37-èmes Journées sur les Arithmétiques Faibles

37-th Weak Arithmetics Days

JAF 37

May 28-30, 2018

Villa Finaly, Florence - Italy

Conference Programme

Monday, May 28 2018

Morning

9h: Registration

9h45: Openning session

10h: Olivier Finkel (Paris VII) Polishness of some topologies related to automata [Joint work with Olivier Carton and Dominique Lecomte]

10h30: Coffee break

11h15: Laurence Kirby (Baruch College, CUNY) Bounded finite set theory
11h45: Jana Glivická (Prague) Models of arithmetics with linear induction

Lunch (13h)

Afternoon

14h30: Eugenio Omedeo (Trieste, Italy) Further reflections on candidate "rule-them-all" Diophantine equations [Joint work with Domenico Cantone]
15h00: Mihail Starchak (Saint Petersburg) Two Classes of Basic Divisibility Families from NP

15h30: Coffee break

16h15: Petr Glivický (Prague) Fermat's last theorem and Catalan's conjecture in arithmetics with weak exponentiation

Tuesday, May 29 2018

Morning

9h30: Julien Cervelle (Paris 12) Study of stepwise simulation between ASMs [Joint work with Patrick Cégielski]
10h: Charalampos Cornaros (University of Aegean, Greece) Products of primes in weak systems of arithmetic

10h30: Coffee break

11h15: Yuri Gurevich (Ann Arbor) LOGIC in computer science, computer engineering and mathematics

Lunch (13h)

Afternoon

14h30: Fedor Pakhomov (Steklov Institute, Moscow) Weak Set Theories and Δ_0-Collection
15h30: Jean-Eric Pin (Paris VII) Regular languages, profinite topologies and weak arithmetic

16h30: Coffee break

17h15: Costas Dimitracopoulos (Athens) End extensions of models of fragments of PA [Joint work with Vasileios Paschalis]

19h00: Special Dinner

Wednesday, May 30 2018

9h30: Michał Tomasz Godziszewski (Warzaw) Π^0_1-computable quotient presentation of a nonstandard model of arithmetic
10h: Pierre Valarcher (Paris 12) Primitive recursion and algorithmically-completeness for Primitive Recursive Class of functions [Joint work with Patrick Cégielski and Serge Grigorieff]

10h30: Coffee break

11h15: Mateusz Łełyk (Poland) How useful are pure compositional axioms for the truth predicate?

12h15: Closure - Distribution of lunch boxes

Further reflections on candidate "rule-them-al" Diophantine equations

Domenico Cantone [a] and Eugenio G. Omodeo [b]

If the quaternary quartic equation

$$9\,\left(u^2+7\,v^2\right)^2-7\,\left(r^2+7\,s^2\right)^2 \quad = \quad 2 \qquad (*)$$

which M. Davis put forward in 1968 has only finitely many solutions in integers, then—as observed by M. Davis, J. Robinson, and Yu. V. Matiyasevich in 1976—every listable set would turn out to admit a single-fold Diophantine representation.

In 2017, we proposed another candidate for the role of "rule-them-all" equation, namely the quaternary quartic equation

$$3\,\left(r^2+3\,s^2\right)^2-\left(u^2+3\,v^2\right)^2 \quad = \quad 2\,, \qquad (\dagger)$$

whose significance can be supported by much the same arguments found in Davis's original paper. Directly from the unproven assertion that this novel equation has only finitely many solutions in integers, and closely following Davis's 'recipe', we showed how to construct a Diophantine relation of exponential growth. Short after the JAF 36 conference in St. Petersburg, two non-trivial solutions to (†) were found by Dr. Boris Z. Moroz and by Carsten Roschinski, and kindly communicated to us.

Then we sought further candidate "rule-them-all" equations, in the hope that one would prove easier to analyze than the others. Pietro Corvaja gave us clues on how to proceed systematically: When $d>1$ is a square-free rational integer for which the integers of the quadratic field $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization ring, Davis's approach can be pursued without difficulty; in absence of unique factorization, the situation becomes more cumbersome but nonetheless viable for infinitely many discriminants $-d$. Following those clues, we have successfully tackled the relatively unproblematic cases $d=2$ and $d=11$, obtaining the following rule-them-all equations:

$$\begin{aligned} 2\,\left(r^2+2\,s^2\right)^2-\left(u^2+2\,v^2\right)^2 &= 1\,,\\ 11\,\left(r^2\pm r\,s\,+3\,s^2\right)^2-\left(u^2\pm u\,v+3\,v^2\right)^2 &= 2\,. \end{aligned}$$

[a] DMI, University of Catania, Italy; cantone@dmi.unict.it
[b] DMG/DMI, University of Trieste, Italy; eomodeo@units.it

Polishness of some topologies related to automata

Olivier Carton [a], Olivier Finkel [b] and Dominique Lecomte [c]

The languages of infinite words, also called ω-languages, accepted by finite automata were first studied by Büchi to prove the decidability of the monadic second order theory of one successor over the integers. Since then regular ω-languages have been much studied and used for specification and verification of non-terminating systems [9, 7].

The Cantor topology is a very natural topology on the set Σ^ω of infinite words over a finite alphabet Σ which is induced by the prefix metric. It has been used in particular to study the topological complexity of languages of infinite words accepted by various kinds of automata, and firstly to locate them with regard to the Borel and the projective hierarchies [9].

However, as noticed in [8] by Schwarz and Staiger and in [3] by Hoffmann and Staiger, it turned out that for several purposes some other topologies on a space Σ^ω are useful, for instance for studying fragments of first-order logic over infinite words or for a topological characterisation of random infinite words (see also [4]). In particular, Schwarz and Staiger studied four topologies on the space Σ^ω of infinite words over a finite alphabet Σ which are all related to automata, and refine the Cantor topology on Σ^ω: the Büchi topology, the automatic topology, the alphabetic topology, and the strong alphabetic topology. These four topologies are shown to be metrizable in [8].

We prove that the Büchi topology, the automatic topology, the alphabetic topology and the strong alphabetic topology are Polish, and provide consequences of this. We also show that this cannot be fully extended to the case of a space of infinite labelled binary trees; in particular, the Büchi and the Muller topologies in that case are not Polish.

[a] IRIF, Université Paris Diderot, Paris, France; Olivier.Carton@irif.fr
[b] CNRS et Institut de Mathématiques de Jussieu-Paris Rive Gauche, Université Paris Diderot, Paris, France; finkel@math.univ-paris-diderot.fr
[c] Institut de Mathématiques de Jussieu-Paris Rive Gauche, Sorbonne Université, Paris, France; dominique.lecomte@upmc.fr

References

[1] O. Carton, O. Finkel, and D. Lecomte, *Polishness of Some Topologies Related to Automata*. In Valentin Goranko and Mads Dam, editors, 26th EACSL Annual Conference on Computer Science Logic (CSL 2017), volume 82 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:16, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[2] O. Carton, O. Finkel, and D. Lecomte, *Polishness of Some Topologies Related to Automata (Extended version)*, 2017. Preprint, available from ArXiv:1710.04002.

[3] S. Hoffmann and L. Staiger, *Subword metrics for infinite words*, In Frank Drewes, editor, *Implementation and Application of Automata - 20th International Conference, CIAA 2015, Umeå, Sweden, August 18-21, 2015, Proceedings*, volume 9223 of Lecture Notes in Computer Science, pages 165–175. Springer, 2015.

[4] S. Hoffmann, S. Schwarz, and L. Staiger, *Shift-invariant topologies for the Cantor space X^ω*, Theoretical Computer Science, 679:145–161, 2017.

[5] A. S. Kechris, *Classical descriptive set theory*. Springer-Verlag, New York, 1995.

[6] Y. N. Moschovakis. *Descriptive set theory*, volume 155 of Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, second edition, 2009.

[7] D. Perrin and J.-E. Pin, *Infinite words, automata, semigroups, logic and games*, volume 141 of Pure and Applied Mathematics. Elsevier, 2004.

