Russian Academy of Sciences
St. Petersburg Department of V.A. Steklov Institute of Mathematics

Journées sur les Arithmétiques Faibles
JAF 36

In honour of Yuri Matiyasevich on the occasion of his 70th birthday

St.Petersburg, Russia
June 5-7, 2017

Abstracts

St.Petersburg, 2017

The conference is supported by

- the Russian Foundation for Basic Research (RFBR grant 17-01-20189);
- the Government of the Russian Federation (grant 14.Z50.31.0030).

Content

Reflection calculus and conservativity spectra

Lev D. Beklemishev[1]
Steklov Mathematical Institute, Moscow, Russia
bekl@mi.ras.ru

Strictly positive logics recently attracted attention both in the description logic and in the provability logic communities for their combination of efficiency and sufficient expressivity. The language of Reflection Calculus RC consists of implications between formulas built up from propositional variables and constant 'true' using only conjunction and diamond modalities which are interpreted in Peano arithmetic as restricted uniform reflection principles.

We extend the language of RC by another series of modalities representing the operators associating with a given arithmetical theory T its fragment axiomatized by all theorems of T of arithmetical complexity Π^0_n, for all $n > 0$. We note that such operators, in a precise sense, cannot be represented in the full language of modal logic.

We formulate a formal system extending RC that is sound and, as we conjecture, complete under this interpretation. We show that in this system one is able to express iterations of reflection principles up to any ordinal $< \varepsilon_0$. On the other hand, we provide normal forms for its variable-free fragment. Thereby, the variable-free fragment is shown to be algorithmically decidable and complete w.r.t. its natural arithmetical semantics.

The normal forms for the variable-free formulas of RC^∇ are related in a canonical way to the collections of proof-theoretic ordinals of arithmetical theories for each complexity level Π^0_{n+1} that we call *conservativity spectra*. Joost Joosten [2] established a one-to-one correspondence between conservativity spectra (for a certain class of theories) and the points of the universal model for the variable-free fragment of GLP due to Konstantin Ignatiev [1].

The third part of our paper provides an algebraic model $\mathfrak{I}$ for the variable-free fragment of RC^∇. Our main theorem states the isomorphism of several representations of $\mathfrak{I}$: the Lindenbaum–Tarski algebra of the variable-free fragment of RC^∇; a constructive representation in terms of sequences of ordinals below ε_0; a representation in terms of the semilattice of bounded RC-theories and as the algebra of cones of the Ignatiev model.

References

[1] K.N. Ignatiev. On strong provability predicates and the associated modal logics. *The Journal of Symbolic Logic*, 58:249–290, 1993.

[2] J.J. Joosten. Turing–Taylor expansions of arithmetical theories. *Studia Logica*, 104:1225–1243, 2015. doi:10.1007/s11225-016-9674-z.

[1] Research financed by a grant of the Russian Science Foundation (project No. 16-11-10252)

Subrecursive dialectica interpretations for subrecursive realizations

Anatoly Beltiukov
Udmurt State University, Izhevsk, Russia
belt.udsu@mail.ru

In this paper a connection of subrecursive variants of Dialectica Godel interpretation and realizational interpretation of Kleene is considered. The result is that you can call implementation with support and opposition. It is shown that implementations with support can be automatically extracted from intuitionistic proofs. The paper is intended for further use in systems of program synthesis together with error analysis modules.

We consider the following types of constructive interpretation assertions: $p : Q : r$ - Godel's interpretation (dialectica) [1], $a : A$ - Kleene's realization [2].

Formula $p : Q : r$ informally can be read as follows: the object p confirms the statement Q in the face of opposition r. Formula $\grave{a} : A$ means: the object $\grave{a}$ is a realization of the formula A, or: the object a solves the constructive problem in the formula A. The combination of these structures together gives a formula of the form $p : (a : A) : r$. For brevity, we omit the brackets: $p : a : A : r$. This formula can be read as follows: the object a realizes formula A in the face of opposition r with support of the object p". The practical meaning of this statement is that the object a is a solution of the task, written in the form of the formula A, the object r is a condition in which this solution is used, and the object p is used to check correctness of this condition. Then the whole statement $p : a : A : r$ means, that application of opbject a for solution of task A in the condition r with support p passed successfully (there were no errors in the solution with unerring condition).

For atomic formulas, the truth of the statement $p : a : P(c) : q$ is determined by the interpretation, i.e. each predicate P can be considered an algorithm with the property: $P(p, a, c, q) = (p : a : P(c) : q)$. The most interesting case of complex formulas is the realization of the implication:

$$(g, h) : f : (A \Rightarrow B) : (c, a, b) \Leftrightarrow$$
$$(c : a : A : g(c, a, b) \Rightarrow h(c, a) : f(a) : B : b).$$

Here the support consists of two parts: g is a premise check module and h is a conclusion realization support module.

It is proved that for natural deductive systems one can construct such polynomial algorithms $extrp$ and $extra$, that

$$Proof(d, A) \Rightarrow (extrp(d) : extra(d) : A : x)$$

for any opposition x, where $Proof(d, A)$ means, that d is a proof of the formula A.

In the deductive system, various limited induction schemes can be included depending on the complexity class used in the functions of realizations [3].

References

[1] Godel, K. Uber eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes. In Feferman, S., Dawson, Jr., J. W., Kleene, S. C., Moore, G. H., Solovay, R. M., and

van Haijenoort, J., editors, Collected Works, volume II, pages 240–251. Oxford University Press, 1990.

[2] Kleene S.C. *Introduction to metamathematics*, North-Holland, 1951, 500 p.

[3] Beltiukov A.P. Intuitionistic formal theories with realizability in subrecursive classes, *Annals of Pure and Applied Logic*, 1997, vol. 89, p. 3–15.

A note on counting quantifiers

Christian Choffrut
IRIF, University of Paris 7, France
choffrut@irif.fr

A *unary counting quantifier* is a construct of the form $\exists_x^{=y}$ and serves as a prefix of a first order formula of the Presburger arithmetics, i.e., the arithmetics of the integers $\mathbb{Z}$ without the multiplication, denoted FO(+). A formula $\exists_{x_n}^{=y}\phi(x_1, x_2, \ldots, x_n)$ is true under the interpretation $a_1, a_2, \ldots, a_{n-1}$ for $x_1, x_2, \ldots, x_{n-1}$ and b for y if and only if the number of integer values a satisfying $\phi(a_1, a_2, \ldots, a_{n-1}, a)$ equals b. For example the formula $\exists_x^{=y}(-1 \leq x \leq 3)$ interprets to true if and only if $y = 5$. The logic $FO(+)$ extends to $FOC(+)$ (c for *counting*) by allowing, along with the ordinary quantifiers, these counting quantifiers. It seems that the term appeared for the first time in [2]. However, the notion was known well before. Apelt[1] proved in 1966 that this logic does not have a greater expressive power expressiveness than $FO(+)$, [1, p. 156]. It was rediscovered by Nicole Schweikardt in [6]. It can be stated as follows.

Theorem 1. *Given a Presburger formula $\phi(x_1, \ldots, x_n)$ with free variables $x_1, \ldots, x_n$, there exists a Presburger formula $\psi(x_1, x_2, \ldots, x_{n-1}, y)$ equivalent to the formula $\exists_{x_n}^{=y}\phi(x_1, \ldots, x_n)$*

The purpose of this short note is to show that the use of Ginsburg' and Spanier's characterization of Presburger definable subsets along with the more precise version of Eilenberg and Schützenberger allows us to eliminate some technicalities of the original proofs. It thus claims no novelty and is a mere effort to reduce ad hoc demonstrations as much as possible.

1 Semilinear sets

We refer to [3] for a full exposition of the theory of rational subsets of $\mathbb{N}^n$ and $\mathbb{Z}^n$. In order to keep our work self-contained, we content ourselves with recalling the properties needed for our purpose only.

It is convenient to view the elements of $\mathbb{Z}^n$ or $\mathbb{N}^n$ as vectors and to write them in boldface and scalars in lightface. The operation of addition extends to subsets: if $X, Y \subseteq \mathbb{Z}^n$, then the *sum* $X + Y \subseteq \mathbb{Z}^n$ is the set of all sums $\mathbf{x} + \mathbf{y}$ where $\mathbf{x} \in X$ and $\mathbf{y} \in Y$. When X is a singleton $\{\mathbf{x}\}$ we simply write $\mathbf{x} + Y$. Given $\mathbf{x}$ in $\mathbb{Z}^n$, the expression $\mathbb{N}\mathbf{x}$ represents the subset of all vectors $n\mathbf{x}$ where n ranges over $\mathbb{N}$ and similarly for $\mathbb{Z}\mathbf{x}$. For example, $\mathbb{Z}\mathbf{x} + \mathbb{Z}\mathbf{y}$ represents the subgroup generated by the vectors $\mathbf{x}$ and $\mathbf{y}$.

