy Transfer'. As $\mathbb{NSA}$ does not include non-trivial Transfer Principles, only some formulas $A$ satisfy $A \leftrightarrow {}^*A$.

This interpretation from BISH into Nonstandard Analysis can be called 'natural' and 'faithful' in the following threefold way:

(i) Non-constructive principles (LPO, LLPO, MP, etc.) are interpreted as Transfer Principles which are not available in the system $\mathbb{NSA}$.

(ii) The interpretation preserves the equivalences of *Constructive Reverse Mathematics* ([2, 3]).

(iii) The interpretation preserves the property that the BISH-notion of algorithm is weaker than that of recursive function (See [1]).

We discuss the interpretation from BISH into $\mathbb{NSA}$, and related topics.

## REFERENCES

[1] Errett A. Bishop, *Schizophrenia in contemporary mathematics*, Errett Bishop: reflections on him and his research, Contemp. Math., vol. 39, Amer. Math. Soc., 1985, pp. 1–32.

[2] Hajime Ishihara, *Reverse mathematics in Bishop's constructive mathematics*, Philosophia Scientiae (Cahier Spécial) **6** (2006), 43-59.

[3] ———, *Constructive reverse mathematics: compactness properties*, From sets and types to topology and analysis, Oxford Logic Guides, vol. 48, 2005.

[4] Vladimir Kanovei and Michael Reeken, *Nonstandard analysis, axiomatically*, Springer, 2004.

[5] Abraham Robinson, *Non-standard analysis*, North-Holland, Amsterdam, 1966.

[6] Sam Sanders, *A tale of three Reverse Mathematics*, Submitted (2012).

[7] ———, *Reuniting the antipodes: Bringing together Nonstandard and Constructive Analysis*, Submitted to JSL (2012), pp. 49. Available from `http://cage.ugent.be/~sasander/papers/SALGO.pdf`.

[8] ———, *On algorithm and robustness in a Non-standard sense* (Hanne Andersen, Dennis Dieks, Wenceslao Gonzalez, Thomas Übel, and Gregory Wheeler, eds.), The Philosophy of Science in a European Perspective, Springer, 2013.

[9] ———, *Algorithm and Proof as $\Omega$-invariance and Transfer: A new model of computation in Nonstandard Analysis*, Electronic Proceedings in Computer Science, DCM (2012), In Press.

GHENT UNIVERSITY, DEPARTMENT OF MATHEMATICS, KRIJGSLAAN 281, 9000 GENT (BELGIUM)
MUNICH CENTER FOR MATHEMATICAL PHILOSOPHY, LUDWIG-MAXIMILIAN-UNIVERSITÄT
*E-mail address*: `sasander@cage.ugent.be, http://cage.ugent.be/∼sasander`.

# Decidability for type-related problems of 2nd-order $\lambda$-calculi and negative translations

Ken-etsu Fujita

Gunma University, Kiryu, Japan,
fujita@cs.gunma-u.ac.jp

We provide a framework that enables systematic proofs of the undecidability for type-related problems of $\lambda^\exists$ (minimal logic with negation, conjunction and 2nd order existential types) from the corresponding undecidability results for those of $\lambda 2$ (intuitionistic logic with implication and 2nd order universal types), see Fig 1. This framework is applicable to various styles of the system $\lambda^\exists$, e.g., Church, hole-application, domain-free, type-free, and Curry styles, see Fig 2.

| Problems \ Styles | Church | Hole-application | Domain-free | Type-free | Curry |
|---|---|---|---|---|---|
| Type checking | Yes | Yes | No | No | No |
| Typability | No | No | No | No | No |

"Yes" means that the problem is decidable, and "No" means undecidable.

**Fig. 1.** Decidability for type-related problems of $\lambda 2$ and styles of $\lambda$-terms

$$\begin{tikzcd}
\lambda 2 : \text{Church} \arrow[r, "|\,|^{\mathrm{ch}}_{\mathrm{df}}"] \arrow[d, shift right, "*^{\mathrm{ch}}"'] & \text{DF} \arrow[r, "|\,|^{\mathrm{df}}_{\mathrm{tf}}"] \arrow[d, shift right, "*^{\mathrm{df}}"'] & \text{TF} \arrow[r, "|\,|^{\mathrm{tf}}_{\mathrm{cu}}"] \arrow[d, shift right, "*^{\mathrm{tf}}"'] & \text{Curry} \arrow[d, shift right, "*^{\mathrm{cu}}"'] \\
\lambda^\exists : \text{Church} \arrow[r, "|\,|^{\mathrm{ch}}_{\mathrm{df}}"] \arrow[u, shift right, "\sharp^{\mathrm{ch}}"'] & \text{DF} \arrow[r, "|\,|^{\mathrm{df}}_{\mathrm{tf}}"] \arrow[u, shift right, "\sharp^{\mathrm{df}}"'] & \text{TF} \arrow[r, "|\,|^{\mathrm{tf}}_{\mathrm{cu}}"] \arrow[u, shift right, "\sharp^{\mathrm{tf}}"'] & \text{Curry} \arrow[u, shift right, "\sharp^{\mathrm{cu}}"']
\end{tikzcd}$$