[8] S. Schwarz and L. Staiger, *Topologies refining the Cantor topology on X^ω*, In C. S. Calude and V. Sassone, editors, *Theoretical Computer Science - 6th IFIP TC 1/WG 2.2 International Conference, TCS 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010. Proceedings*, volume 323 of IFIP Advances in Information and Communication Technology, pages 271–285. Springer, 2010.

[9] L. Staiger, *ω-languages*, In *Handbook of formal languages, Vol. 3*, pages 339–387. Springer, Berlin, 1997.

Study of stepwise simulation between ASMs

Patrick Cégielski [a] and Julien Cervelle [b]

Yuri Gurevich gave a schema of languages which is not only a *Turing-complete language* (a language allowing to program each computable function), but which also allows to describe step-by-step the behavior of all algorithms for each computable function (it is an *algorithmically complete language*).

ASM (*Abstract State Machine*) is the only known model of computation to have the property of capturing any execution of a model of computation. However, some other models of computation are interesting because they respect a weaker variant of this property. The idea is to liberalize a condition: Instead of requiring perfect matching of the runs, one allows the runs to be only equivalent in a sense that there exists k and k' such that equality holds for only an element every k elements for the first run, and an element every k' elements for the second run (defined as k, k'*-equivalence* in the paper). As ASM can be sped up by any linear factor, it corresponds to some weak algorithmic completeness.

Moreover, some authors (see for instance [2]), proving this weaker property for their model, insist on having regularly an element every k elements (for instance 2, 4, 6, ... for $k = 2$) and not just allowing to discard at most $k - 1$ elements (for instance 1, 3, 4, 5, 7, ...). No explanation is given to justify such a constraint but this causes them to add some `skip` instructions (steps during which the machine does nothing) to align things precisely.

Then a natural question arises: Is it essential to force the regularity? One way of getting enlightenment about the question is to see if we can build two ASMs A and B whose traces are all equal up to irregular dilatation but such that the set of points to be removed is not a recursive set. This means that the two computations are equivalent but that, somehow, one of the ASMs computes something more in its run than the other one.

The authors proves that one can build two ASMs whose runs are equivalent but without the regularity and such that the positions to be removed (at most two of them) are not computable from the input. This proves that enforcing the regularity is essential since it takes into account the computation time and not only the computed values.

[a] LACL, Université Paris-Est Créteil, France; `patrick.cegielski@u-pec.fr`

[b] LACL, Université Paris-Est Créteil, France; `julien.cervelle@u-pec.fr`

References

[1] Gurevich, Yuri, *Reconsidering Turing's Thesis: Toward More Realistic Semantics of Programs*, University of Michigan, Technical Report CRL–TR–38–84, EECS Department (1984)

[2] Marquer, Yoann and Valarcher, Pierre, *An Imperative Language Characterizing PTIME Algorithms*, in *Studies in Weak Arithmetics 3*, Patrick Cégielski, Ali Enayat and Roman Kossak, eds., Lecture Note 217, CSLI Publications, Stanford, 2016.

Products of primes in weak systems of arithmetic

Charalambos Cornaros
University of the Aegean, Greece
kornaros@aegean.gr

We study the strength of axioms asserting the existence of products of primes $\prod_{p \text{ prime}, p\leq x} p$ for various x (x greater than a logarithm). Variations of these axioms can also be formulated when we enumerate the primes inside the product:

$$\exists p \exists s \left(p \text{ is the } x\text{-th prime} \geq 2 \wedge s = \prod_{q \text{ prime},\ q\leq p} q \right)$$

The axiom

$$\forall x \exists t \left(t = \prod_{p \text{ prime},\ p\leq x} p \right)$$

cannot be proven from $I\Delta_0$. This axiom is equivalent with the axiom PRO:

$$(\forall p)(prime(p) \rightarrow \exists x (x = \textstyle\prod_{q \text{ prime},\ q\leq p} q))$$

studied in [1] and so is equivalent with exp over $I\Delta_0$. From the proof of Lemma 6.1 in [4], we know that there are two fixed standard numbers $C, D \in \mathbb{N}$, such that

$$I\Delta_0 \vdash \forall x \exists y \left(y = \prod_{p \text{ prime},\ p\leq C\log(x)} p \wedge x < y < x^D \right),$$

where $\log(x)$ denotes $[\log_2(x)]$. It follows that all products $\prod_{p \text{ prime},\ p\leq \log(x)} p$ do exist for all x in any model of $I\Delta_0$. The $\log(x)$ in the bound of the factors of this product can be replaced with bigger quantities less than x, like

$$\log(x)\log^{(2)}(x), \log^2(x), \log(x)^{\log^{(2)}(x)}, \log(x)^{\log^{(2)}(x)^{\log^{(3)}(x)}} \ldots$$

We study the strength of axioms expressing the existence of these products and prove some results in relation to the $(\Omega_n), n \in \mathbb{N}$, hierarchy(see, eg, [3]). For example, we prove that the axiom

$$\forall x \geq 2 \exists y \left(y = \prod_{p \text{ prime},\ p\leq \log^2(x)} p \right)$$

is equivalent with Ω_1 over $I\Delta_0$ and, under Bertrand's Postulate, the axiom

$$\forall x \geq 2 \exists y \left(y = \prod_{p \text{ prime},\ p\leq p_{(x)}} p \right)$$

is equivalent with Ω_1 over $I\Delta_0$. $p_{(x)}$ is the $\log^2(x)$-th prime in an increasing enumeration of primes $p_1 = 2, p_2 = 3, \ldots$ and prove some equivalences in relation to the Ω hierarchy.

Taking any model of $I\Delta_0 + \neg\Omega_1$, we conclude that there exist models of $I\Delta_0$ such that all products of the form

$$\forall x \geq 2 \exists y \left(y = \prod_{p \text{ prime},\ p\leq \log(x)} p,\ x \geq 2, \right)$$

exist, but which do not satisfy

$$\forall x \geq 2 \exists y \left(y = \prod_{p \text{ prime},\ p\leq \log^2(x)} p \right).$$

References

[1] Ch. Cornaros, C. Dimitracopoulos, *A note on exponentiation*, J. Symbolic Logic 58 (1993), 64–71.

[2] C. Dimitracopoulos, J. Paris, *The pigeonhole principle and fragments of arithmetic*, Z.Math. Logik Grundlag. Math, vol. 32 (1986), 73–80.

[3] P Hájek, Pavel Pudlák, *Metamathematics of First-Order Arithmetic*, Springer (1998), p. 272.

[4] A. R. Woods, *Some problems in logic and number theory and their connections*, in P. Cegielski, C. Cornaros and C. Dimitracopoulos(eds.): New Studies in Weak Arithmetics, CSLI Publications, 2013, 275–365.

End extensions of models of fragments of PA

Costas Dimitracopoulos [a] and Vasileios Paschalis [b]

In this paper, we prove results concerning the existence of proper end extensions of arbitrary models of fragments of Peano arithmetic (PA). In particular, we give alternative proofs of two results concerning the end extendability of arbitrary models of fragments of PA. Our proofs concern (a) a result of P. Clote (see [1] and [2]), on the end extendability of arbitrary models of Σ_n-induction, for $n \geq 2$, and (b) the fact that every model of Σ_1-induction has a proper end extension satisfying Δ_0-induction (although this fact was not explicitly stated before, it follows by earlier results of A. Enayat and T. L. Wong - see [4] and [5]).

References

[1] P. Clote, *A note on the MacDowell-Specker theorem*, Fund. Math. 127 (1986), no. 2, 163–170.

[2] P. Clote, *Addendum to: "A note on the MacDowell-Specker theorem" [Fund. Math. 127 (1987), no. 2, 163–170]*, Fund. Math. 158 (1998), no. 3, 301–302.

[3] C. Dimitracopoulos and V. Paschalis, *End extensions of models of weak arithmetic theories*, Notre Dame J. Formal Logic 57 (2016), 181–193.

[4] A. Enayat and T. L. Wong, *Unifying the model theory of first-order and second-order arithmetic via* WKL_0^*, Ann. Pure Appl. Logic 168 (2017), 1247–1252.