We need a preliminary definition.

[1] Apelt refers to Härtig for the original definition which is equivalent, yet different from that given here.

Definition 1. A subset of $\mathbb{Z}^n$ (resp. $\mathbb{N}^n$) is *linear* if it is of the form

$$\mathbb{N}\mathbf{b_1} + \cdots + \mathbb{N}\mathbf{b_p} \tag{1}$$

for some n-vectors $\mathbf{a}, \mathbf{b_1}, \ldots, \mathbf{b_p}$ in $\mathbb{Z}^n$ (resp.in $\mathbb{N}^n$). It is *simple* if furthermore, the vectors $\mathbf{b_1}, \ldots, \mathbf{b_p}$ are linearly independent when considered as embedded in $\mathbb{Q}^n$. It is *semilinear* if it is a finite union of linear (resp. simple) sets.

The main result on semilinear sets is summarized in the Theorem below. Ginsburg and Spanier proved the equivalence of the first two statements for $\mathbb{N}^n$, [4], but it can readily be seen to hold for $\mathbb{Z}^n$. Eilenberg and Schützenberger, [3] proved the equivalence of the first two statements in the general case of commutative monoids and established furthermore their equivalence with the last statement for $\mathbb{Z}$ and $\mathbb{N}$, a result which was explicitly left open by Ginsburg and Spanier and which was independently obtained by Ito [5].

We denote $\mathcal{Z}$ and $\mathcal{N}$ respectively, the first order structure $\langle \mathbb{Z}; +, 0, 1, < \rangle$ and $\langle \mathbb{N}; +, 0, 1, < \rangle$.

Theorem 2. *Given a subset X of $\mathbb{Z}^n$ (resp. $\mathbb{N}^n$), the following assertions are equivalent: (i) X is first-order definable in $\mathcal{Z}$ (resp. $\mathcal{N}$);*
(ii) X is $\mathbb{N}$-semilinear;
(iii) X is a finite union of disjoint simple subsets.

Consequently, a subset in $\mathbb{Z}^n$ (resp. $\mathbb{N}^n$) is first-order definable in the above structure if and only if it is a disjoint union of simple subsets of $\mathbb{Z}^n$ (resp. $\mathbb{N}^n$).

2 A significant example

We study an example in order to highlight the specific properties that we take advantage of in order to more easily produce an equivalent counting predicate. Consider the first-order formula

$$\begin{aligned}&\phi(x_1, x_2, x_3, x_4) \equiv \exists z_1, z_2, z_3 : z_1, z_2, z_3 \geq 0\\ &(x_1 = z_1 + 2z_2 - z_3) \wedge (x_2 = 2z_1 + 4z_2 - 2z_3) \wedge (x_3 = 2z_1 + z_2) \wedge (x_4 = z_1 + z_2 - z_3)\end{aligned}$$

which we write as a linear system of equations

$$\begin{array}{lclclcl} z_1 & + & 2z_2 & - & z_3 & = x_1 \\ 2z_1 & + & 4z_2 & - & 2z_3 & = x_2 \\ 2z_1 & + & z_2 & & & = x_3 \\ z_1 & + & z_2 & - & z_3 & = x_4 \end{array}$$

The two specific features enjoyed by this example is the lack of disjunction and the fact that every submatrix of rank 3 necessarily contains the row of the matrix corresponding to the variable to be counted, namely the fourth row. We will see that these two conditions can always be assumed. The subsystem consisting of the first, third and fourth rows has determinant equal to 2. We solve the subsystem in the unknowns z_1, z_2 and z_3, which yields

$$\begin{array}{ll} 2z_1 & = -x_1 + x_3 + x_4 \\ 2z_2 & = 2x_1 - 2x_4 \\ 2z_3 & = x_1 + x_3 - 3x_4 \end{array}$$

Now, we must express the fact that the variables z_1, z_2, z_3 are positive integers. This is the case if and only if the following conditions hold (the coefficient 6 is the least common multiple of the coefficients of the variable x_4)

$$\begin{aligned} 6x_4 &\geq 6x_1 - 6x_3 \\ 6x_4 &\leq 6x_1 \\ 6x_4 &\leq 2x_1 + 2x_3 \\ x_1 + x_3 + x_4 &= 0 \bmod 2 \end{aligned} \tag{2}$$

The first three conditions are equivalent to

$$6x_1 - 6x_3 \leq 6x_4 \leq \min\{6x_1, 2x_1 + 2x_3\} \tag{3}$$

There are four different cases according to whether or not $2x_1 + 2x_3 \leq 6x_1$ and whether or not $x_1 + x_3 = 0 \bmod 2$. We only treat the case where these two conditions hold, implying in particular because of (2), we get $x_4 = 0 \bmod 2$. Observe that $2x_1 + 2x_3 \leq 6x_1$ is equivalent to $x_3 \leq 2x_1$ and therefore (3) can be expressed as

$$6x_1 - 6x_3 \leq 6x_4 \leq 2x_1 + 2x_3 \tag{4}$$

Then the number of even values x_4 satisfying (4) is equal to

$$\lfloor \frac{1}{6 \times 2}(2x_1 + 2x_3 - (6x_1 - 6x_3) \rfloor = \lfloor \frac{1}{3}(2x_3 - x_1) \rfloor$$

Consequently, the counting predicate $\exists^y_{x_4} \phi(x_1, x_2, x_3, x_4)$ is a disjunction of four predicates. One of the four predicates corresponds to $2x_1 + 2x_3 \leq 6x_1$ and $x_1 + x_3 = 0 \bmod 2$. It expresses that the variable x_4 varies in the interval (4) and is as follows

$$\exists x_4 \ \phi(x_1, x_2, x_3, x_4) \wedge (x_3 \leq 2x_1) \wedge (x_1 + x_3 =_2 0) \wedge (x_1 \leq 2x_3) \wedge y = \lfloor \frac{1}{3}(2x_3 - x_1) \rfloor$$

3 The proof

Because of Ginsburg's charaterization, every formula of Presburger arithmetic with free variables $x_1, \ldots, x_n$ is equivalent to a formula of the form

$$\phi(x_1, \cdots, x_n) \equiv \phi_1(x_1, \cdots, x_n) \vee \cdots \vee \phi_r(x_1, \cdots, x_n)$$

where the ϕ_i's define disjoint simple subsets $R_i \subseteq \mathbb{Z}^n$. Now we have

$$\begin{aligned} &\exists^{=y}_{x_n} \phi(x_1, \cdots, x_n) \equiv \exists y_1, \ldots, \exists y_r \\ &\exists^{=y_1}_{x_n} \phi_1(x_1, \cdots, x_n) \vee \cdots \vee \exists^{=y_r}_{x_n} \phi_r(x_1, \cdots, x_n) \wedge (y_1 + \cdots + y_r = y) \end{aligned}$$

It thus suffices to prove the case $r = 1$, which means that we can assume that $\phi(x_1, \cdots, x_n)$ defines a simple subset. We express the problem in terms of linear algebra. We use the expression (1) and we denote by $M \in \mathbb{Z}^{n \times p}$ the matrix of rank p whose columns are the linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_p}$. We are interested in solving the following equation where $\mathbf{x}$ and $\mathbf{a}$ are n-column integer vector and $\mathbf{z}$ is a p-column nonnegative integer vector

$$\mathbf{a} + M\mathbf{z} = \mathbf{x} \tag{5}$$

In particular we get

$$\phi(\mathbf{x}) \Leftrightarrow \exists \mathbf{z} \in \mathbb{N}^p : \mathbf{a} + M\mathbf{z} = \mathbf{x}$$

which in terms of matrices and with the convention that $b_{i,j}$ and a_i are the i-th components of the vector $\mathbf{b}_j$ and $\mathbf{a}$ respectively, is equivalent to the following system of equations

$$\begin{array}{lllllll} b_{1,1}z_1 & + & \cdots & + & b_{1,p}z_p & = x_1 - a_1 \\ \cdots \\ b_{n,1}z_1 & + & \cdots & + & b_{n,p}z_p & = x_n - a_n \end{array} \tag{6}$$