**Fig. 2.** Overview of the framework

The framework essentially relies on two properties: (1) the commutativity of type-forgetful (type-erasing) mappings $|\cdot|$ and translations $*, \sharp$ between $\lambda 2$ and $\lambda^\exists$ such that $|N^{*^s}|^s_t = (|N|^s_t)^{*^t}$ and $|Q^{\sharp^s}|^s_t = (|Q|^s_t)^{\sharp^t}$; and (2) the lifting $|\ |^{-1}$ of terms to increasingly well-defined terms having the proper type information. The translations $*$ are so called negative translations or CPS-translations [1], and the definitions are lifted to derivations from terms. In this way, $*^t$-translation can be implemented by means of $|\ |$ and $*^s$, see Fig 3. Based on this approach, the following problems of $\lambda^\exists$ are shown to be undecidable: (i) the typability and type checking problems in the type-free style, and (ii) the type checking problem in the Curry style. Finally, we observe an interesting correspondence to a negative translation of semi-unification problems [2].

$$\begin{tikzcd}
\Gamma \vdash N : A \text{ for some } N \text{ in } s\text{-style } \lambda 2 \text{ s.t. } |N| = M \arrow[d, "\text{Negative translation } *^{s}"'] & \Gamma \vdash M : A \text{ in } t\text{-style } \lambda 2 \arrow[l, "\text{lifting } |\,|^{-1}"'] \arrow[d, "M^{*^{t}} = |N|^{*^{t}} = |N^{*^{s}}|"] \\
\neg\Gamma^*, a : A^* \vdash N^* : \bot \text{ in } s\text{-style } \lambda^\exists \arrow[r, "\text{erasing } |\,|"] & \neg\Gamma^*, a : A^* \vdash |N^*| : \bot \text{ in } t\text{-style } \lambda^\exists
\end{tikzcd}$$

**Fig. 3.** Soundness of $t$-style $\lambda 2$

## References

1. K. Fujita: CPS-translation as adjoint, Theoret. Comput. Sci. 411, 324–340, 2010.
2. K. Fujita: A framework for reduction from $\lambda 2$-calculi to $\lambda^\exists$-calculi, Computer Software 28-4, pp. 341–357, 2011.

# Subsystems of arithmetic as type theories with inductive definitions

Gyesik Lee

Hankyong National University
gslee@hknu.ac.kr

**Abstract.** This talk is about a project called "Reverse Mathematics in Coq".

The program called *reverse mathematics* is a foundation of mathematics that focuses on the analysis of the logical force of the most standard mathematical theorems. The logical framework in which mathematics is put down is one of the subsystems of second-order arithmetic, including the so-called big five: $\mathrm{RCA}_0$, $\mathrm{WKL}_0$, $\mathrm{ACA}_0$, $\mathrm{ATR}_0$, $\Pi^1_1$-$CA_1$. The best reference is Simpson [2010].

On the other hand, the past 40 years have seen the link between logic and computing, and more specifically between proofs and programs. The link got more intimate with the development of type theory by P. Martin-Löf in the course of 80 years which is both a logic system and a programming language and by the development of linear logic by J.-Y. Girard whose associated concept of polarity allows a detailed analysis of computational properties of the basic concepts of mathematical logic.

Since its introduction by H. Friedman in 1975, the research program of reverse mathematics has been extremely productive. It has in particular shown that the big five are sufficient for the formalization of the majority of standard mathematical theorems. However, the framework remained that of classical logic. Moreover, reverse mathematics has confined itself to the language of arithmetic which is not so efficient in practice.

Our work aims at providing a concrete framework based on a uniform type which is finer and more useful in practice than the big five, so that any logician or mathematician interested in formalizing the results of reverse mathematics can use it.

**Keywords:** Reverse mathematics, subsystems of arithmetic, type theories, Coq

## References

S. G. Simpson. *Subsystems of Second Order Arithmetic.* Perspectives in Logic. Cambridge University Press, 2010.

# An interactive semantics for classical proofs

Michele Basaldella

Japan Advanced Institute of Science and Technology (JAIST)
Research Center for Integrated Science (RCIS)
michele@jaist.ac.jp

The aim of this talk is to present a **semantics** for **proofs** in **classical logic**.