[5] T.L. Wong, *Interpreting Weak König's Lemma using the arithmetized completeness theorem*, Proc. Amer. Math. Soc. 144 (2016), 4021–4024.

[a] University of Athens, Greece, cdimitr@phs.uoa.gr
[b] University of Athens, Greece, vpasxal@math.uoa.gr

Models of arithmetics with linear induction

Jana Glivická
University of Economics, Prague, Czech Republic
jana.glivicka@gmail.com

We say that a formula $\varphi(x, y_1, \ldots, y_n)$ in the language of arithmetic is x-linear if every multiplication occurring in $\varphi(x, \bar{y})$ is of the form $y_i \cdot t$ or $t \cdot y_i$, for some $i < n$, where t is a term. Linear induction is then induction over x for x-linear formulas and the theory extending Robinson arithmetic by full linear induction is denoted ILin. In the talk, we will present some results of an ongoing research on ILin and its models conducted in collaboration with Petr Glivický, Josef Mlček and Jan Šaroch.

We focus mainly on a certain class of models of ILin that can be obtained as substructures of nonstandard models of Peano arithmetic generated from one nonstandard element by operations of addition, multiplication and standard division (if possible). Such structures are, up to isomorphism, determined by one parameter τ, describing the moduli of the generator after division by standard powers of standard primes.

We show how the choice of τ impacts validity of certain natural arithmetical properties, in particular we show how to construct models such that a) prime pairs are cofinal in the model, b) primes are cofinal, but prime pairs are not, c) primes are not cofinal. We also present a connection between cofinality of prime pairs and definability of elements of the model and further results about related theories concerning decidability, quantifier elimination or existence of prime models.

Fermat's last theorem and Catalan's conjecture in arithmetics with weak exponentiation

Petr Glivický
University of Economics, Prague, Czech Republic
petrglivicky@gmail.com

Wiles's proof of Fermat's Last Theorem (FLT) has stimulated a lively discussion on how much is actually needed for the proof. Despite the fact that the original proof uses set-theoretical assumptions unprovable in Zermelo-Fraenkel set theory with axiom of choice (ZFC) - namely, the existence of Grothendieck universes - it is widely believed that "certainly much less than ZFC is used in principle, probably nothing beyond Peano arithmetic, and perhaps much less than that." (McLarty)

In this talk, I will present a joint work with V. Kala. We studied (un)provabiliy of FLT and Catalan's conjecture in arithmetical theories with weak exponentiation, i.e. in theories in the language $L = (0, 1, +, \cdot, exp, <)$ where the $(0, 1, +, \cdot, <)$-fragment is usually very strong (often even the complete theory $\mathrm{Th}(\mathbb{N})$ of natural numbers in that language) but the exponentiation satisfies only basic arithmetical properties and not much of induction. In such theories, Diophantine problems such as FLT or Catalan's conjecture, are formalized using the exponentiation exp instead of the exponentiation definable in the $(0, 1, +, \cdot, <)$-fragment.

I will present a natural basic set of axioms Exp for exponentiation (consisting mostly of elementary identities) and show that the theory $T = \mathrm{Th}(\mathbb{N}) + Exp$ is strong enough to prove Catalan's conjecture, while FLT is still unprovable in T. This gives an interesting separation of strengths of the two famous Diophantine problems. Nevertheless, I show that by adding just one more axiom for exponentiation (the, so called, "coprimality" of exp) the theory becomes strong enough to prove FLT, i.e. FLT is provable in T+"coprimality". (Of course, in the proof of this, we use the Wiles's result too.)

References

P. Glivický and V. Kala, *Fermat's last theorem and Catalan's conjecture in weak exponential arithmetics*, Mathematical Logic Quarterly **63** (2017), no. 3-4, pp. 162-174, arXiv:1602.03580.

Π^0_1-computable quotient presentation of a nonstandard model of arithmetic

Michał Tomasz Godziszewski
University of Varsaw, Poland
mtgodziszewski@gmail.com
https://uw.academia.edu/MichalGodziszewski

Introduction

A *computable quotient presentation* of a mathematical structure $\mathcal{A}$ consists of a computable structure on the natural numbers $\langle \mathbb{N}, \star, *, ... \rangle$ meaning that the operations and relations of the structure are computable, and an equivalence relation E on $\mathbb{N}$, not necessarily computable but which is a congruence with respect to this structure, such that the quotient $\langle \mathbb{N}, \star, *, ... \rangle / E$ is isomorphic to the given structure $\mathcal{A}$. Thus, one may consider computable quotient presentations of graphs, groups, orders, rings and so on, for any kind of mathematical structure. In a language with relations, it is also natural to relax the concept somewhat by considering the *computably* enumerable quotient presentations, which allow the pre-quotient relations to be merely computably enumerable, rather than insisting that they must be computable.

At the 2016 conference Mathematical Logic and its Applications at the Research Institute for Mathematical Sciences (RIMS) in Kyoto, Bakhadyr Khoussainov outlined a sweeping vision for the use of computable quotient presentations as a fruitful alternative approach to the subject of computable model theory. In his talk, he outlined a program of guiding questions and results in this emerging area. Part of this program concerns the investigation, for a fixed equivalence relation E or type of equivalence relation, which kind of computable quotient presentations are possible with respect to quotients modulo E.

Khoussainov had made two specific conjectures in Kyoto:

Conjecture (Khoussainov).

1. No nonstandard model of arithmetic admits a computable quotient presentation by a computably enumerable equivalence relation on the natural numbers.
2. Some nonstandard model of arithmetic admits a computable quotient presentation by a co-c.e. equivalence relation.

I will report on the proof of first conjecture and present in details:

1. refutations of several natural variations of the second conjecture - obtained in a joint work with J. D. Hamkins,
2. proof of the central case of the second conjecture - obtained in a joint work with T. Slaman and L. Harrington.

In addition, I consider and settle the natural analogues of the conjectures for models of set theory.

Observation 1. *Every consistent c.e. theory T in a functional language admits a computable quotient presentation by an equivalence relation E of low Turing degree.*

The observation is closely connected with a fundamental fact of universal algebra, namely, the fact that every algebraic structure is a quotient of the term algebra on a sufficient number of generators. Every countable group, for example, is a quotient of the free group on countably many generators, and more generally, every countable algebra (a structure in a language with no relations) arises as the quotient of the term algebra on a countable number of generators. Since the term algebra of a computable language is a com- putable structure, it follows that every countable algebra in a computable language admits a computable quotient presentation.
One of the guiding ideas of the theory of computable quotients is to take from this observation the perspective that the complexity of an algebraic structure is contained not in its atomic diagram, often studied in computable model theory, but rather solely in its equality relation. The algebraic structure on the term algebra, after all, is computable; what is difficult is knowing when two terms represent the same object. Thus, the program is to inves- tigate which equivalence relations E or classes of equivalence relations can give rise to a domain $\mathbb{N}/E$ for a given type of mathematical structure. There are many open questions and the theory is just emerging.

The following results confirms that Khoussainov's first conjecture is true.

Theorem 2. *No nonstandard model of arithmetic has a computable quotient presentation by a c.e. equivalence relation. Indeed, this is true even in the restricted (but fully expressive) language $\{+,.\}$ with only addition and multiplication: there is no computable structure $\langle \mathbb{N}, \oplus, \odot \rangle$ and a c.e. equivalence relation E, which is a congruence with respect to this structure, such that the quotient $\langle \mathbb{N}, \oplus, \odot \rangle / E$ is a nonstandard model of arithmetic.*

Theorem 3. *There is no computable structure $\langle \mathbb{N}, \oplus, \odot \rangle$ and a co-c.e. equivalence relation E, which is a congruence with respect to this structure, such that the quotient $\langle \mathbb{N}, \oplus, \odot \rangle / E$ is a nonstandard model of true arithmetic.*

Theorem 4. *There is no computable structure $\langle \mathbb{N}, \oplus, \odot \rangle$ and a co-c.e. equivalence relation E, which is a congruence with respect to this structure, such that the quotient $\langle \mathbb{N}, \oplus, \odot \rangle / E$ is a Σ_1-sound nonstandard model of arithmetic, or even merely a nonstandard model of arithmetic with $0'$ in the standard system of the model.*

Corollary 5 *No nonstandard model of arithmetic in the language $\{+,.,0,1,<\}$ and with $0'$ in its standard system has a computably enumerable quotient presentation by any equivalence relation, of any complexity.*

Note that containing $0'$ in the standard system is a strictly weaker property than being Σ_1-sound, since a simple compactness argument allows us to insert any particular set into the standard system of an elementary extension of any particular model of arithmetic.