Observe that $p \leq n$. The matrix has rank p. If there is a submatrix of rank p obtained by selecting p among the $n-1$ first rows, then the $x_i - a_i$'s for which i is the index of a row among the selected rows define uniquely all $x_j - a_j$'s for all indices outside the selected rows. In particular there is a unique possible value for $x_n - a_n$'s. A Presburger formula expressing this relation is

$$\exists^{=y}_{x_n}\phi(x_1, \ldots, x_n) \equiv \exists x_n \phi(x_1, \ldots, x_n) \wedge y = 1.$$

Consider now the second case where all submatrices of rank p contain the last row. This means that there exist $p-1$ among the $n-1$ first rows that determine the values of the variables x_i, for $i < n$. Thus we may assume without loss of generality that $n = p$. By Cramer's rules, $z_1, \ldots z_p$ can be uniquely expressed as a function of x_i's, i.e.,

$$Dz_i = \lambda_{i,p}x_p + \sum_{j=1}^{p-1} \lambda_{i,j}x_j + \gamma_i \quad i \in \{1, \ldots, p\} \tag{7}$$

where D is the absolute value of the determinant of the matrix M and where the coefficients $\lambda_{i,j}, \gamma_i$ are integers. We want to express in FO(+) the fact that the z_i's are nonnegative integers. For that purpose we let $-\lambda_{i,p} = \frac{m}{\eta_i}$ where m is the least common positive multiple of the $-\lambda_{i,p}$'s, we let $S_i(x_1, \ldots, x_{p-1})$ be the polynomial $\sum_{j=1}^{p-1} \lambda_{i,j}x_j + \gamma_i$ and we set

$$\begin{cases} U_i(x_1, \ldots, x_{p-1}) = \eta_i S_i & \text{if } \eta_i > 0 \\ E_i(x_1, \ldots, x_{p-1}) = S_i & \text{if } \lambda_{i,p} = 0 \\ L_i(x_1, \ldots, x_{p-1}) = \eta_i S_i & \text{if } \eta_i < 0 \end{cases}$$

Let $A \subseteq \{1, \ldots, p\}$ be the set of indices i for which $\eta_i > 0$ and let $B \subseteq \{1, \ldots, p\}$ be the set of indices i for which $\eta_i < 0$. Then, the z_i's are nonnegative integers if and only if the following holds

$$U_i(x_1, \ldots, x_{p-1}) \geq mx_p \text{ for all } i \in A) \tag{8}$$

$$E_i(x_1, \ldots, x_{p-1}) \geq 0 \text{ for all } i \notin A \cup B \tag{9}$$

$$L_i(x_1, \ldots, x_{p-1}) \leq mx_p \text{ for all } i \in B) \tag{10}$$

$$\sum_{j=1}^{p} \lambda_{i,j}x_j + \gamma_i \equiv_D 0 \text{ for all } i = 1, \ldots, p \tag{11}$$

If $A = \emptyset$, for a fixed interpretation $a_1, \ldots, a_p$ of the variables $x_1, \ldots, x_p$ satisfying $\phi(x_1, \ldots, x_p)$ there are infinitely many values b such that $\phi(a_1, \ldots, a_{p-1}, b)$ holds. By convention we set $\exists^{=y}_{x_p}\phi = \texttt{false}$ and we treat similarly the case where $B = \emptyset$. We thus assume $A, B \neq \emptyset$. The conjunction of conditions (8) and (10) is equivalent to

$$\max_{\beta \in B} L_\beta(x_1, \ldots, x_{p-1}) \leq mx_p \leq \min_{\alpha \in A} U_\alpha(x_1, \ldots, x_{p-1}) \tag{12}$$

For all $\alpha \in A, \beta \in B$ set

$$\begin{array}{ll} H_{\alpha,\beta}(x_1,\ldots,x_{p-1}) & \equiv L_\beta(x_1,\ldots,x_{p-1}) = \max_{\beta'\in B} L_{\beta'}(x_1,\ldots,x_{p-1}) \\ & \wedge U_\alpha(x_1,\ldots,x_{p-1}) = \min_{\alpha'\in A} U_{\alpha'}(x_1,\ldots,x_{p-1}) \end{array}$$

Then condition (12) is equivalent to the following disjunction

$$\bigvee_{\alpha\in A,\beta\in B} H_{\alpha,\beta}(x_1,\ldots,x_{p-1}) \wedge L_\beta(x_1,\ldots,x_{p-1}) \leq mx_p \leq U_\alpha(x_1,\ldots,x_{p-1}) \tag{13}$$

Observe that if for two different pairs $(\alpha,\beta),(\alpha',\beta')$ the $p-1$-tuple $(x_1,\ldots,x_{p-1})$ satisfies both $H_{\alpha,\beta}$ and $H_{\alpha',\beta'}$ then the set of x_p associated is the same. Therefore we are left with computing the number of elements satisfying condition (11) in the interval between $L_\beta(x_1,\ldots,x_{p-1})$ and $U_\alpha(x_1,\ldots,x_{p-1})$ for fixed α,β. To that purpos let F be the set of mappings $f:\{1,\ldots,p\}\mapsto\{0,\ldots,D-1\}$ such that $\sum_{j=1}^{p}\lambda_{i,j}f(j)+\gamma_i \equiv_D 0$ for all $i=1,\ldots,p$ and let G be the set of mappings $g:\{1,\ldots,p-1\}\mapsto\{0,\ldots,D-1\}$. For $g\in G$ and $0\leq\theta<D$ the pair (g,θ) denotes the mapping $f\in F$, when it exists, whose restriction to $\{1,\ldots,p-1\}$ is g and such that $f(p)=\theta$. It is an easy exercise to verify that the predicate

$$\psi_{m,D,\theta}(y,u,v) \equiv y = \#\{k\in\mathbb{N} \mid u \leq m(kD+\theta) \leq v\}$$

is expressible in $\mathcal{Z}$. It thus suffices to replace the double inequality of (13) by the following disjunction over $g\in G$.

$$\begin{array}{l} \bigvee_{g\in G} \left[x_1 \equiv_D g(1) \wedge \cdots \wedge x_{p-1} \equiv_D g(p-1) \wedge \exists y_1,\ldots,y_c\ y = y_1+\cdots+y_c\right. \\ \left.\bigwedge_{(g,\theta_j)\in F} \psi_{m,D,\theta_j}(y_j, L_\beta(x_1,\ldots,x_{p-1}), U_\alpha(x_1,\ldots,x_{p-1})\right] \end{array} \tag{14}$$

4 The structure $\mathcal{N}$

We now deal with the structure $\langle\mathbb{N};+,<\rangle$. In order to rewrite the condition (7), we let $\eta_i S_i(x_1,\ldots,x_{p-1}) = P_i(x_1,\ldots,x_{p-1}) - N_i(x_1,\ldots,x_{p-1})$ where the coefficients of the two polynomials P_i and N_i are strictly positive. We let $A\subseteq\{1,\ldots,p\}$ be the subset of integers i such that $\eta_i>0$ and $B\subseteq\{1,\ldots,p\}$ be the subset of integers i such that $\eta_i<0$. Requiring that z_i be nonnegative is equivalent to requiring $P_i\geq N_i$ if $\eta_i>0$ and $N_i\geq P_i$ if $\eta_i<0$. Thus condition (12) is expressed as follows in $\mathcal{N}$

$$\max_{b\in B}\{\max\{P_b-N_b,0\}\} \leq mx_p \leq \min_{a\in A}\{\max\{P_a-N_a,0\}\}$$

The predicate $H_{\alpha,\beta}$ takes on the following form

$$\begin{array}{ll} H_{\alpha,\beta}(x_1,\ldots,x_{p-1}) = & \exists_{\alpha'\in A}u_{\alpha'}\exists_{\beta'\in B}v_{\beta'} \\ & \bigwedge_{\alpha'\in A}(u_{\alpha'}+N_{\alpha'}=P_{\alpha'} \vee u_{\alpha'}=0) \bigwedge_{\beta'\in B}(v_{\beta'}+N_{\beta'}=P_{\beta'} \vee v_{\beta'}=0) \\ & \wedge u_\alpha = \min_{\alpha'\in A} u_{\alpha'} \wedge v_\beta = \max_{\beta'\in B} v_{\beta'} \end{array}$$

and (13) takes on the form

$$\bigvee_{\alpha\in A,\beta\in B} H_{\alpha,\beta}(x_1,\ldots,x_{p-1}) \wedge u_\alpha \leq mx_p \leq v_\beta \tag{15}$$

The final predicate is obtained by substituting $\psi_{m,D,\theta_j}(y_j,v_\beta,u_\alpha)$ for $\psi_{m,D,\theta_j}(y_j,L_\beta,U_\alpha)$ in (14).