**Classical logic.** We use a variant of the proof–system introduced by Tait [5] (see also [4, 3, 1]), a system which is often used for analyzing the proof–theory of first–order classical arithmetic and its fragments. The language of this logic consists of infinitary propositional formulas, and the proof–system for this language is a sequent calculus with infinitary rules of inferences.

**Proofs.** The target of our analysis is not the provability predicate "the formula $\mathbf{A}$ is provable", but the relation "$\pi$ is a proof of the formula $\mathbf{A}$", which we abbreviate as $\pi \rhd \mathbf{A}$. In order to define this relation, we need to introduce the concept of "formula–free proofs", i.e., proofs that does not depend (too much) on the formulas they prove. To understand the idea behind this concept, consider the untyped lambda calculus. By the Curry–Howard correspondence, untyped lambda terms can be seen as a "formula–free" formalization of natural deduction proofs for the implicational fragment of intuitionistic propositional logic. In this context, $\pi \rhd \mathbf{A}$ can be read as "the untyped lambda term $\pi$ has (simple) type $\mathbf{A}$ in the Curry–style type assignment." Here we use a similar idea: we define a class of objects that we call *tests* which play the role of the untyped lambda terms, and we define $\pi \rhd \mathbf{A}$ by using Tait's *normal rules* as type assignment.

**Semantics.** Our semantics is deeply inspired by Girard's ludics [2]. As in untyped lambda calculus $\beta$–reduction can be seen as the natural deduction normalization procedure "without types", we similarly define a "formula–free" *cut–elimination* procedure which involves tests, that we call *interaction.* Using the notion of interaction, we define a relation $\pi \blacktriangleright \mathbf{A}$ which essentially states that the interaction between $\pi$ and any counter–test for $\mathbf{A}$ successfully terminates. The relation $\pi \blacktriangleright \mathbf{A}$ is the semantical counterpart of $\pi \rhd \mathbf{A}$. We finally show a soundness–and–completeness theorem: $\pi \rhd \mathbf{A}$ if and only if $\pi \blacktriangleright \mathbf{A}$.

## References

1. Coquand, T.: A semantics of evidence for classical arithmetic. J. Symb. Log. **60**(1) (1995) 325–337.
2. Girard, J.–Y.: Locus solum: From the rules of logic to the logic of rules. Math. Struct. in Comp. Sci. **11**(3) (2001) 301–506.
3. Pohlers, W.: Proof theory: an introduction. Spinger–Verlag (1989).
4. Schwichtenberg, H.: Proof theory: some applications of cut-elimination. In: Handbook of Mathematical Logic (Jon Barwise, editor) (1977) 867–895.
5. Tait, W.W.: Normal derivability in classical logic. In: The syntax and semantics of infinitary languages (Jon Barwise, editor), LNM **72** Springer–Verlag (1968) 204–236.

# Recursively defined trees and their maximal order types

Jeroen Van der Meeren

Department of Mathematics, Ghent University, Belgium
jvdm@cage.ugent.be

Well-partial-orderings (hereafter wpo) play an important role in for example logic, computer science and mathematics. They are the essential ingredient of famous theorems like Higman's lemma, Kruskal's theorem, Friedman's version of Kruskal's theorem ([2]) and the graph minor relation. In logic, wpo's are quite often related with the proof-theoretical ordinal of an axiomatic system and with ordinal notation systems. Hence, wpo's are important things to investigate.
A *well-partial-ordering* is a well-founded partial ordering $(X, \leq_X)$ with no infinite antichains. Hence, wpo's are the natural generalizations of the normal well-orderings. There is a natural connection between these two notions: every linear extension of a wpo is a well-ordering. Furthermore, De Jongh and Parikh [1] proved the following theorem: for every wpo $(X, \leq_X)$, there is a linear extension $\leq^+$ of $\leq_X$ such that the order type of the well-ordering $(X, \leq^+)$ is maximal. The order type of this maximal extension $\leq^+$ is denoted as $o(X)$ and is called the *maximal order type* of the wpo $(X, \leq_X)$. The maximal order type captures a lot of information about the wpo itself. Additionally, the maximal order type of a wpo is quite often equal to the proof-theoretical ordinal of a specific theory $T$. Hence, maximal order types, and therefore wpo's, are crucial things to study.

In [3], Weiermann introduced a specific class of trees depending on a mapping $W$ such that $\forall X(WPO(X) \rightarrow WPO(W(X)))$. That class of recursively defined trees is introduced to study the class of trees with a Friedman-style gap-condition for embeddability [2]. In this talk, I will give the definition of those recursively defined trees and talk about a general principle to compute their maximal order types. Furthermore, I want to discuss the natural question: 'Which theories $T$ can (and which cannot) prove the well-partial-orderedness of a given partial ordering $X$', and more specifically with $X$ equal to that class of recursively defined trees.