Main result

The results above have not settled what might be considered the central case of the second conjecture:

Question 6. *Is there a nonstandard model of PA in the usual language of arithmetic $\{+,.,0,1,<\}$ that has a computably enumerable quotient presentation by some co-c.e. equivalence relation? Equivalently, is there a nonstandard model of PA in that language with a computably enumerable quotient presentation by any equivalence relation, of any complexity?*

The answer is given by the following:

Theorem 7. *There exists a nonstandard model $M \models PA$ s.t.*

$$M \cong \langle \mathbb{N}, \oplus, \otimes, S, 0, 1 \rangle / E,$$

where $\langle \mathbb{N}, \oplus, \otimes, S, 0, 1 \rangle$ is computable and E is co-c.e., i.e. Π^0_1

The idea of the proof consists in extending the language $\mathcal{L}_{PA}$ to $\mathcal{L}^+ = LPA + \{c_i : i \in \omega\}$, letting $T^+ = PA + \neg Con_{PA}$ and simulating the Henkin construction via finite injury priority argument, doing two things:

1. building a Henkin tree,
2. enumerating inequalities, which will give us a c.e. complement of E, making E co-c.e.

Doing it carefully, and using Hilbert's Basis Theorem we obtain the following lemmas:

Lemma 8 (Injury Lemma). *For every l (level of the tree) there is a stage s such that for all $t \geq s$ the Boolean value of φ_l does not change at stage t and the Henkin witness assigned to φ_l does not change.*

Lemma 9 (Completeness Lemma). *Let*

$$\Gamma = PA + \neg Con_{PA} + \{\varphi_i : \varphi_i \text{is stabilized with Boolean value 1}\}$$

Γ is a complete, consistent theory and $\Gamma = Th(\langle \mathbb{N}, \oplus, \otimes, S, 0, 1 \rangle / E)$ for some computable $\langle \mathbb{N}, \oplus, \otimes, S, 0, 1 \rangle$ and a Π^0_1 equivalence E.

LOGIC in computer science, computer engineering and mathematics

Yuri Gurevich
University of Michigan, Ann Arbor, MI, USA
gurevich@umich.edu

In software industry, engineers do formal logic day in and day out, even though they may not and usually do not realize that. As a rule, they have not studied logic. Instead, they studed calculus which they use rarely, if ever.

We illustrate why logic is so relevant to computer science and to computer industry and why it is so hard for software engineers to pick it up.

At the end we discuss the uses of formal logic in mathematics and the prospects of logic in mathematics departments.

Bounded finite set theory

Laurence Kirby
Baruch College, City University of New York, USA
Laurence.Kirby@baruch.cuny.edu

We define a theory of bounded induction on sets, $I\Delta_0 S$, which is analogous to $I\Delta_0$ in arithmetic. We establish some independence results for basic set-theoretic axioms over this theory, and consider the question: given a model M of $I\Delta_0$, is there a model of $I\Delta_0 S$ whose ordinals are isomorphic to M?

How useful are pure compositional axioms for the truth predicate?

Mateusz Łełyk
University of Warsaw, Poland
mlelyk@student.uw.edu.pl

The next natural question to ask when establishing the conservativity of a theory Th_1 over its subtheory Th_2, is whether the former allows easier proofs of theorems of the latter. In order to formally grasp when one proof is easier then another, we measure the number of symbols used when writing them. The shorter the proof, the better. Next definition clarifies this intuition:

Definition *Let Th_1 and Th_2 be two theories and Φ a set of functions $\mathbb{N} \to \mathbb{N}$. We shall say that Th_2 has a* speed-up over *Th_1 with respect to Φ (or* super Φ speed-up*) if there exists an infinite sequence of formulae $\phi_0, \phi_1, \ldots$, provable in both Th_1 and Th_2 such that for every function $f \in \Phi$ there exists $k \in \mathbb{N}$ such that for every $n \geq k$ we have*

$$\| \phi_n \|_{\mathrm{Th}_1} > f(\| \phi_n \|_{\mathrm{Th}_2}),$$

where $\| \phi_n \|_{\mathrm{Th}}$ denotes the length of the shortest proof of ϕ in Th.

One can show e.g. that ACA_0 has a super-elementary speed-up over PA, while being very conservative over it (not only proof-theoretically, but also model-theoretically). The same is the case with the pair GB and ZFC. These results together with the above definition were given in [5]. In general, if a theory admits a super-polynomial speed-up over its subtheory Th, we can treat it as a useful extension of Th.

In the talk we discuss the situation with the theory of basic compositional truth for the language of arithmetic, known as CT^-[a]. This theory is formulated with the use of a fresh unary predicate T and extends PA with finitely many axioms being the natural arithmetization of Tarski's inductive definition of truth (in the extended language but only for the language of arithmetic). CT^- is well-known to be conservative over PA and three essentially different proofs demonstrating this can be found in [3] (KKL Theorem), [4] and [1].

In our presentation we sketch the proof that CT^- does not have a superpolynomial speed-up over PA. The proof idea has been given by Ali Enayat and it consists in a neat arithmetization of the model-theoretic conservativity proof of CT^- over PA, given in [1]. More concretely, it can be shown that there exists a feasible interpretation of CT^- in PA, i.e. one in which the translation of every axiom is provable in PA with a proof of length polynomial in the length of the axiom.

[a] Called also $\mathrm{CT}_\uparrow$ in [2] and CT[PA] in [4]

References

[1] Enayat A., Visser A. (2015), *New Construction of Satisfaction Classes*, [In:] Achourioti T., Galinon H., Martínez Fernández J., and Fujimoto K. (eds), Unifying the Philosophy of Truth, Springer-Verlag.

[2] Halbach V. (2014), *Axiomatic Truth Theories*, Cambridge University Press.

[3] Kaye R. (1991), *Models of Peano Arithmetic*, Oxford University Press, New York.

[4] Leigh G. (2015), *Conservativity of Theories of Compositional Truth via Cut Elimination*, Journal of Symbolic Logic, 80(3), pp. 845-865.

[5] Pudlak P. (1998), *The lenghts of proofs*, in: *Handbook of Proof Theory*, S.R. Buss ed., Elsevier, pp. 547-637.

[6] Pudlak P. (1986), *On the length of proofs of finitistic consistency statements in first order theories*, in: *Logic Colloquium 84*, J.B. Paris, A.J. Wilkie. and G.M.Wiliners, Elsevier, pp. 167-196.

[7] Hájek P., Pudlák P. (1998), *Metamathematics of First Order Arithmetic*, Springer-Verlag.

Weak set theories and Δ_0-collection

Fedor Pakhomov [a]
Steklov Mathematical Institute of Russian Academy of Sciences,
Moscow, Russia
pakhfn@mi.ras.ru

Abstract

We study weak Π_2-axiomatizable set theories. We give two criteria of whether a given theory T could be Π_2-conservatively extended by Δ_0-Collection axiom. We also develop class existence principle that is an analogue of Weak König's Lemma in our setting. We prove that any T that could be Π_2-conservatively extended by Δ_0-Collection axiom also could be Π_2-conservatively extended by our analogue of Weak König's Lemma. Our conservation results are quite general and could be applied to easily achieve several already known conservation results for both first and second order arithmetic. In particular $\mathsf{EA} \equiv_{\Pi_2} \mathsf{EA} + \mathsf{B}\Sigma_1 \equiv_{\Pi_2} \mathsf{WKL}_0^\star$ and $\mathsf{ACA}_0 \equiv_{\Pi^1_2} \Sigma^1_1\text{-}\mathsf{AC}_0 \equiv_{\Pi^1_2} \Sigma^1_1\text{-}\mathsf{AC}_0 +$ "there is a non-principal ultrafilter".