References

[1] Harry Apelt. Axiomatische Untersuchungen über einige mit der Presburgerischen arithmetik verwandte Systeme. *Zeitschr.f. Logik und Grundlagen d. Mat.*, 12:131–168, 1966.

[2] David A. Mix Barrington, Neil Immerman, and Howard Straubing. On uniformity within NC^1. *J. Comput. Syst. Sci.*, 41(3):274–306, 1990.

[3] S. Eilenberg and M.-P. Schützenbeger. Rational sets in commutative monoids. *Journal of Algebra*, 13(2):173–191, 1969.

[4] S. Ginsburg and E.H. Spanier. Semigroups, Presburger formulas, and languages. *Pacific J. Math.*, 16:285–296, 1966.

[5] Ryuichi Ito. Every semilinear set is a finite union of disjoint linear sets. *J. Comput. System Sci.*, 3:221–231, 1969.

[6] Nicole Schweikardt. Arithmetic, first-order logic, and counting quantifiers. *ACM Trans. Comput. Log.*, 6(3):634–671, 2005.

Roots of exponential polynomials

Paola D'Aquino

Universita' della Campania "L. VANVITELLI", Italy

paola.daquino@unicampania.it

Zilber identified a new class of exponential fields (pseudo-exponential fields) proving a categoricity result in every uncountable cardinality. He conjectured that the complex exponential field is the unique pseudo-exponential field of cardinality continuum. I will present a result jointly obtained with A. Fornasiero and G. Terzo in which we prove some instances of one of Zilber's axioms for ($\mathbb{C}$; exp).

Computable groups of low complexity

Henri-Alex Esbelin

LIMOS, Université Clermont Auvergne, France

henri.esbelin@uca.fr

Building on Rabin's definition of computable groups in [4], Cannonito defined in [1] a hierarchy of such groups, measuring the complexity of computation by the classes of functions $\mathcal{E}^\alpha$ of the Grzegorczyk's Hierarchy. Roughly speaking, a $\mathcal{E}^\alpha$-group has an integer indexing function of the elements, such that the product and inverse may be computed in $\mathcal{E}^\alpha$.

He proved numerous theorems of closure of the class of the $\mathcal{E}^\alpha$-groups under free or amalagamated products, quotients, etc... Due to his way of indexing, his results hold for $\alpha \geq 3$.

Studies on the Word Problem went far from this point of view, although Lipton and Zalcstein solved in [3] one of the main problem stated in [1], proving that the word problem for free groups and the membership problem for the two-sided Dyck language are solvable in logspace.

Building on their idea, we extend the definition and some results of Cannonito to computable groups with complexity in low classes $\mathcal{E}^\alpha$ and in the smallest classes of polynomially bounded functions with graphs in $\Delta_0^{\mathbb{N}}$ (the so-called rudimentary functions) or in $\left(\Delta_0^{\sharp}\right)^{\mathbb{N}}$ (for informations about these classes, see [2].)

References

[1] F. B. Cannonito, Hierarchies of Computable Groups and the Word Problem, Journal of Symbolic Logic, vol. 31 (3), 1966, pp. 376-392

[2] H.A. Esbelin, M. More, Rudimentary relations: a toolbox, Theoret. Comput. Sci., 193, 1998, pp. 129-148

[3] R. J. Lipton and Y. Zalcstein, Word Problems Solvable in Logspace, JACM, vol. 24 (3), 1977 pp 522-526

[4] M. O. Rabin, Computable algebra, general theory and theory of computable fields, Transactions of the American Mathematical Society, vol. 95, 1960, pp. 341-360.

Nonstandard methods and models of weak arithmetics

Jana Glivická

Charles University, Czech Republic

jana.glivicka@gmail.com

We show how to use nonstandard methods of set theory to obtain various models of weak arithmetics. The nonstandard methodology provides us with class mapping * defined on $\mathbf{V}$, the class of all sets. To construct models of arithmetics, we start with the structure $({}^{\cdot}\mathbb{N}, {}^{\cdot}+, {}^{\cdot}\cdot)$, which is obtained as the limit of an elementary chain $(\mathbb{N}, +, \cdot) \preccurlyeq ({}^{*}\mathbb{N}, {}^{*}+, {}^{*}\cdot) \preccurlyeq ({}^{**}\mathbb{N}, {}^{**}+, {}^{**}\cdot) \preccurlyeq \cdots \preccurlyeq ({}^{n*}\mathbb{N}, {}^{n*}+, {}^{n*}\cdot) \preccurlyeq \cdots$. The structure $({}^{\cdot}\mathbb{N}, {}^{\cdot}+, {}^{\cdot}\cdot)$ and its basic properties are due to work by Josef Mlček and Petr Glivický. For every $a \in {}^{\cdot}\mathbb{N}$, its rank is defined by $r(a) = \min\{n \in \mathbb{N}; a \in {}^{n*}\mathbb{N}\}$.

Graded arithmetical structures arise when functions ${}^{\cdot}+$ and ${}^{\cdot}\cdot$ are replaced by their so called graded versions. Given g_0, g_1, functions from $\mathbb{N}^2$ to $\mathbb{N}$, the graded version of $f(x, y)$ with respect to g_0, g_1 is defined as $f({}^{g_0(r(x),r(y))*}x, {}^{g_1(r(x),r(y))*}y)$.

We study basic properties of graded functions and explore how various choices of g_0, g_1 result in very different graded arithmetical structures. An important tool in analyzing the behavior of graded functions is the so called depth function.

We are especially interested in how grading influences prime numbers. By Chen's theorem, there are infinitely many primes p such that $p + 2$ is a product of at most two prime numbers. Using grading, it is possible to enforce that some composite numbers become primes with respect to the new multiplication; such numbers are called graded primes. Using Chen's theorem, we show how to obtain a structure that is a model of Robinson (and Presburger) arithmetic and in which the twin prime conjecture holds for graded primes.

Model theory of linear fragments of Peano arithmetic

PETR GLIVICKY
University of Economics, Prague, , Czech Republic
petrglivicky@gmail.com

We give a survey of our results (partialy a joint work with P. Pudlák) on linear arithmetics – linear fragments of Peano arithmetic (PA). For a cardinal k, the k-linear arithmetic LA_k is a theory extending Presburger arithmetic (in the language $(0, 1, +, <)$) by k unary functions of multiplication by distinguished (nonstandard) elements (called scalars) and containing the full scheme of induction for its language.

We give a classification of all definable sets in models of LA_1 and, as a corollary, show that LA_1 is a tame theory – model complete, decidable, NIP, having recursive nonstandard models...

On the other hand we prove that LA_2 (as well as any LA_k with $k > 2$) is model theoretically wild. As a manifestation of this fact we show that there is a model M of LA_2 in which an infinitely large initial segment of Peano multiplication (i.e. a multiplication $\cdot$ such that $(M, \cdot)$ is a model of PA) is 0-definable. Consequently, the theories LA_k with $k > 1$ are not model complete nor NIP.

Each model of a linear arithmetic naturally corresponds to a discretely ordered module over the ordered ring generated by the scalars. Our results on LA_2 thus yield a non NIP ordered module answering negatively the question of Chernikov and Hils whether all ordered modules are NIP.

Congruence Preservation and Recognizability

PATRICK CÉGIELSKI[1,3], SERGE GRIGORIEFF[2,3], IRÈNE GUESSARIAN[2,3,4]

We proved [1] that if $f : \mathbb{N} \longrightarrow \mathbb{N}$ is non decreasing then conditions (1) and (2) below are equivalent

(1) for all $a, b \in \mathbb{N}$, $a - b$ divides $f(a) - f(b)$ and $f(a) \geq a$,

(2) every lattice $\mathcal{L}$ of regular subsets of $\mathbb{N}$ which is closed under $x \mapsto x - 1$ is also closed under f^{-1}: i.e., for every $L \in \mathcal{L}$, $f^{-1}(L) = \{n \in \mathbb{N} \mid f(n) \in L\} \in \mathcal{L}$.

[1]LACL, EA 4219, Université Paris-Est Créteil, IUT Sénart-Fontainebleau, France cegielski@u-pec.fr
[2]IRIF, UMR 8243, Université Paris 7 Denis Diderot, France FirstName.LastName@irif.fr
[3]Partially supported by TARMAC ANR agreement 12 BS02 007 01
[4]Emeritus at UPMC Université Paris 6

Does this property still hold when we replace the semi-ring of natural integers $\mathbb{N}$ with the ring of integers $\mathbb{Z}$ or with the ring of profinite integers $\widehat{\mathbb{Z}}$? The corresponding property does not hold in the same terms, but the two conditions in **(1)** are fortunately equivalent to the notion of "congruence preservation" in the case of $\mathbb{N}$; we thus will use the latter notion of congruence preservation.