## References

1. D. H. J. de Jongh, R. Parikh: *Well-partial orderings and hierarchies.* Proc. K. Ned. Akad. Wet., Ser. A 80 (Indigationes Math. 39), 1977, pp. 195–207.
2. S. G. Simpson: *Nonprovability of certain combinatorial properties of finite trees.* Harvey Friedman's research on the foundations of mathematics, Studies in Logic and the foundation of mathematics, Elsevier Science Publishers B.V., The Netherlands, 1985, pp. 87–117.
3. A. Weiermann: *A computation of the maximal order type of the term ordering on finite multisets.* Mathematical Theory and Computational Practice (CiE 2009), vol. 5635/2009, Springer Berlin/Heidelberg, 2009, pp. 488–498.

# Inductive Definitions in Bounded Arithmetic: A New Way to Approach P vs. PSPACE*

Naohi Eguchi

Mathematical Institute, Tohoku University, Japan
eguchi@math.tohoku.ac.jp

Cook-Nguyen style second order bounded arithmetic has been developed mainly to deal with computational complexity classes smaller than **P**, the class of polynomial-time computable predicates, cf. [1]. It can be shown that a system $\mathrm{V}^1$ of second order bounded arithmetic captures **P** in the following sense.

1. A (string) function is polytime computable if and only if it is $\Sigma^{\mathrm{B}}_1$-definable in $\mathrm{V}^1$.
2. This implies that a predicates is polytime computable if and only if it is $\Delta^{\mathrm{B}}_1$-definable in $\mathrm{V}^1$.

(For the definition of the system $\mathrm{V}^{\mathrm{n}}$ ($n \in \mathbb{N}$) or $\Sigma^{\mathrm{B}}_{\mathrm{n}}$-formulas, see [1].) In [3] Alan Skelley has extended the system $\mathrm{V}^1$ to a system $\mathrm{W}^1_1$ of *third order* bounded arithmetic, capturing the class **PSPACE** of polynomial-space computable predicates. On the other hand, in finite model theory, it is known that polytime-computations can be captured by the least fixed points of monotone operators, while polyspace-computations can be captured by certain fixed points of non-monotone operators, cf. Ebbinghaus and Flum [2].

Motivated by those facts mentioned above we propose a principle LFP that formalise the existence of the least fixed point of a monotone operator, which is quite common in usual second order arithmetic. We show that a string function is polytime computable if and only if it is $\Sigma^{\mathrm{B}}_1$-definable in $\mathrm{V}^0 + \Sigma^{\mathrm{B}}_0$-LFP. Further we will generalise the least fixed principle LFP to non-monotone inductive definitions. The approach proposed in this talk will make it possible to discuss about polyspace-computations without using any third order notion, and hence would enable us to find a new aspect of the relationship between **P** and **PSPACE**.

## References

1. Stephen Cook and Phuong Nguyen. *Logical Foundations of Complexity.* Cambridge University Press, 2010.
2. Heinz-Dieter Ebbinghaus and Jörg Flum. *Finite Model Theory. Second edition.* Perspectives in Mathematical Logic. Springer, 1999.
3. Alan Skelley. A Third-order Bounded Arithmetic Theory for PSPACE. In *Proceedings of CSL 2004, LNCS*, volume 3210, pages 340–354. Springer, 2004.

* This work is generously supported by the research project *Philosophical Frontiers in Reverse Mathematics* sponsored by the John Templeton Foundation.

# Theories of concatenation, arithmetic, and undecidability

Yoshihiro Horihata[1]

Yonago National College of Technology,
Hikona 4448, Yonago, Tottori, JAPAN,
horihata@yonago-k.ac.jp,
WWW home page: https://sites.google.com/site/yoshihirohorihata/

**Abstract.** In 2005, Grzegorczyk introduced a theory $\mathsf{TC}$ of concatenation and proved its undecidability. In 2009, Visser, Švejdar, and Ganea independently proved that TC and Robinson's arithmetic $\mathsf{Q}$ are mutually interpretable. In this talk, we introduce a much weaker subtheory $\mathsf{WTC}$ of $\mathsf{TC}$, and show that $\mathsf{WTC}$ and Mostowski-Robinson-Tarski's arithmetic $\mathsf{R}$ are mutually interpretable. Since $\mathsf{R}$ is essentially undecidable, so is $\mathsf{WTC}$. We also show that some versions of $\mathsf{WTC}$ are to be minimal theories which are essentially undecidable.