[a] This work is supported by the Russian Science Foundation under grant 16-11-10252

Conservativity of collection for systems of first order arithmetic is a well-known phenomenon. J. Paris [10] and H. Friedman showed that theories $\mathsf{B}\Sigma_{n+1}$ are Π_{n+2} conservative over $\mathsf{I}\Sigma_n$. Latter Beklemishev have [4] generalized this result and showed that a Π_{n+2}-axiomatizable theory could be Π_{n+2} conservatively extended by axiom $\mathsf{B}\Sigma_{n+1}$ iff it is closed under Σ_{n+1}-Collection Rule.

The study of conservation results for axioms of choice in systems of second-order arithmetic were initiated by Friedman [5]. The system $\Sigma^1_1\text{-}\mathsf{AC}_0$ is known to be Π^1_2-conservative extension of ACA_0, the system $\Sigma^1_2\text{-}\mathsf{AC}_0$ is known to be Π^1_3-conservative extension of $\Pi^1_1\text{-}\mathsf{CA}_0$ and further $\Sigma^1_{k+3}\text{-}\mathsf{AC}_0$ is known to be Π^1_4-conservative extension of $\Pi^1_{k+2}\text{-}\mathsf{CA}_0$ (see [12, Section IX.4])

Kripke Platek set theory with urelements KPU in its current form were introduced by J. Barwise in his book [3]. The theory KPU is known to be quite strong from proof-theoretic point of view. Namely, base KPU have the same proof-theoretic power as Peano arithmetic PA and the proof-theoretic strength of KPU with the axiom of Infinity exceeds the proof-theoretic strength of predicative theories [8]. This strength is the result of interplay of the schemes of Δ_0-Collection and Foundation.

The versions of Kripke-Platek without Foundation were studied by G. Jäger [7, 8]. The conservation results of this paper could be regarded as extention and generalization of conservativity of a version of Kripke Platek over PA [8]. K. Sato [11] studied set theories with restrictions on Foundation, Extensionality, and Δ_0-Separation. We note that Sato's setting is somewhat different from our's. In particular, we consider only theories with full Δ_0-Separation and allow urelements. And his main focus were on revers mathematical kind of results rather than conservation results. Nevertheless like in Sato's work we develop uniform set theoretical context to incoroprate bresults for first-order and second-order arithmetic.

We follow standard conventions with regard to set theories with urelements, see [3] (note that we use $x, y, z, \dots$ for arbitrary objects, $a, b, c, \dots$ for sets, and $p, q, \dots$ for urelements). The axioms of our base theory ES are

1. $\exists a\, (x \in a \wedge y \in a)$ (Pair);
2. $\exists b\, \forall c \in a\, \forall x \in c\, x \in b$ (Union);
3. $\exists b\, (\forall x \in b\, (x \in a) \wedge \forall x \in a\, (\varphi(x) \leftrightarrow x \in b))$, for all Δ_0 formulas without free occurrences of b (Δ_0-Sep).

The scheme of Δ_0-Coll is

$$\forall x \in a\, \exists y\, \varphi(x, y) \to \exists b\, \forall x \in a\, \exists y \in b\, \varphi(x, y),$$

for all $\Delta_0[\Omega]$ formulas without free occurrences of b The theory KPU^- is $\mathsf{ES} + \Delta_0$-Coll.

We also consider larger signatures $\Omega \supseteq \Omega_0 = \{=, \in, \mathsf{Ur}\}$ and relativized theories $\mathsf{ES}[\Omega]$, $\mathsf{KPU}^-[\Omega]$, where we extend all schemes to relativized classes. Note that if Ω contains functional symbols then bounded quantifiers in $\Delta_0[\Omega]$ formulas are term-bounded.

The $\Delta_0[\Omega]$ collection rule ($\Delta_0[\Omega]$-CollR):

$$\frac{\forall x\ \exists y\ \varphi(x,y)}{\forall a\ \exists b\ \forall x \in a\ \exists y \in b\ \varphi(x,y)},$$

where $\varphi(x,y)$ is $\Delta_0[\Omega]$ formula without free variables other than x and y.

We say that a term $t'(y_1,\dots,y_n)$ is a collecting term for a term $t(x_1,\dots,x_n)$ in theory T if

$$\mathsf{T} \vdash x_1 \in y_1 \wedge \dots \wedge x_n \in y_n \to t(x_1,\dots,x_n) \in t'(y_1,\dots,y_n).$$

We say that a theory $\mathsf{T} \supseteq \mathsf{ES}[\Omega]$ of signature Ω have *witnessed collection property* if

1. T is $\Pi_1[\Omega]$ axiomatizable;
2. for each functional symbol of Ω there is a collecting term;
3. there are T-terms $\emptyset$, $\cup(x)$, and $\{x,y\}$ without other free variables such that T proves natural properties for them.

Theorem 1. *For any theory $\mathsf{T} \supseteq \mathsf{ES}[\Omega]$ axiomatizable by $\Pi_2[\Omega]$-sentences the following conditions are equivalent:*

1. *the theory $\mathsf{T} + \mathsf{KPU}^-[\Omega]$ is $\Pi_2[\Omega]$-conservative over T;*
2. *the theory T is closed under $\mathbf{\Delta_0[\Omega]}$-$\mathsf{CollR}$;*
3. *there is a conservative extension $\mathsf{U} \supseteq \mathsf{T}$ with witnessed collection property.*

We note that somewhat similar approach of extending base language of set theory by witnessing function were used by J. Avigad in his approach to ordinal analysis of $\mathsf{KP}\omega$ [2]

We also investigate class theories over our set theories. The axiom scheme $\Delta^0_1[\Omega]$-CA is

$$\forall x\ (\varphi_\Pi(x) \leftrightarrow \varphi_\Sigma(x)) \to \exists X\ \forall x\ (x \in X \leftrightarrow \varphi_\Pi(x)),$$

where φ_Π and φ_Σ are $\Pi^0_1[\Omega]$ and $\Sigma^0_1[\Omega]$, respectively (they may contain additional free variables).

We introduce the axiom CCP of Class Compactness Principle. It states[a] that if there is a class of pairs C such that

1. for each $\langle a,b\rangle \in C$ we have $b \subseteq a$;
2. for each a some pair $\langle a,b\rangle$ is in C;
3. for each $a' \subseteq a$ and $\langle a,b\rangle \in C$ the pair $\langle a', b \cap a'\rangle \in C$;

then there is a class P such that $\forall a \exists b (a \cap P = b \wedge \langle a,b\rangle \in C)$. We note that CCP could be regarded as a generalization of Weak König's Lemma.

Theorem 2. *Suppose $\mathsf{T} \supseteq \mathsf{ES}[\Omega]$ is $\Pi_2[\Omega]$-axiomatizable theory for which any(all) items of Theorem 1. hold. Then T is $\Pi_2[\Omega]$ conservative over $T + \Delta^0_0[\Omega]$-$\mathsf{Coll} + \Delta^0_1[\Omega]$-$\mathsf{CA} + \mathsf{CCP}$.*

Finally we demonstrate how we apply our result about set theories to theories in other signatures. Let us outline the reduction of a conservation result for ACA_0 (essentially it is A. Keruzer's result [9]) to our general Theorem 2.