Moreover, as regular subsets coincide with recognizable subsets for $\mathbb{N}$, we will use "recognizable" subsets in condition **(2)**, leading to a statement more amenable to generalizations for algebras different from $\langle \mathbb{N}, + \rangle$. The above equivalence can thus be restated as

Theorem 1. *If $f : \mathbb{N} \longrightarrow \mathbb{N}$ is non decreasing then conditions (1) and (2) below are equivalent*

(1) *f is congruence preserving on $\mathbb{N}$ and, for all $a \in \mathbb{N}$, $f(a) \geq a$*

(2) *for every recognizable subset L of $\mathbb{N}$ the smallest lattice of subsets of $\mathbb{N}$ containing L and closed under $x \mapsto x - 1$ is also closed under f^{-1}.*

In the present paper, we investigate the relationships between congruence preservation, recognizability and lattices of recognizable sets. We will show that Theorem 1 extends to suitably ordered *residually finite algebras*, i.e., algebras where every congruence is an intersection of finite index congruences. Consequently, Theorem 1 also holds for $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, +, \times \rangle$. Extending Theorem 1 to the additive group of p-adic integers requires more work.

- the generalization holds for $\langle \mathbb{Z}_p, +, \times \rangle$ if we substitute "closure under all translations" for "closure under decrement".
- the generalization holds for $\langle \mathbb{Z}_p, + \rangle$ if we substitute "continuously recognizable subsets" for "recognizable subsets".

References

[1] P. Cégielski, S. Grigorieff, I. Guessarian, *On Lattices of Regular Sets of Natural Integers Closed under Decrementation*, Information Processing Letters 114(4): 197-202, 2014.

The logical strength of automata theory

Leszek Kolodziejczyk
Institute of Mathematics, University of Warsaw, Poland
lak@mimuw.edu.pl

I will talk about some recent results concerning the axiomatic strength needed to prove two classical theorems of automata theory: (1) the complementation theorem for nondeterministic automata on infinite words, which plays a key role in the proof of Büchi's theorem on the decidability of the MSO theory of the natural numbers with order, and (2) the complementation theorem for nondeterministic automata on infinite trees, which plays a key role in in the proof of Rabin's theorem on the decidability of the MSO theory of the full infinite binary tree.

Typical proofs of the complementation theorem for automata on words make use of either Ramsey's Theorem or Weak Kőnig's Lemma. We show that the axiomatic requirements of the theorem are actually rather tame, as it is equivalent to the Σ^0_2 induction principle over RCA_0. Also Büchi's decidabiliy theorem, to the extent that it can be stated in the language of second-order arithmetic, is equivalent to Σ^0_2 induction over RCA_0.

Typical proofs of the complementation theorem for automata on trees invoke the determinacy of some Borel games, more specifically of games in which winning conditions are given by boolean combinations of $\mathbf{\Sigma^0_2}$ sets. We show that this is in some sense necessary, as the complementation theorem is equivalent to $\mathrm{Bool}(\mathbf{\Sigma^0_2})$-determinacy over RCA_0. By results due to MedSalem and Tanaka as well as Heinatsch and Möllerfeld, it follows that complementation for automata on infinite trees is unprovable from Π^1_2-comprehension. Moreover, if Π^1_2-comprehension is taken as the base theory, then also Rabin's decidabiliy theorem, to the extent that it can be stated in the language of second-order arithmetic, becomes equivalent to $\mathrm{Bool}(\mathbf{\Sigma^0_2})$-determinacy.

The talk will be based on joint work with Henryk Michalewski, Pierre Pradic and Michał Skrzypczak.

Recent results on combinatorics and algorithmics of repeats in strings

Gregory Kucherov
CNRS & Université Paris-Est, Marne-la-Vallée, France
`Gregory.Kucherov@univ-mlv.fr`

We will present some recent combinatorial and algorithmic results on repeated structures in strings. In particular, we will focus on *α-gapped repeats* in strings [7, 4], defined as factors of the form uvu with $|uv| = |u| + |v| \leq \alpha|u|$. By way of introduction, we will summarize main results on *periodicities* in strings – a classic combinatorial notion that has long been a subject of study for "stringology" researchers [5] – including some major recent advancements [1].

Our main result is the $O(\alpha n)$ bound on the number of *maximal* α-gapped repeats in a string of length n, previously proved to be $O(\alpha^2 n)$ in [4]. For a closely related notion of maximal δ-subrepetition (maximal factors of exponent between $1 + \delta$ and 2), our result implies the $O(n/\delta)$ bound on their number, which improves the bound of [6] by a $\log n$ factor.

We also present an algorithmic time bound $O(\alpha n + S)$ (S size of the output) for computing all maximal α-gapped repeats. Together with our bound on S, this implies an $O(\alpha n)$-time algorithm for computing all maximal α-gapped repeats.

In the conclusion, we will mention some open questions and directions for future research.

Joint work with Maxime Crochemore (King's College London and Université Paris-Est) and Roman Kolpakov (Moscow University). Main results published in LATA'2016 conference [2].

References

[1] Hideo Bannai, Tomohiro I, Shunsuke Inenaga, Yuto Nakashima, Masayuki Takeda, and Kazuya Tsuruta. A new characterization of maximal repetitions by lyndon trees. In Piotr Indyk, editor, *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete*

Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015, pages 562–571. SIAM, 2015.

[2] Maxime Crochemore, Roman Kolpakov, and Gregory Kucherov. Optimal bounds for computing α-gapped repeats. In *Proc. of the 10th International Conference on Language and Automata Theory and Applications (LATA), Prague, Czech Republic, March 14-18, 2016*, volume 9618 of *Lecture Notes in Computer Science*, pages 245–255. Springer, April 2016.

[3] Pawel Gawrychowski, Tomohiro I, Shunsuke Inenaga, Dominik Köppl, and Florin Manea. Efficiently finding all maximal α-gapped repeats. In Nicolas Ollinger and Heribert Vollmer, editors, *33rd Symposium on Theoretical Aspects of Computer Science, STACS 2016, February 17-20, 2016, Orléans, France*, volume 47 of *LIPIcs*, pages 39:1–39:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[4] Pawel Gawrychowski and Florin Manea. Longest α-gapped repeat and palindrome. In Adrian Kosowski and Igor Walukiewicz, editors, *Fundamentals of Computation Theory - 20th International Symposium, FCT 2015, Gdańsk, Poland, August 17-19, 2015, Proceedings*, volume 9210 of *Lecture Notes in Computer Science*, pages 27–40. Springer, 2015.

[5] Roman Kolpakov and Gregory Kucherov. Periodic structures in words. In M. Lothaire, editor, *Applied Combinatorics on Words*. Cambridge University Press, 2005.

[6] Roman Kolpakov, Gregory Kucherov, and Pascal Ochem. On maximal repetitions of arbitrary exponent. *Information Processing Letters*, 110(7):252–256, 2010.

[7] Roman Kolpakov, Mikhail Podolskiy, Mikhail Posypkin, and Nickolay Khrapov. Searching of gapped repeats and subrepetitions in a word. In Alexander S. Kulikov, Sergei O. Kuznetsov, and Pavel A. Pevzner, editors, *Combinatorial Pattern Matching - 25th Annual Symposium, CPM 2014, Moscow, Russia, June 16-18, 2014. Proceedings*, volume 8486 of *Lecture Notes in Computer Science*, pages 212–221. Springer, 2014.

[8] Yuka Tanimura, Yuta Fujishige, Tomohiro I, Shunsuke Inenaga, Hideo Bannai, and Masayuki Takeda. A faster algorithm for computing maximal α-gapped repeats in a string. In Costas S. Iliopoulos, Simon J. Puglisi, and Emine Yilmaz, editors, *String Processing and Information Retrieval - 22nd International Symposium, SPIRE 2015, London, UK, September 1-4, 2015, Proceedings*, volume 9309 of *Lecture Notes in Computer Science*, pages 124–136. Springer, 2015.