**Keywords:** Theories of concatenation, First-order arithmetic, essentially undecidability

# Computably measurable sets and computably measurable functions in terms of algorithmic randomness

Kenshi Miyabe

Research Institute for Mathematical Sciences, Kyoto University

Measure theory has been used in many fields in mathematics such as probability theory, statistics and dynamical systems. Furthermore, their results have been used in many prorams running on computers. Thus, the relation with computation should not be unvalued.

One big problem of measure theory is that almost all theorems are equipped with the word "almost everywhere". By considering computability, we will be able to replace it with "all sufficiently random points". This is a big improvement.

There were some study of a computable version of measure theory in computable analysis. The research by Hoyrup and Rojas [2] was the first one that studied computable measure theory in terms of algorithmic randomness, that is, Martin-Löf randomness. However, it turned out that Schnorr randomness is more natural in the study of computable measure theory [4, 3]. Thus, we restart it again in terms of Schnorr randomness.

The notion of computable measurable set has been studied in the literature and there are two major approaches, the approximation approach [6, 1, 2] and the approach via regularity [1, 2]. However, we can show that they induce exactly the same notion up to Schnorr null. Similarly, we can show that the notion of computable measurable functions is equivalent to Schnorr layerwise computability. By combining with my previous work [3], a computable measurable function has a computable integral iff it is an effective $L^1$-computable function [5, 4, 3]. Thus, two computable measurable functions are equal almost everywhere iff they are equal at all Schnorr random points.

## References

1. Edalat, A.: A computable approach to measure and integration theory. Information and Computation 207(5), 642–659 (2009)
2. Hoyrup, M., Rojas, C.: An Application of Martin-Löf Randomness to Effective Probability Theory. In: CiE. pp. 260–269 (2009)
3. Miyabe, K.: $L^1$-computability, layerwise computability and Solovay reducibility, submitted
4. Pathak, N., Rojas, C., Simpson, S.G.: Schnorr randomness and the Lebesgue Differentiation Theorem, to appear in Proceedings of the American Mathematical Society
5. Pour-El, M.B., Richards, J.I.: Computability in analysis and physics. Springer (1989)
6. Sanin, N.: Constructive Real Numbers and Constructive Function Spaces, Translations of Mathematical Monographs, vol. 21. Ametican Mathematical Society, Providence (1968)

# On the Notions of Relative Randomness

NingNing Peng

Mathematical Institute, Tohoku University
Sendai-shi, Miyagi-ken, 980-8578, Japan
sa8m42@math.tohoku.ac.jp

**Abstract**

Let $\Gamma$ be a set of (Turing) oracles. A set $Z$ is called $\Gamma$-random if $Z$ is ML-random relative to $A$ for all $A \in \Gamma$. We use $\mathbb{L}$ and $\mathbb{G}$ to denote the set of low sets and the set of 1-generic sets, respectively. In [1], Yu proved that $\mathbb{L}$-randomness is equivalent to $\emptyset'$-Schnorr randomness, where $\emptyset'$ denotes the halting problem. In this talk, we show that $(\mathbb{G} \cap \mathbb{L})$-randomness is still equivalent to $\emptyset'$-Schnorr randomness. On the other hand, we study the lowness and highness properties for certain randomness notions.

## References

[1] Liang Yu: *Characterizing strong randomness via Martin-Löf randomness.* Annals of Pure and Applied Logic, vol.**163**, no. 3, pp. 214-224 (2012).

[2] NingNing Peng, Kojiro Higuchi, Takeshi Yamazaki and Kazuyuki Tanaka: *Relative Randomness for Martin-Löf random Sets.* Lecture Notes in Computer Science, vol.**7318**, pp 581-588 (2012).

# The Generic Group Model and Algorithmic Randomness

Kohtaro Tadaki Norihisa Doi

Research and Development Initiative, Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
E-mail: tadaki@kc.chuo-u.ac.jp, doi@doi.ics.keio.ac.jp

**Abstract.** In modern cryptography, the generic group model [6] is widely used as an *imaginary* framework in which the security of a cryptographic scheme is discussed. In particular, the generic group model is often used to discuss the computational hardness of problems, such as the discrete logarithm problem and the Diffie-Hellman problem, which are used as a computational hardness assumption to prove the security of a cryptographic scheme. In this talk, we apply the concepts and methods of *algorithmic randomness* to the generic group model, and consider the secure instantiation of the generic group, i.e., a random encoding of the group elements. In particular we show that the generic group can be instantiated by a specific computable function while keeping the computational hardness of the problems originally proved in the generic group model.