Theorem 3. ACA_0 *is Π^1_2 conservative over third-order theory*

$$\Sigma^1_1\text{-}\mathsf{AC}_0 + \text{"there exists a non-principal ultrafilter"}.$$

Proof. We consider signature Ω_{ar} that is the extension of Ω_0 by relational signature of arithmetic. Theory $\mathsf{ES}^{\mathrm{ar}}$ is $\mathsf{ES}[\Omega_{\mathrm{ar}}]$ plus axioms of Q for urelements, plus axiom of set-induction over naturals, plus existence of the set of all naturals. We naturally extend $\mathsf{ES}^{\mathrm{ar}}$ by new functions to obtain $\mathsf{ESW}^{\mathrm{ar}}$ with witnessed collection property that is conservative over $\mathsf{ES}^{\mathrm{ar}} + \Delta_0[\Omega_{\mathrm{ar}}]$-$\mathsf{CollR}$ (see [**?**]). By restricting consideration of sets to subsets of $\mathbb{N}$, the language of second-order arithmetic could be regarded as a sublanguage of $\mathsf{ESW}^{\mathrm{ar}}$. Thus we regard ACA_0 as a subsystem of $\mathsf{ESW}^{\mathrm{ar}}$. On the other hand ACA_0 naturally interprets $\mathsf{ESW}^{\mathrm{ar}}$, most importantly the interpretation of $\in$ is

$$X \in^I Y \overset{\mathrm{def}}{\iff} \exists n \forall m\ (\langle n,m\rangle \in Y \leftrightarrow n \in X).$$

Thus $\mathsf{ESW}^{\mathrm{ar}}$ is a conservative extension of ACA_0. Hence the theory $\mathsf{T} = \mathsf{ESW}^{\mathrm{ar}} + \Delta^0_0[\Omega_{\mathrm{ar}}]$-$\mathsf{Coll} + \Delta^0_1[\Omega_{\mathrm{ar}}]$-$\mathsf{CA} + \mathsf{CCP}$ is Π^1_2 conservative extension of ACA_0. Now we just build an appropriate interpretation of the third-order theory Σ^1_1-AC_0 + "there exists a non-principal ultrafilter" in T. □

[a] note that in the sake of simplicity we give formulation in the case of presence of Extensionality

References

[1] Toshiyasu Arai, *Axiomatizing some small classes of set functions*, arXiv:1503.07982, 2015

[2] Jeremy Avigad, *An ordinal analysis of admissible set theory using recursion on ordinal notations*. Journal of Mathematical Logic, 2(2001), 91 – 112, 2002.

[3] Jon Barwise, *Admissible Sets and Structures: An Approach to Definability Theory*. 1975.

[4] Lev Beklemishev, *A proof-theoretic analysis of collection*. Archive for Mathematical Logic, 37(5-6):275–296, 1998.

[5] Harvey Friedman, *Iterated Inductive Defintions and* Σ^1_2*-ac*. In Studies in Logic and the Foundations of Mathematics, volume 60, pages 435–442. Elsevier, 1970.

[6] Gerhard Jäger, *Zur Beweistheorie der Kripke-Platek-Mengenlehre über den natürlichen Zahlen*. Archiv für mathematische Logik und Grundlagenforschung, 22(3–4):121–139, 1980.

[7] Gerhard Jäger, *The strength of admissibility without foundation*. The Journal of Symbolic Logic, 49(3) pp. 867–879, 1984.

[8] Gerhard Jäger, *A version of Kripke-Platek set theory which is conservative over Peano arithmetic*. Mathematical Logic Quarterly, 30(1-6):3–9, 1984.

[9] Alexander Kreuzer, *Non-principal ultrafilters, program extraction and higher-order reverse mathematics*. Journal of Mathematical Logic, 12(01), 2012.

[10] Jeff Paris, *A hierarchy of cuts in models of arithmetic*. In *Model theory of algebra and arithmetic*, pages 312–337. Springer, 1980.

[11] Kentaro Sato, *The strength of extensionality* Π*-weak weak set theories without infinity*. Annals of Pure and Applied Logic, 162(8):579–646, 2011.

[12] Stephen Simpson, *Subsystems of second order arithmetic*, volume 1. Cambridge University Press, 2009.

Recognisable sets, profinite topologies and weak arithmetic

Jean-Éric Pin [a]
IRIF, CNRS and Université Paris-Diderot, France.
Jean-Eric.Pin@irif.fr

If A is a one-letter alphabet, the free monoid A^* is isomorphic to the additive monoid $\mathbb{N}$. One can therefore expect that any result on A^* trivializes for a one-letter alphabet. But surprisingly enough, this is not always the case. The aim of this survey is to present such cases, which lead to unexpected results on weak arithmetic.

1 Definitions

1.1 Recognisable subsets

Let M be a monoid. A subset P of a monoid M is *recognisable* if there exist a *finite monoid* F, a monoid morphism $\varphi : M \to F$ and a subset Q of F such that $P = \varphi^{-1}(Q)$. According to Kleene theorem, a subset of A^* is recognisable if and only if it is regular.

1.2 Regular languages

A *lattice of languages* is a set $\mathcal{L}$ of regular languages of A^* containing $\emptyset$ and A^* and closed under finite union and finite intersection. It is *closed under quotients* if, for each $L \in \mathcal{L}$ and $u \in A^*$, the languages $u^{-1}L$ and Lu^{-1} are also in $\mathcal{L}$.
A *renaming* or *length-preserving morphism* is a morphism φ from A^* into B^*, such that, for each word u, the words u and $\varphi(u)$ have the same length. It is equivalent to require that, for each letter a, $\varphi(a)$ is also a letter, that is, $\varphi(A) \subseteq B$. Similarly, a morphism is *length-decreasing* if the image of each letter is either a letter or the empty word.

[a]The author is partially funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 670624) and by the DeLTA project (ANR-16-CE40-0007)

A *class of languages* is a correspondence $\mathcal{C}$ which associates with each alphabet A a set $\mathcal{C}(A^*)$ of regular languages of A^*. A *positive variety of languages* is a class of regular languages $\mathcal{V}$ such that (a) for every alphabet A, $\mathcal{V}(A^*)$ is a lattice of languages closed under quotients and (b) if $\varphi : A^* \to B^*$ is a morphism, $L \in \mathcal{V}(B^*)$ implies $\varphi^{-1}(L) \in \mathcal{V}(A^*)$. If Condition (b) is only satisfied by length-decreasing [length-preserving] morphisms, the class $\mathcal{V}$ is a *positive ld-variety* [*lp-variety*] *of languages*.
A *variety of languages* is a positive variety $\mathcal{V}$ such that each lattice $\mathcal{V}(A^*)$ is closed under complement. The following result is proved in [1].

Theorem 4. *Every commutative positive ld-variety of languages is a positive variety of languages.*

Setting, for each subset L of $\mathbb{N}$ and each positive integer k,

$$L - 1 = \{n \in \mathbb{N} \mid n + 1 \in L\}$$
$$L \div k = \{n \in \mathbb{N} \mid kn \in L\}$$

one gets the following corollary [4].

Corollary 1. *Let $\mathcal{L}$ be a lattice of regular subsets of $\mathbb{N}$ such that if $L \in \mathcal{L}$, then $L - 1 \in \mathcal{L}$. Then for each positive integer k, $L \in \mathcal{L}$ implies $L \div k \in \mathcal{L}$.*

1.3 Profinite metrics

A monoid F *separates* two elements $x, y \in M$ if there exists a morphism $\varphi : M \to F$ such that $\varphi(x) \neq \varphi(y)$.
A monoid is *residually finite* if any pair of distinct elements of M can be separated by a finite monoid. Finite monoids, free monoids, free groups and products of residually finite monoids are residually finite.
Let M be a residually finite monoid. The *profinite metric* d on M is defined by setting, for $u, v \in M$:

$$r(u, v) = \min\{|F| \mid F \text{ separates } u \text{ and } v\}$$
$$d(u, v) = 2^{-r(u,v)}$$

with the conventions $\min \emptyset = +\infty$ and $2^{-\infty} = 0$. One can show that d is not only a metric, but an ultrametric, that is, satisfies the stronger inequality $d(u, w) \leqslant \max(d(u, v), d(v, w))$.