On the Strength of Various Truth Principles

Mateusz Łełyk
University of Warsaw, Poland
lelyk@op.pl

An *axiomatic theory of truth* is an extension of PA formulated in a language $\mathcal{L}_{\rm PA} + T$, where T is a fresh unary predicate. The basic classically compositional theory of truth, $\rm CT^-$, is the extension of PA with sentences naturally corresponding to inductive Tarski's truth conditions for $\mathcal{L}_{\mathrm{PA}}$, e.g.

$$\forall\phi \quad \big(\mathrm{Sent}_{\mathcal{L}_{\mathrm{PA}}}(\phi) \to T(\neg\phi) \equiv \neg T(\phi)\big)^1. \tag{NEG}$$

The starting point of the talk is the theorem on multiple axiomatizations of CT^- extended with a Δ_0 induction for formulae with the T predicate (CT_0): putting together the results of Cieśliński ([2], [1], [3]), Kotlarski ([5]) and myself we can show that CT_0 is deductively equivalent to extensions of CT^- with various reflection principles, e.g.

TPA $\forall\phi \quad \big(\mathrm{Pr}_{\mathrm{PA}}(\phi) \to T(\phi)\big)$ ("All theorems of PA are true"),

TL $\forall\phi \quad \big(\mathrm{Pr}_{\emptyset}(\phi) \to T(\phi)\big)$ ("All theorems of First-Order Logic are true"),

REF $\forall\phi \quad \big(\mathrm{Pr}^T_{\emptyset}(\phi) \to T(\phi)\big)$ ("Consequences of true sentences are true").

Then we study the role the axiom NEG plays in obtaining these equivalences: we investigate analogous extensions of PT^-, the theory in which NEG is replaced with axioms of the form

$$\forall\phi,\psi \quad \Big(\mathrm{Sent}_{\mathcal{L}_{\mathrm{PA}}}(\phi) \wedge \mathrm{Sent}_{\mathcal{L}_{\mathrm{PA}}}(\psi) \to \big(T(\neg(\phi\vee\psi)) \equiv T(\neg\phi) \wedge T(\neg\psi)\big)\Big)^2.$$

It turns out that in this context adding bounded induction results one more axiomatization of CT_0. However differences between "completeness" (**TPA**, **TL**) and "closure" (**REF**) reflection principles become visible: PT^- extended with

1. **TL** is conservative over PA,
2. **TPA** is conservative over the Uniform Reflection scheme over PA, hence is strictly weaker than CT_0,
3. **REF** is the same as CT_0.

References

[1] Cezary Cieśliński. Deflationary truth and pathologies. *Journal of Philosophical Logic*, 39(3):325–337, 2010.

[2] Cezary Cieśliński. Truth, conservativeness, and provability. *Mind*, 119(474):409–422, 2010.

[3] Cezary Cieśliński. *The Epistemic Lightness of Truth. Deflationism and its Logic*. Cambridge University Press, forthcoming.

[4] Cezary Cieśliński, Mateusz Łełyk, and Bartosz Wcisło. Models of PT^- with internal induction for total formulae. *The Review of Symbolic Logic*, 10(1):187–202, 2017.

[5] Henryk Kotlarski. Bounded induction and satisfaction classes. *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik*, 32(31-34):531–544, 1986.

[6] Mateusz Łełyk and Bartosz Wcisło. Notes on bounded induction for the compositional truth predicate. *Review of Symbolic Logic*, to appear.

[1] For the details see [6]

[2] Similarly for $\neg\exists\phi$, $\neg\neg\phi$ and $\neg(s=t)$, where s,t are terms. For the details see [4]

Lipschitz determinacy for initial levels of the Hausdorff hierarchy in Second Order Arithmetic

Manuel José S. Loureiro
Lusófona University, Lisbon, Portugal
mloureiro@ulusofona.pt

Lipschitz games in the Cantor space are infinite two person games where players I and II alternately choose an element of $\{0, 1\}$ and built two infinite sequences. We know that Lipschitz games are determinate for all Borel sets in second order arithmetic. However, there is no analysis of the strength of Lipschitz games in terms of subsystems of second order arithmetic.

In this talk we show how to formalize Lipschitz games within second order arithmetic and we investigate the reverse mathematics of Lipschitz determinacy, as well as the tightly related semilinear order principle, for the first levels of the Hausdorff hierarchy. It turns out that the subsystem WKL_0 proves Lipschitz determinacy and semilinear order principle for clopen sets in the Cantor space. If we assume a certain dichotomy principle we can also derive Lipschitz determinacy for open sets within the subsystem WKL_0. Most remarkably, we can fully characterize ACA_0 in terms of Lipschitz determinacy for differences of closed sets in Cantor space.

This is joint work with Andrés Cordón-Franco (University of Seville) and F. Félix Lara-Martín (University of Seville).

The Four Color Conjecture as a particular case of Hilbert's tenth problem

Yuri Matiyasevich
St. Petersburg Department of V.A.Steklov Institute of Mathematics,
St.Petersburg, Russia
yumat@pdmi.ras.ru

Besides conventional proof of the undecidability of Hilbert's tenth problem there is a very informal "explanation" of the difficulty of Diophantine equations. Namely, according to DPRM-theorem many outstanding mathematical problems can be reformulated as assertions about non-existence of solutions of certain Diophantine equations. Examples of such problems are: Fermat's Last Theorem, Goldbach's Conjecture, Riemann's Hypothesis, and the Four Color Conjecture (4CC).

Hardly we can hope to give a new (or the first) solution of any of these four problems by examining corresponding (rather complicated) Diophantine equation. But we can look at such reformulations from the other side. Namely, the undecidability of Hilbert's tenth problem implies that we need to invent more and more ad hoc methods for dealing with more and more Diophantine equations. Now 4CC (proved forty years ago by K. Appel and W. Haken) can be viewed as a very sophisticated method of tackling a particular Diophantine equation.

One could try to "distill" their technique and then apply it to other equations. The success would heavily depend on the way of constructing such an equation, the universal technique of arithmetizing would just ruin the specificity of the Four Color Problem.

The talk will present a Diophantine equation equivalent to the Four Color Conjecture; in its construction the speaker tried to use the peculiarity of the 4CC as he could.

"One equation to rule them all", revisited

Domenico Cantone[1], Eugenio G. Omodeo[2]

If the quaternary quartic equation

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

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 1995, D. Shanks and S. S. Wagstaff conjectured that (*) has *in*finitely many solutions; while in doubt, it seemed wise to us to seek another candidate for the role of "one equation to rule them all". We put forward another quaternary quartic equation, namely

$$3\ (r^2 + 3\,s^2)^2 - (u^2 + 3\,v^2)^2 \;\;=\;\; 2\,,$$

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, we show how to construct a Diophantine relation of exponential growth.

Interpretations by Positive Existential Formulas and the Diophantine-Class Problems over Algebraic Structures

Albert Garreta, Alexei Miasnikov, and Denis Ovchinnikov
Stevens Institute of Technology, USA
dovchinn@stevens.edu

For an algebraic structure $\mathcal{M}$, the Diophantine problem over $\mathcal{M}$ (or $\mathcal{D}(\mathcal{M})$) is an agorithmic problem to decide, by a given finite system of equations over $\mathcal{M}$, if it has a solution or not. Despite the obvious interest in studying decidabilty of $\mathcal{D}(\mathcal{M})$, most of results concern the case when $\mathcal{M}$ is a commutative associative ring (a.g. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[X]$). I will try to avoid looking at these specific structures, and instead talk about $\mathcal{D}(\mathcal{M})$ for general structures $\mathcal{M}$.

I will explain the general machinery of interpretations by positive existential formulas (or PE-interpretations) that often allows one to reduce undecidability of $\mathcal{D}(\mathcal{M})$ to undecidabilty

[1]DMI, University of Catania, Italy. Email: cantone@dmi.unict.it
[2]DMG/DMI, University of Trieste, Italy. Email: eomodeo@units.it

of $\mathcal{D}(\mathcal{A})$ for some well known $\mathcal{A}$ (in particular $\mathcal{A} = \mathbb{Z}$), even if the initial structure $\mathcal{M}$ had a different signature.

I will focus on examples of new results about $\mathcal{D}(\mathcal{M})$ that can be obtained using this technique. Examples include wide classes of nilpotent or metabelian groups, as well as certain rings (not necessary commutative or associative).

Gödel's Second Incompleteness Theorem Without Arithmetization

FEDOR PAKHOMOV[1]
Steklov Mathematical Institute, Moscow, Russia
pakhfn@mi.ras.ru

Kurt Gödel in his famous paper on incompleteness theorems [Gö31] have introduced Gödel numbering of formulas. As far as the author is aware, all the existing presentations of Gödel's second incompleteness theorem rely on either an arithmetization of formal language or on formalization of it in terms of other notions of the same or higher expressibility power.