*Key words*: cryptography, provable security, generic group model, instantiation, discrete logarithms, Diffie-Hellman problem, lower bounds, algorithmic randomness

## References

1. D. Aggarwal and U. Maurer, Breaking RSA Generically Is Equivalent to Factoring. *Proc.* EUROCRYPT 2009, Lecture Notes in Computer Science, Springer-Verlag, Vol.5479, pp.36–53, 2009.
2. A. W. Dent, Adapting the Weaknesses of the Random Oracle Model to the Generic Group Model. *Proc.* ASIACRYPT 2002, Lecture Notes in Computer Science, Springer-Verlag, Vol.2501, pp.100–109, 2002.
3. U. Maurer and S. Wolf, Lower Bounds on Generic Algorithms in Groups. *Proc.* EUROCRYPT'98, Lecture Notes in Computer Science, Springer-Verlag, Vol.1403, pp.72–84, 1998.
4. D. Moriyama, R. Nishimaki and T. Okamoto, *Theory of Public-Key Cryptography.* Industrial and Applied Mathematics Series Vol.2. JSIAM, Kyoritsu Shuppan Co., Ltd., Tokyo, 2011. In Japanese.
5. A. Nies, *Computability and Randomness.* Oxford University Press, New York, 2009.
6. V. Shoup, Lower Bounds for Discrete Logarithms and Related Problems. *Proc.* EUROCRYPT'97, Lecture Notes in Computer Science, Springer-Verlag, Vol.1233, pp.256–266, 1997.
7. K. Tadaki and N. Doi, Instantiating the Random Oracle Using a Random Real. *Proc.* SCIS2012, 2A3-4, January 30-February 2, 2012, Kanazawa, Japan.
8. K. Tadaki and N. Doi, A Secure Instantiation of the Random Oracle by a Computable Function. *Proc.* SITA2012, 3.4.1, pp.212–217, December 11-14, 2012, Beppu, Oita, Japan.

# Where closure under Turing jumps can replace elementarity between structures

Tin Lok Wong

Department of Mathematics, Ghent University, Belgium
wtl@cage.ugent.be

Structures of the form $(M, I)$, where $I$ is an initial segment of a nonstandard model of arithmetic $M$, have long been of interest to nonstandard analysts. These structures recently gained interests amongst model theorists working on nonstandard arithmetic too. Surprisingly, such pairs $(M, I)$ were rarely studied in the context of model theory. One of the two notable exceptions is Vladimir Kanovei's 1996 paper on external Scott algebras.

In Kanovei's paper, he observed that if $M$ is a proper elementary extension of the natural numbers $\mathbb{N}$, then the external Scott algebra of $M$ contains a real from the Turing degree $\mathbf{0}^{(\omega)}$. This talk is about some variants of this observation from my joint work with Richard Kaye (University of Birmingham, UK) and Roman Kossak (City University of New York, USA). Amongst other things, we showed that Kanovei's elementarity condition can be replaced by $M$ being a nonstandard model of Peano arithmetic whose standard system is closed under the Turing jump operation. Results of this kind open new lines of research in the model theory of nonstandard arithmetic.

# Several versions of Friedman's self-embedding theorem

Keita Yokoyama*

Department of Mathematical and Computing Sciences, Tokyo Institute of Technology,
2-12-1 Oh-okayama, Meguro-ku, Tokyo 152-8551, JAPAN.
e-mail: yokoyama.k.ai@m.titech.ac.jp

In [1], H. Friedman showed the famous self-embedding theorem for PA which asserts that every countable model of PA has an initial segment which is isomorphic to itself. Actually, it can be generalize to the following (see e.g., [2, Section 12]): for every countable model of $\mathrm{I}\Sigma_n$, (†) there exists a $\Sigma_n$-elementary initial segment which is isomorphic to itself.

However, this statement is not strong enough to characterize countable models of $\mathrm{I}\Sigma_n$, *i.e.*, there exists a countable model $M$ which satisfies (†) but $M \not\models \mathrm{I}\Sigma_n$. In fact, (†) characterizes $\mathrm{B}\Sigma_n$ in the following sense.

**Theorem 1.** *Let $n \geq 0$, and let $M$ be a countable recursively saturated model of $\mathrm{I}\Sigma_0 + \exp$. Then, $M$ is a model of $\mathrm{B}\Sigma_{n+1}$ if and only if there exists a $\Sigma_n$-elementary self-embedding $f : M \to M$ such that $f(M) \subsetneq_e M$.*

Then, can we characterize countable models of $\mathrm{I}\Sigma_n$ by a self-embedding theorem? The answer is yes. Actually, (†) with the notion of semi-regular cut characterizes $\mathrm{I}\Sigma_n$.