1.4 p-group languages

A profinite metric can be actually attached to any Boolean algebra of regular subsets of M. An interesting case occurs when the Boolean algebra is the set of p-group languages of a free monoid.
Let p be a prime number. A *p-group* is a group whose order is a power of p. A *p-group language* is a language whose syntactic monoid is a p-group. Let $\mathcal{G}_p$ be the Boolean algebra of p-group languages.
A word $u = a_1 a_2 \cdots a_n$ (where $a_1, \ldots, a_n$ are letters) is a *subword* of a word v if v can be factored as $v = v_0 a_1 v_1 \cdots a_n v_n$. For instance, *ab* is a subword of *cacbc*. Given two words u and v, we denote by $\binom{v}{u}$ the number of distinct ways to write u as a subword of v. More formally, if $u = a_1 a_2 \cdots a_n$, then

$$\binom{v}{u} = \text{Card}\{(v_0, v_1, \ldots, v_n) \mid v_0 a_1 v_1 \cdots a_n v_n = v\}$$

Eilenberg and Schützenberger [7] have proved that a language of A^* is a p-group language if and only if it is a Boolean combination of languages of the form

$$L(x, r, p) = \{u \in A^* \mid \binom{u}{x} \equiv r \bmod p\}, \tag{1}$$

where $0 \leqslant r < p$ and $x \in A^*$.

2 Regularity-preserving functions

A function $f : A^* \to B^*$ is *regularity-preserving* if, for each regular language L of B^*, $f^{-1}(L)$ is also *regular*. More generally, if $\mathcal{C}$ is a class of *regular languages*, f is said to be *$\mathcal{C}$-preserving* if, for each $L \in \mathcal{C}$, $f^{-1}(L)$ is also in $\mathcal{C}$. A long term objective is the following:

> *Find a complete description of regularity-preserving (respectively $\mathcal{C}$-preserving) functions.*

The problem can be extended to functions between arbitrary monoid as follows. Let M and N be monoids. A function $f : M \to N$ is *recognisability-preserving* if, for each recognisable language L of B^*, $f^{-1}(L)$ is also *recognisable*. The following result [10] gives a topological characterization of these functions.

Theorem 5. *Let M and N be two finitely generated, residually finite monoids. A function $M \to N$ is recognisability-preserving if and only if it is uniformly continuous for the profinite metrics.*

Further properties are discussed in [5, 6, 10, 11, 12].

The characterization of $\mathcal{G}_p$-preserving functions is also an interesting problem. For functions from $\mathbb{N}$ to $\mathbb{N}$, the solution boils down to a famous result of Mahler in p-adic analysis [8, 9]. The case of functions from A^* to $\mathbb{N}$ was settled by Silva and the author [12] and the general case (functions from A^* to B^*) was recently solved by Reutenauer and the author.

3 Back to integers

It is well-known that a set S of nonnegative integers is regular if and only if it is a finite union of arithmetic progressions.

Example 1. Let $S = \{1, 3, 4, 9, 11\} \cup \{7 + 5n \mid n \geqslant 0\} \cup \{8 + 5n \mid n \geqslant 0\} = \{1, 3, 4, 7, 8, 9, 11, 12, 13, 17, 18, 22, 23, 27, 28, \ldots\}$. Then S is a finite union of arithmetic progressions.

A function $f : \mathbb{N} \to \mathbb{N}$ is said to be *ultimately periodic modulo n* if the function $n \to f(n) \bmod n$ is ultimately periodic. It is *cyclically ultimately periodic* if it is ultimately periodic modulo n for all $n > 0$. The following result, which has been rediscovered several times, goes back at least to Siefkes [**?**] and to Seiferas-MacNaughton [14].

Proposition 2. *A function $f : \mathbb{N} \to \mathbb{N}$ is ultimately periodic modulo n if and only if for $0 \leqslant k < n$, the set $f^{-1}(k + n\mathbb{N})$ is regular.*

Corollary 3. *A function $f : \mathbb{N} \to \mathbb{N}$ is regularity-preserving if and only if it is cyclically ultimately periodic and, for every $k \in \mathbb{N}$, the set $f^{-1}(k)$ is regular.*

Properties of cyclically ultimately periodic (cup) functions have been studied or used by various authors, see [2, 3, 14, 15, 16]. The notion of a cup function can be extended to functions from $\mathbb{N}^k$ to $\mathbb{N}$. Siefkes [15] has shown that cup functions satisfy a recursion scheme, which can be used to prove the following result:

Theorem 6. *Let $f, g : \mathbb{N} \to \mathbb{N}$ be cyclically ultimately periodic functions. Then so are the following functions:*

1. *$g \circ f$, $f + g$, fg, f^g, and $f - g$ provided that $f \geqslant g$ and $\lim_{n\to\infty}(f - g)(n) = +\infty$,*
2. *(*generalised sum*) $n \to \sum_{0\leqslant i\leqslant g(n)} f(i)$,*
3. *(*generalised product*) $n \to \prod_{0\leqslant i\leqslant g(n)} f(i)$.*

For instance, the functions $n \to 2^n$ and $n \to 2^{2^{2^{\cdot^{\cdot^{\cdot^2}}}}}$ (exponential stack of 2's of height n) are cyclically ultimately periodic. However, the function $n \to \binom{2n}{n}$ is not ultimately periodic modulo 4 since $\binom{2n}{n} \equiv 2 \bmod 4$ if and only if n is a power of 2, and $\binom{2n}{n}$ is divisible by 4 otherwise.
It is an interesting open problem to know whether all primitive recursive cup functions can be generated by using Siefkes' recursive scheme.

References

[1] Almeida, Jorge and Ésik, Zoltán and Pin, Jean-Éric, *Commutative positive varieties of languages*, Acta Cybernetica, 23, 2017, pp. 91–111

[2] Berstel, Jean and Boasson, Luc and Carton, Olivier and Pin, Jean-Éric and Restivo, Antonio, *The expressive power of the shuffle product*, Information and Computation, 208, 2010, pp. 1258–1272

[3] Carton, Olivier and Thomas, Wolfgang, *The Monadic Theory of Morphic Infinite Words and Generalizations*, Inform. Comput., 176, 2002, pp. 51–76

[4] Cégielski, Patrick and Grigorieff, Serge and Guessarian, Irène, *On lattices of regular sets of natural integers closed under decrementation*, Inform. Process. Lett., 114(4), 2014, pp. 197–202

[5] Cégielski, Patrick and Grigorieff, Serge and Guessarian, Irène, *Integral difference ratio functions on integers, in Computing with new resources*, Lecture Notes in Comput. Sci., 8808, 2014, pp. 277–291, Springer, Cham

[6] Cégielski, Patrick and Grigorieff, Serge and Guessarian, Irène, *Newton representation of functions over natural integers having integral difference ratios*, Int. J. Number Theory, 11(7), 2015, pp. 2109–2139

[7] Eilenberg, S., *Automata, Languages and Machines*, Academic Press, New York, 1976, vol. B

[8] Mahler, K., *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math., 199, pp. 23–34, 1958

[9] Mahler, K., *A correction to the paper "An interpolation series for continuous functions of a p-adic variable."*, J. Reine Angew. Math., 208, pp. 70–72, 1961

[10] Pin, Jean-Éric and Silva, Pedro V., *A topological approach to transductions*, TCS, 2005, 340, pp. 443–456

[11] Pin, Jean-Éric and Silva, Pedro V., *On profinite uniform structures defined by varieties of finite monoids*, IJAC, 21, 2011, pp. 295–314

[12] Pin, Jean-Éric and Silva, Pedro V., *A noncommutative extension of Mahler's theorem on interpolation series*, European J. Combin., 36, 2014, pp. 564–578

[13] Pin, Jean-Éric and Silva, Pedro V., *On uniformly continuous functions for some profinite topologies*, Theoret. Comput. Sci., 658, 2017, pp. 246–262

[14] Seiferas, J. I. and McNaughton, R., *Regularity-preserving relations*, Theoret. Comput. Sci., 2 (2), 1976, pp. 147–154

[15] Siefkes, D., *Decidable extensions of monadic second order successor arithmetic*, in *Automatentheorie und formale Sprachen* (Tagung, Math. Forschungsinst., Oberwolfach, 1969), pp. 441–472, Bibliographisches Inst., Mannheim, 1970

[16] Zhang, Guo-Qiang, *Automata, Boolean matrices, and ultimate periodicity*, Inform. and Comput., 152(1), 1999, pp. 138–154

Two Classes of Basic Divisibility Families from NP

Mikhail Starchak
St. Petersburg State University, St. Petersburg, Russia
mikhstark@gmail.com

We will consider time-complexity of two sets defined by a system of linear divisibilities. The study of such sets followed the results of A.P. Bel'tyukov [1] and L. Lipshitz [2] on the decidability of the existential theory of the structure $\langle \mathbb{N}; +, 1, | \rangle$. Some number-theoretical and time-complexity properties of sets, existentially definable in this structure, were studied in [3] and [4].