The key part of the usual proofs of the theorem is the use of Diagonal Lemma in order to construct a sentence that is equivalent to its own unprovability. We show that in certain much less expressive formal theories T it is still possible to formalize formal language and prove Diagonal Lemma. Namely, our requirement is that T interprets certain theory $\mathsf{Syn}(\mathsf{T})$ that we consider to be a "natural" theory of the syntax of T; note that the theory $\mathsf{Syn}(\mathsf{T})$ is mutually interpretable with the theory of pairing function on an infinite domain. In particular, it is possible to prove Diagonal Lemma for the elementary theory $\mathsf{Th}(\mathbb{N}, C)$ of Cantor pairing function $C(n,m) = (n+m)(n+m+1)/2+m$; in contrast with arithmetical theories, the theory is known to be complete and decidable [CGR00].

For T as above, Gödel Second Incompleteness Theorem holds for any provability predicate $\mathsf{Prv}(x)$ that satisfy Hilbert-Bernays-Löb derivability conditions. Also, we show that a theory T is undecidable if some $\mathsf{Prv}(x)$ satisfy the natural condition $\mathsf{T} \nvdash \underbrace{\mathsf{Prv}(\ulcorner \ldots \mathsf{Prv}}_{n \text{ times}}(\ulcorner \bot \urcorner) \ldots \urcorner)$, for all n.

References

[CGR00] Patrick Cégielski, Serge Grigorieff, and Denis Richard. La théorie élémentaire de la fonction de couplage de Cantor des entiers naturels est décidable. *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 331(2):107–110, 2000.

[Gö31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38(2):173–198, 1931.

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

Goodstein-type theorems and fast-growing functions

DENIS I. SAVELIEV[1]
Steklov Mathematical Institute, Moscow, Russia
d.i.saveliev@gmail.com

Goodstein's theorem [1] states that each process of a certain kind starting with any given natural number n and growing very fast, the faster the bigger n is, nonetheless terminates at 0. It was shown that this arithmetical fact is unprovable in Peano arithmetic [2]. Actually, the length of the process starting with $n \geq 4$ is extremely large and can be precisely calculated in terms of the Hardy [3] and Löb–Wainer [4] fast-growing hierarchies.

We consider similar processes where decompositions of natural numbers into a sum of powers of a given base, used in Goodstein's theorem, are replaced by decompositions into a sum of some functions growing faster than exponentiation. These processes also terminate at 0, and this fact has a higher proof-theoretic strength. The length of them also can be calculated via some faster-growing functions. Finally, we discuss some natural types of decompositions of large natural numbers.

References

[1] R. Goodstein. *On the restricted ordinal theorem.* Journal of Symbolic Logic, 9 (1944), 33–41.

[2] L. Kirby, J. Paris. *Accessible independence results for Peano arithmetic.* Bulletin of the London Mathematical Society, 14:4 (1982), 285–293.

[3] E. Cichon. *A short proof of two recently discovered independence results using recursive theoretic methods.* Proceedings of the American Mathematical Society, 87 (1983), 704–706.

[4] A. Caicedo. *Goodstein's function.* Revista Colombiana de Matemáticas, 41:2 (2007), 381–391.

Global neighbourhood completeness of the Gödel-Löb provability logic

DANIYAR SHAMKANOV[2]
Steklov Mathematical Institute, Moscow, Russia
daniyar.shamkanov@gmail.com

The Gödel-Löb provability logic GL is a modal logic describing all universally valid principals of the formal provability in Peano arithmetic. In this talk, we consider neighbourhood (topological) semantics of GL. As was independently noticed by H. Simmons [5] and L. Esakia [1],

[1]The author was supported by Grant 16-11-10252 of the Russian Science Foundation.
[2]This work is supported by the Russian Science Foundation under grant (14-50-00005).

formulas of GL can be interpreted as subsets of a scattered topological space, where boolean connectives correspond to boolean operations and the modal connective $\Diamond$ corresponds to the topological derivative operator acting on the given topological space. L. Esakia proved that GL is complete with respect to this topological interpretation. In addition, he established that scattered topological spaces coincide with neighbourhood GL-frames. In other words, neighbourhood semantics of GL and its topological interpretion coincide with each other. Further, V. Shehtman proved that GL is also strongly complete with respect to its neighbourhood semantics [4].

This strong completeness result is obtained for the so-called local semantic consequence relation. Recall that, over neighbourhood GL-models, a formula A is a local semantic consequent of Γ if for any neighbourhood GL-model $\mathcal{M}$ and any world x of $\mathcal{M}$

$$(\forall B \in \Gamma \ \mathcal{M}, x \vDash B) \Rightarrow \mathcal{M}, x \vDash A \ .$$

A formula A is a global semantic consequent of Γ if for any neighbourhood GL-model $\mathcal{M}$

$$(\forall B \in \Gamma \ \mathcal{M} \vDash B) \Rightarrow \mathcal{M} \vDash A \ .$$

This talk is devoted the case of the global semantic consequence relation over neighbourhood GL-models.

Recently a new proof-theoretic description for the Gödel-Löb provability logic GL in the form of a sequent calculus allowing non-well-founded proofs was given in [3, 2]. We consider Hilbert-style non-well-founded derivations in GL and establish that GL with the obtained derivability relation is strongly neighbourhood complete in the case of the global semantic consequence relation.

References

[1] L. Esakia. "Diagonal constructions, Löb's formula and Cantor's scattered space". In Russian. In: *Studies in Logic and Semantics* 132.3 (1981), pp. 128-143.

[2] R. Iemhoff. "Reasoning in circles". In: *Liber Amicorum Alberti. A Tribute to Albert Visser.* Ed. by Jan van Eijck et al. London: College Publications, 2016, pp. 165-178.

[3] D. Shamkanov. "Circular proofs for the Gödel-Löb provability logic". In: *Mathematical Notes* 96.3 (2014), pp. 575-585.

[4] V. Shehtman. "On neighbourhood semantics thirty years later". In: *We Will Show Them! Essays in Honour of Dov Gabbay.* Ed. by S. Artemov et al. Vol. 2. London: College Publications, 2005, pp. 663-692.

[5] H. Simmons. "Topological aspects of suitable theories". In: *Proceedings of the Edinburgh Mathematical Society* 19.4 (1975), pp. 383-391.

On entropic measures of computations

Anatol Slissenko
Université Paris-Est Créteil, LACL, France
anatol.slissenko@sfr.fr

It is intuitively clear that an algorithm (program or circuit), while computing a function, diminishes the uncertainty of its knowledge about the result. The classical measure of uncertainty in mathematics is entropy. However, this notion does not represent adequately our intuition about (deterministic) computations. E.g., if the domain of search diminishes then intuitively so does the uncertainty but, in general, not entropy.

An entropy-style measure demands a probabilistic distribution. We take a measure reflecting the *principle of maximal uncertainty*: imagine that an algorithm plays against an adversary who wishes to maximize the uncertainty of the result; then all outputs should be equiprobable.

Denote by F the function computed by an algorithm $\mathfrak{A}$. We restrict the analysis to the inputs of the domain of F of a fixed size $\boldsymbol{n}$, where $\boldsymbol{n}$ is not far from the bitwise size (e.g., the number of vertices or edges of a graph). Below $\boldsymbol{dm}$ is this finite domain of F (for better intuition we suppose that it is big, say of a cardinality exponential in $\boldsymbol{n}$), $\boldsymbol{rn}$ is the respective range $F(\boldsymbol{dm})$ and $M = |\boldsymbol{rn}|$ (the number of values of F over $\boldsymbol{dm}$). According the principle of maximal uncertainty we take as a probabilistic measure $\boldsymbol{P}(f^{-1}(v)) = \frac{1}{|\boldsymbol{rn}(f)|}$. On $F^{-1}(v)$, $v \in \boldsymbol{rn}(f)$, we make it uniform. On can think about non-uniform measures inside sets $F^{-1}(v)$ or dynamic measures that change during the execution of $\mathfrak{A}$ but we do not discuss it here.

Intuitively, when processing an input, say X, algorithm $\mathfrak{A}$ searches in what set $F^{-1}(v)$ the input is placed. We represent the runs of $\mathfrak{A}$ as traces. Each trace is a sequence of events, and each event is either an update (assignment) or a guard (the condition in a conditional branching). We tacitly suppose that the complexity of an event is much smaller than the time complexity of $\mathfrak{A}$. Each trace us transformed into a sequence of literals containing only inputs and basic operations of $\mathfrak{A}$ (arithmetical, logical operations, shifts etc.). This transformation eliminates some events that do not explicitly depend on inputs, like those related to looping etc. Besides its technical role, such a logical representation of runs permits to better understand the type of algorithms we deal with, and put a question of lower bounds of complexity for such particular models that are much simpler and better comprehensible than general algorithms; however, they englobe many practical ones.