**Theorem 2.** *Let $n \geq 1$, and let $M$ be a countable model of $\mathrm{I}\Sigma_0 + \exp$. Then, $M$ is a model of $\mathrm{I}\Sigma_n$ if and only if there exists a $\Sigma_n$-elementary self-embedding $f : M \to M$ such that $f(M) \subsetneq_e M$ is a semi-regular cut.*

Using self-embedding theorems, we can also characterize subsystems of second-order arithmetic. The most important example is Tanaka's self-embedding theorem for $\mathsf{WKL}_0$ [3]. In this talk, I will introduce several notions of cuts, and give several versions of self-embedding theorems which characterize important subsystems of Peano arithmetic or second-order arithmetic.

## References

1. Harvey Friedman. Countable models of set theories. In *Cambridge Summer School in Math. Logic*, volume 337 of *Lecture Notes in Math.*, pages 539–573, 1973.
2. Richard Kaye. *Models of Peano Arithmetic.* Oxford Logic Guides, 15. Oxford University Press, 1991. x+292 pages.
3. Kazuyuki Tanaka. The self-embedding theorem of $\mathsf{WKL}_0$ and a non-standard method. *Annals of Pure and Applied Logic*, 84:41–49, 1997.

* This research was supported by a JSPA postdoctoral fellowship for young scientists, and by a grant from the John Templeton Foundation.

# Parameterized Uniform Complexity in Numerics: from Smooth to Analytic, from $\mathcal{NP}$–hard to Polytime[*]

Akitoshi Kawamura[1], Norbert Th. Müller[2], Carsten Rösnick[3], Martin Ziegler[3]

[1] University of Tokyo [2] Universität Trier [3] TU Darmstadt

The synthesis of classical Computational Complexity Theory with Recursive Analysis [4, 7, 10] provides a quantitative foundation to reliable numerics [1]. Here the operators of maximization and integration are known to map (even smooth, i.e. infinitely often differentiable) polynomial-time computable functions to instances which are 'hard' for classical complexity classes $\mathcal{NP}$ and $\#\mathcal{P}$ [5]; but, restricted to analytic functions, map polynomial-time computable ones to polynomial-time computable ones [8, 9] — non-uniformly! We investigate the uniform parameterized complexity of the above operators in the setting of [2] when climbing up Gevrey's hierarchy of functions from analytic to smooth:

**Definition 1** *Write $G_{\ell,A,K}[-1;1]$ for the class of $C^\infty$–functions $f:[-1;1]\to\mathbb{R}$ satisfying*

$$\forall|x|\le 1,\ \forall j\in\mathbb{N}: \qquad |f^{(j)}(x)| \ \le\ A\cdot K^j\cdot j^{j\ell} \ ; \tag{1}$$

*$G_\ell := \bigcup_{A,K\ge 1} G_{\ell,A,K}$ and $G := \bigcup_{\ell\in\mathbb{N}} G_\ell$. Let $\tilde\gamma$ denote the following second-order representation of $G[-1;1]$: A name of $f$ satisfying Equation (1) is a length-monotone mapping*

$$\{\mathtt{0},\mathtt{1}\}^* \ \ni\ \vec{w}\ \mapsto\ \mathtt{1}^{\log A+K+|\vec{w}|^\ell}\,\mathtt{0}\,\psi(\vec{w})\ \in\{\mathtt{0},\mathtt{1}\}^*\ ,$$

*where $\psi$ denotes a $\delta_\square$–name of $f$ according to* [2, §4.3].

Note that $G_1$ coincides with the class of analytic functions [6]. Our main result is

**Theorem 2.** *Representation $\tilde\gamma$ renders evaluation, addition, multiplication, (iterated) differentiation, integration, and maximization uniformly computable in time polynomial in $K+\log A+n^{\operatorname{poly}\ell}$. For fixed $\ell\in\mathbb{N}$, $(\delta_\square,\rho_{\mathrm{sd}})$–computing $f\mapsto\max(f)$ on $G_{\ell+1,1,1}[-1;1]$ requires time at least $\Omega(n^\ell)$.*