Recall the definition from [4] of *subdivisibility sets* as projections of a finite union of *basic divisibility sets* of the form

$$\left\{ \overline{x} \in \mathbb{Z}^n : \bigwedge_{i=1}^{m_1} f_i(\overline{x}) \mid g_i(\overline{x}) \wedge \bigwedge_{j=1}^{m_2} h_j(\overline{x}) \geq 0 \right\}, \tag{1}$$

where every f_i, g_i, h_j is linear in $\overline{x}$ over $\mathbb{Z}$. In non-deterministic polynomial time (see [5]) the decision problem for every subdivisibility set is reducible to the problem of deciding sets of the form

$$\left\{ \overline{y} \in \mathbb{Z}^l : \exists \overline{x} \bigvee_{j=1}^{k} \left(\bigwedge_{i=1}^{m} f_{i,j}(\overline{x}, \overline{y}) \mid g_{i,j}(\overline{x}, \overline{y}) \right) \wedge \overline{x} \geq 0 \wedge \overline{y} \geq 0 \right\}, \tag{2}$$

for polynomials $f_{i,j}, g_{i,j}$ linear in $\overline{x}, \overline{y}$ over $\mathbb{Z}$ with non-negative integer coefficients.

When we study decision problem for this theory we have to consider families of divisibility formulas. This leads us to the following definition. Analogously we define *divisibility family* as a finite union of *basic divisibility families*, defined as

$$\left\{ \overline{y} \in \mathbb{N}^l : \exists \overline{x} \bigwedge_{i=1}^{m} f_{i,j}(\overline{x}, \overline{y}) \mid g_{i,j}(\overline{x}, \overline{y}) \wedge \overline{x} \geq 0 \right\}, \tag{3}$$

for quadratic polynomials $f_{i,j}, g_{i,j}$ with non-negative integer coefficients, linear in $\overline{x}$ over $\mathbb{Z}[\overline{y}]$ and in $\overline{y}$ over $\mathbb{Z}[\overline{x}]$.

Every subdivisibility set is obviously a divisibility family but this is not true in the other direction. For example, graph of squaring function is a basic divisibility family and not a subdivisibility set. We will further consider complexity of deciding basic divisibility families. Note that after introducing some bound variables, every such family can be regarded as a set of pairs of matrices (A, B) with non-negative integer entries, where every such pair corresponds to the set of coefficients of linear polynomials in the divisibility system

$$\bigwedge_{i=1}^{m} a_{i,0} + a_{i,1}x_1 + ... + a_{i,n}x_n \mid b_{i,0} + b_{i,1}x_1 + ... + b_{i,n}x_n. \tag{4}$$

This form is more convenient when we study various classes of basic divisibility families as it is easier to formulate restrictions on the elements of some divisibility family. In this case a class is a non-empty set of the decision problems for some basic divisibility families.

In [3] it was shown that the problem of deciding basic divisibility families is NP-hard for every number of divisibilities $m \geq 5$ and is in the class **NP** for every *fixed* number of divisibilities. The general problem is not known to be in **NP**, and the tight upper bound on the length of the minimum satisfying assignment for an arbitrary divisibility system is exponential in the length of the input, as was shown in [5]. This gives **NEXPTIME** upper bound for the problem.

In the following two classes of basic divisibility families we consider one number-theoretical problem from **P** and prove that for some class of basic divisibility families the decision problem for every family from this class is in **NP**. In both these cases the number of divisibilities will be arbitrary.

Let we have a problem of consistency in $\mathbb{N}$ of a system of linear congruences and linear inequalities. This problem defines some basic divisibility family as we can think of a given system of congruences as of a divisibility system (4) with $a_{i,j} = 0$ for $i = 1..m$, $j = 1..n$, introducing some bound variables we can transform given inequalities into a system of divisibilities. Without lost of generality we may assume that $a_{1,0} = ... = a_{m,0} = k$ for some positive integer k. We can denote this problem kLCLI.

Proposition 1. *For every fixed number of the variables n and fixed number of distinct prime factors of k, the problem kLCLI is in the class **P**.*

If we will not fix the number of the variables it is sufficiently to allow only two non-zero coefficients among $b_{i,j}$ for $i = 1..m$, $j = 1..n$ in linear divisibilities and inequalities of the form $\bigwedge_{i=1}^{n} x_i \leq d$ for some $d < k$, to make the problem NP-complete as was shown in [6]. The author doesn't know whether this proposition is true without any restriction on the number of prime factors of k.
The second problem concerns such restrictions on values of non-negative entries of the matrices (A, B) that the decision problem for the corresponding family is in the class **NP**.

Proposition 2. *The problem of deciding basic divisibility families, satisfying the restriction* $(b_{i,j} \neq 0 \Rightarrow a_{i,j} \neq 0)$ *for* $i = 1..m$, $j = 0..n$ *is in the class* ***NP****.*

One corollary from this result is that every divisibility family that comprises only pairs of matrices that have all *positive* integer entries is in **NP**. This restriction was imposed on systems of divisibilities in [7] in the problem denoted simultaneous divisibility of linear polynomials. This problem was marked NP-hard with reference to [3]. In order not to confuse this special case with the general decision problem, we denote the problem SDLP_+. Using NP-hardness result from [6] we conclude that

Corollary 1 from Proposition 2. *The problem* $SDLP_+$ *is NP-complete.*

This subclass is apparently much easier than the decision problem for an arbitrary basic divisibility family.

References

[1] A.P. Bel'tyukov, *Decidability of the universal theory of the natural numbers with addition and divisibility.* Zapiski Nauchnyh Seminarov LOMI, Vol. 60, 1976, pp. 15-28.

[2] L. Lipshitz, *The diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc., Vol. 235, 1978, pp. 271–283.

[3] L. Lipshitz, *Some remarks on the diophantine problem for addition and divisibility*, Bulletin de la Societe mathmatique de Belgique. Srie B, Vol. 33, No. 1, 1981, pp. 41-52.

[4] L. van den Dries, A.J. Wilkie, *The laws of integer divisibility, and solution sets of linear divisibility conditions*, The Journal of Symbolic Logic, Vol. 68, no. 2, 2003, pp. 503–526.

[5] A. Lechner, J. Ouaknine, J. Worrell, *On the complexity of linear arithmetic with divisibility*, Proceedings of 30th Annual IEEE Symposium on Logic in Computer Science, 2015, pp. 667–676.

[6] N.K. Kosovskii, T.M. Kosovskaya, N.N. Kosovskii, M.R. Starchak, *NP-complete problems for systems of divisibilities of values of linear polynomials*, Vestnik SPbSU. Mathematics. Mechanics. Astronomy, Vol. 4 (62), No. 2, 2017, pp. 236–246.

[7] M.R. Garey, D.S. Johnson, *Computers and Intractability: A guide to the theory of NP-completeness*, W. H. Freeman and co., New York , 1979.

Primitive recursion and algorithmically-completeness for Primitive Recursive Class of functions

Patrick Cégielski [a], Serge Grigorieff [b], Julien Cervelle [c] and Pierre Valarcher [d]

One wonders whether certain complexity classes are attainable by some programming languages that implement only the class of recursive primitive functions. For example, we show that the complexity class $O(\log)$ is not accessible in the PRC language : there is no program that compute anything in time $O(\log)$. On the other hand, the class $O(n.\log(n))$ is reachable with the LOOP language.

[a]LACL, Université Paris-Est Créteil, France; patrick.cegielski@u-pec.fr
[b]IRIF, Université Paris Diderot, France; serge.grigorieff@irif.fr
[c]LACL, Université Paris-Est Créteil, France; julien.cervelle@u-pec.fr
[d]LACL, Université Paris-Est Créteil, France; pierre.valarcher.cervelle@u-pec.fr