The next crucial step is to attribute to each event E a subset of $\boldsymbol{dm}$ that is, in a way, defined by this event. The point is that many traces may have events similar to E, so all inputs defining these traces are in the set $\hat{E}$ attributed to E. We order $\boldsymbol{rn}$, and thus the sets $F^{-1}(v)$, and construct an ordered partition $\pi(E)$ of $\boldsymbol{dm}$ that consists of sets $\hat{E} \cap F^{-1}(v)$. For $\pi(E)$ we define a measure $\mathcal{D}(\pi(E))$ with the properties: $\mathcal{D}(\boldsymbol{dm}) = \log M$ (maximal uncertainty); if $S \subseteq F^{-1}(v)$ then $\mathcal{D}(S) = 0$ (maximal certainty); if $S \subseteq S'$ then $\mathcal{D}(S) \leq \mathcal{D}(S')$ (monotone, decreasing).

The analysis of the behavior of $\mathcal{D}$, though technically difficult, gives a valuable information about $\mathfrak{A}$ that shows ways of improving the algorithm. It seems likely that $\mathcal{D}$ may be useful in the search for complexity lower bounds for classes of interesting algorithms (as mentioned above).

This framework is illustrated by examples.

Some technical details, including the transformation of events into literals and a definition of $\mathcal{D}$ can be found in my paper http://arxiv.org/abs/1605.01519.

On weak monadic second-order definability in some weak arithmetical structures

Stanislav O. Speranski
St. Petersburg State University, St. Petersburg, Russia
katze.tail@gmail.com

This talk surveys some recent results on weak monadic second-order definability in

$$\langle \mathbb{N}; +, = \rangle, \quad \langle \mathbb{N}; \times, = \rangle, \quad \langle \mathbb{N}; \mid \rangle \quad \text{and} \quad \langle \mathbb{N}; \perp \rangle$$

where $\mid$ and $\perp$ denote the divisibility relation and the coprimeness relation respectively. In particular, we shall see that for each of these structures, if a set of n-tuples is computably enumerable and closed under automorphisms of this structure, then it is weakly Σ_1^1-definable (by a Σ_1^1-formula with only one set quantifier) in this structure.

To prove these and other results, we use the technique developed in [4] and [5]. Further — in applying this technique to the four structures mentioned above some results on first-order definability in their expansions obtained in [3] and [1] turn out to be helpful, as well as the famous Matiyasevich–Robinson–Davis–Putnam theorem [2].

References

[1] A. Bès and D. Richard (1998). Undecidable extensions of Skolem arithmetic. *Journal of Symbolic Logic* 63:2, 379–401. DOI: 10.2307/2586837

[2] Yu. V. Matiyasevich (1993). *Hilbert's Tenth Problem.* MIT Press.

[3] H. Putnam (1957). Decidability and essential undecidability. *Journal of Symbolic Logic* 22:1, 39–54. DOI: 10.2307/2964057

[4] S. O. Speranski (2013). A note on definability in fragments of arithmetic with free unary predicates. *Archive for Mathematical Logic* 52:5–6, 507–516. DOI: 10.1007/s00153-013-0328-9

[5] S. O. Speranski (2015). Some new results in monadic second-order arithmetic. *Computability* 4:2, 159–174. DOI: 10.3233/COM-150036

Remarks on Lachlan's Theorem

BARTOSZ WCISŁO
University of Warsaw, Poland
bar.wcislo@gmail.com

Our talk concerns satisfaction classes in models of Peano Arithmetic (PA). Let $M \models \mathrm{PA}$ be a model of PA. Then a satisfaction class $S \subset M$ may be viewed as an interpretation of a fresh predicate (intended to represent the truth predicate) satisfying Tarski's compositional clauses for certain (Gödel codes of) arithmetical sentences, including at least some nonstandard ones. If the satisfaction class happens to satisfy the compositional clauses for all (codes of) arithmetical formulae, we call it a **full satisfaction class**. If the class satisfies compositional clauses for (the codes of) all sentences of complexity at most Σ_c for some nonstandard c, we call it a **partial satisfaction class**. If $S \subset M$ is a satisfaction class, either full or partial, and the expanded structure (M, S) satisfies the induction axioms for the expanded language, we call the satisfaction class **inductive**.

It is surprisingly difficult for a model of PA to admit a full satisfaction class. Namely, the following theorem holds:

Theorem 1 (Lachlan)**.** *Let* $M \models \mathrm{PA}$ *be a nonstandard model. Suppose that exists a full satisfaction class* $S \subset M$*. Then* M *is recursively saturated.*

The proof has been originally presented in [1]. In our talk, we will try to present a proof of Lachlan's theorem which closely follows the original argument and the proof of Smith's theorem that every model of PA which has a full satisfaction class also has an undefinable class satisfying Δ_0-induction (which in particular shows that not every recursively saturated model of PA admits a full satisfaction class). We believe however that our presentation is considerably more structured and makes the theorem look much less *ad hoc*. Moreover, it allows for certain generalisations. In particular, if time allows we would like to show how our proof of Lachlan's theorem may be slightly modified to obtain the following result (which has been originally presented in [2]):

Theorem 2. *Let* $M \models \mathrm{PA}$ *be a nonstandard model. Suppose that there exists a partial satisfaction class* $S \subset M$*. Then there exists a partial inductive satisfaction class* $S' \subset M$*.*

One can show relatively easily that any model M which has a partial inductive satisfaction class is recursively saturated. On the other hand, a partial inductive satisfaction class $S' \subset M$ is clearly undefinable in M and satisfies Δ_0-induction. Thus the above result gives a common generalisation of both Lachlan's and Smith's theorems.

References

[1] A. Lachlan, "Full satisfaction classes and recursive saturation," *Canadian Mathematical Bulletin* 24(3), 1981, pp. 295–297.

[2] M. Łełyk and B. Wcisło, "Models of weak theories of truth," *Archive for Mathematical Logic* 2017, doi:10.1007/s00153-017-0531-1, pp. 1–22.

[3] S. T. Smith, "Nonstandard definability," *Annals of Pure and Applied Logic* 42, pp. 21–43.

Interpretations in Presburger Arithmetic

ALEXANDER ZAPRYAGAEV
Moscow State University, Moscow, Russia
rudetection@gmail.com

This is joint work with Fedor Pakhomov.

It is well known that Peano Arithmetic (**PA**) is a *reflexive theory,* that is, it proves the consistency of all its finitely axiomatizable subtheories. All sequential theories with full induction scheme are also reflexive, such as all extensions of **PA** and set theory **ZF**. Reflexivity implies the impossibility to interpret a theory in any of its finite subtheories. But unlike reflexivity this property could be formulated for any theory, not just theories that could formalize consistency statements. A. Visser asked whether a similar phenomenon holds for the interpretations of less expressive theories still possessing the induction principle. In particular, he considered *Presburger Arithmetic* **PrA**, the true theory of $(\mathbb{N}, +)$. J. Zoethout studied Visser's conjecture in one-dimensional case [1] and established it under the assumption of the statement of Theorem 1(b). Thus by proving the following theorem we showed the impossibility to interpret **PrA** one-dimensionally in any of its finite subtheories.

Theorem 1. *Let* $\iota\colon$ **PrA** $\to \mathbb{N}$ *be a one-dimensional parameter-free interpretation of Presburger Arithmetic in the model* $(\mathbb{N}, +)$. *Then (a) the interpretation gives the model that is isomorphic to the standard one; (b) the isomorphism is definable in* $(\mathbb{N}, +)$.

Note that Theorem 1(a) was known to Zoethout, though we found a simpler proof. In order to prove the analogue of Theorem 1(a) for multi-dimensional case we study which orders are interpretable in $(\mathbb{N}, +)$. We show that all such orders are *scattered* (do not contain a dense suborder). Using the notion of VD-rank the following stronger result was obtained:

Theorem 2. *All m-dimensionally interpretable in* **PrA** *linear orders ($m \geq 1$) are of VD-rank $m + 1$ or below.*

In order to prove it, we show that for any infinite **PrA**-definable set $M \subseteq \mathbb{N}^m$ there is a unique number $n \geq 1$ such that there is a Presburger-definable isomorphism between M and $\mathbb{N}^n$. We call n the *Presburger dimension* of M. Theorem 2 immediately implies the multi-dimensional generalization of Theorem 1(a). Whether the (b) part also holds when $m \geq 2$, however, remains an open question.

References

[1] Zoethout, J. *Interpretations in Presburger Arithmetic.* BS thesis. Utrecht University, 2015.