1. M. Braverman, S.A. Cook: "Computing over the Reals: Foundations for Scientific Computing", pp.318–329 in *Notices of the AMS* vol.**53:3** (2006).
2. A. Kawamura, S.A. Cook: "Complexity Theory for Operators in Analysis", pp.495–502 in *Proc. 42nd Ann. ACM Symp. on Theory of Computing* (STOC 2010);
   full version in *ACM Transactions in Computation Theory* vol.**4:2** (2012), article 5.
3. A. Kawamura, H. Ota, C. Rösnick, M. Ziegler: "Computational Complexity of Smooth Differential Equations", pp.578–589 in *Proc. 37th Int. Symp. on Mathematical Foundations of Computer Science* (MFCS'2012), Springer LNCS vol.**7464**.
4. K.-I. Ko: "Polynomial-Time Computability in Analysis", pp.1271–1317 in (Yu. L. Ershov et al., Eds.) *Handbook of Recursive Mathematics* vol.**2** (1998).
5. K.-I. Ko, H. Friedman: "Computational Complexity of Real Functions", pp.323–352 in *Theoretical Computer Science* vol.**20** (1982).
6. S.G. Krantz, H.R. Parks: "*A Primer of Real Analytic Functions*", 2nd Edition, Birkhäuser (2002).
7. S. Labhalla, H. Lombardi, E. Moutai: "Espaces métriques rationnellement présentés et complexité, le cas de l'espace des fonctions réelles uniformément continues sur un intervalle compact", pp.265–332 in *Theoretical Computer Science* vol.**250** (2001).
8. N.T. Müller: "Uniform Computational Complexity of Taylor Series", pp.435–444 in *Proc. 14th Int Coll. on Automata, Languages, and Programming* (ICALP'87), Springer LNCS vol.**267**.
9. N.T. Müller: "Constructive Aspects of Analytic Functions", pp.105–114 in *Proc. Computability and Complexity in Analysis* (CCA), InformatikBerichte FernUniversität Hagen vol.**190** (1995).
10. K. Weihrauch: "Computational Complexity on Computable Metric Spaces", pp.3–21 in *Mathematical Logic Quarterly* vol.**49:1** (2003).

[*] See `arXiv:abs/1211.4974` for the full version. The first author is supported in part by *Kakenhi* (Grant-in-Aid for Scientific Research) `23700009`; the others by the *Marie Curie International Research Staff Exchange Scheme Fellowship* `294962` within the 7th European Community Framework Programme.

# Bounded arithmetic in free logic

Yoriyuki Yamagata
yoriyuki.yamagata@aist.go.jp

National Institute of Advanced Industrial Science and Technology (AIST)

One of the central open questions in bounded arithmetic is whether Buss' hierarchy $S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq T^2_2 \subseteq \cdots$ of theories of bounded arithmetic collapses or not, since collapse of Buss' hierarchy implies the collapse of the polynomial-time hierarchy.

A natural way to demonstrate non-collapse of the theories in Buss' hierarchy would be to identify one of these theories that proves (some appropriate formulation of) a statement of the consistency of some theory below it in the hierarchy. Here, it is clear that we need a delicate notion of consistency since according to previous research, it appears that $S^i_2$ is not able to prove the consistency, unless the system is very weak.

In this talk, we introduce the theory $S^i_2E$ ($i = -1, 0, 1, 2 \ldots$), which for $i \geq 1$ corresponds to Buss' $S^i_2$, and we show that the consistency of strictly $i$-normal proofs that are carried out only in $S^{-1}_2E$, can be proved in $S^{i+2}_2$.

$S^i_2E$ is based on the following observation: The difficulty in proving the consistency of bounded arithmetic inside $S_2$ stems from the fact that inside $S_2$ we cannot define the evaluation function which, given an assignment of natural numbers to the variables, maps the terms of $S_2$ to their values. For example, the values of the terms $2, 2\#2, 2\#2\#2, 2\#2\#2\#2, \ldots$ increase exponentially; therefore, we cannot define the function that maps these terms to their values, since the rate of growth of every function which is definable in $S_2$ is dominated by some polynomial in the length of the input. With a leap of logic, we consider this fact to mean that we cannot assume the existence of values of arbitrary terms in bounded arithmetic. Therefore, we must explicitly prove the existence of values of the terms that occur in any given proof.

Based on this observation, $S^i_2E$ is formulated by using *free logic* instead of the ordinary predicate calculus. Free logic is a logic which is free from ontological assumptions about the existence of the values of terms. Existence of such objects is explicitly stated by an existential predicate rather than being implicitly assumed.

Using free logic, we can force each proof carried out within $S^{-1}_2E$ to somehow "contain" the values of the terms that occur in the proof. By extracting these values from the proof, we can evaluate the terms and then determine the truth value of $\Sigma^b_i$ formulae. The standard argument using a truth predicate proves the consistency of strictly $i$-normal proofs that are carried out only in $S^{-1}_2$. It is easy to see that such a consistency proof can be carried out in $S^{i+2}_2$.

# Computability and Conditional Probability

Cameron E. Freer

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology, Cambridge, MA, USA
freer@math.mit.edu

Conditional probability is a key notion in probability theory and plays a central role in Bayesian statistics and machine learning. I will present several results obtained jointly with Nate Ackerman and Dan Roy, examining the computability of conditional probability. This work makes use of techniques from computable analysis and algorithmic randomness, and has applications to nonparametric Bayesian statistics and probabilistic programming languages.