Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 322 (2004) 1–3

Theoretical Computer Science

www.elsevier.com/locate/tcs

Foreword

Weak arithmetics concern applications of logical methods to Number Theory. Spectacular results of this domain are undecidability in the field of rational numbers by Julia Robinson (1949) and the (negative) solution to the 10th Hilbert's problem by Yuri Matiyasevich (1970), but many other results appear in the domain every year. In a previous special issue of Theoretical Computer Science devoted to weak arithmetics, Denis Richard [1] presented many topics from this domain.

A web site `http://www.univ-paris12.fr/lacl/jaf` is devoted to JAF (*Journées sur les Arithmétiques Faibles/Weak Arithmetics Days*), with a summary of its 23 issues.

Papers of this special issue are extended contributions of selected speakers in a colloquium dedicated to the sixtieth birthday of Denis Richard: `http://llaic3.u-clerm-ont1.fr/conference60/`.

They represent a characteristic choice of research in weak arithmetics and were refered to journal standard.

There are many works around the consistency of arithmetic. Zofia Adamowicz and Leszek Aleksander Kołodziejczyk study a variant of first-order Peano arithmetic. They replace classical induction schema of axioms by some Π_1-expressible combinatorial principles, related to the consistency of Σ_n^b-induction, denoting theories by $Sk(\Sigma_n^b, \mathit{length}\ \log^k)$ and $Sk(\Sigma_n^b, \mathit{depth}\ \log^k)$ (where '*Sk*' stands for 'Skolem'). They show that theory $Sk(\Sigma_n^b, \mathit{depth}\ \log^k)$ implies $Sk(\Sigma_{n+1}^b, \mathit{length}\ \log^k)$ and that theory $Sk(\Sigma_n^b, \mathit{length}\ \log^{k-2})$ implies $Sk(\Sigma_{n+1}^b, \mathit{length}\ \log^k)$.

The Curry–Howard isomorphism has given rise to many developments on extraction of algorithms. The idea is to build formal intuitionistic theories with a relatively strong induction scheme, for which any provable formula of the form

$$\forall x \exists y B(x, y)$$

is realizable by an algorithm f, that is computable in a polynomial time

$$\forall x B(x, f(x)).$$

The paper of Anatoly Petrivich Beltiukov is such a study.

Sometimes, works around Weak Arithmetics allow the improvement of methods in general logic. This is the case with the method of *destinies*, introduced by Francis Nézondet, whose known applications concern Number Theory. Annie Chateau compares two classes of decidable structures: the class of H-bounded structures, in which quantifiers can be bounded by some recursive function H, and the class of

doi:10.1016/j.tcs.2004.03.021

structures with recursive destinies. She shows that the first class is strictly included in the second one and she characterizes the first class as the class of structures with strongly recursive destinies.

Locally finite ω-languages are defined by second-order quantifications followed by a first-order locally finite sentence. They enjoy very nice properties and extend languages accepted by finite automata or defined by monadic second-order sentences, linked to Presburger arithmetic. Olivier Finkel studies closure properties of the family LOC_ω of locally finite omega languages. In particular, he shows that the class LOC_ω is neither closed under intersection nor under complementation.

In the context of possibly infinite computations yielding finite or infinite (binary) outputs, the space $2^{\leqslant\omega} = 2^* \cup 2^\omega$ appears to be one of the most fundamental spaces in Computer Science. Verónica Becher and Serge Grigorieff study some of its properties involving topology and computability. The paper is an encyclopedical survey with new results. The link with Computable Analysis is beyond Weak Arithmetics but is related.

Yassine Hachaïchi introduces and studies some fragments of monadic second- and first-order Peano arithmetic and their connections to famous complexity classes. Starting from descriptive complexity results, and exhibiting an effective method for translating formulas between different logical structures representing encodings of integers, he gives some arithmetical characterizations of NP, PH, NL, and P.

Pairing is important in Weak Arithmetics: multiplication is not definable with addition alone but it is with addition and pairing. Hence, definability of pairing is a central issue. Andrea Formisano, Eugenio Omedeo, and Alberto Policriti explore many definitions of pairing by a method introduced by Tarski and Givant.

A theorem of Tarski shows importance of axioms of large cardinals in Weak Arithmetics: existence of solution to a given diophantine equation depends on the universe of sets (related to consistency). Jean-Pierre Ressayre gives a new proof of finite state determinacy, inspired by Martin's proof of analytic determinacy using the large cardinal axiom of sharps.

Karine Shahbazyan and Yuri Shoukourian study recognizability and definability for Existential Monadic Second Order (EMSO) logic for homogeneous flow event structures. A homogeneous flow event structure is specified by an arbitrary poset $G = (V, \leqslant)$ and a finite flow event structure F as a result of copying F in vertices of G with additional homogeneous flow and conflict relations on the events of adjacent vertices. They show that the sets of configurations of homogeneous flow event structures and languages of proving sequences are EMSO-definable.

Alan Woods exhibits a lower bound of complexity for testing primality. A Σ_3^2 Boolean circuit has three levels of gates. The input level is comprised of OR gates each taking as inputs 2, not necessarily distinct, literals. Each of these OR's feeds one or more AND gates at the second level. Their outputs form the inputs to a single OR gate at the output level. Using the projection technique of Paturi, Saks, and Zane, he shows that the smallest Σ_3^2 Boolean circuit testing primality for any number given by n binary digits has size $2^{n-o(n)}$. Disjunctive normal form (DNF) formulas can be considered to be a special case of Σ_3^2 circuits, and this bound applies to them too.

Igor Zaslavsky defines first-order theory PRAU as an extension of R.L. Goodstein's system PRA of the primitive recursive arithmetic, based on the consideration of functions similar to primitive recursive functions, but in general not defined everywhere. He proves that PRAU is a conservative extension of PRA. He introduces some classes of program schemes (PRA-schemes and PRAU-schemes) and proves that the classes of functions computable by such schemes coincide with the classes of functions taking part, correspondingly, in PRA and PRAU.

Acknowledgements

This research is supported by Intas Grant "Weak Arithmetics" 001-447. Guest editors want to thank following referees for their assistance:
Alexis Bès, University Paris 12
Guillaume Bonfante, École des Mines de Nancy
Christian Choffrut, University Paris 7
Constantin Dimitracopoulos, University of Athens
Arnaud Durand, University Paris 12
Irène Guessarian, University Paris 6
Akihiro Kanamori, Boston University
Johann Makowsky, Technion—Israel Institute of Technology
Chris Pollett, San José State University
Nicole Schweikardt, Humboldt University in Berlin
Valentin Shehtman, King's College and Moscow University
Igor Shparlinski, Macquarie University, Sydney
Ludwig Staiger, Halle University.

Patrick Cégielski
LACL, UMR-FRE 2673, Université Paris 12
IUT Route Forestière Hurtault
F-77300 Fontainebleau, France
E-mail address: cegielski@univ-paris12.fr

Malika More
LLAIC1, EA 2146, Université d'Auvergne
IUT Informatique
B.P. 86, F-63172 Aubière, Cedex, France
E-mail address: more@llaic3.u-clermont1.fr

References

[1] D. Richard, What are Weak Arithmetics? Theoret. Comput. Sci. 257 (1–2) (2001) 17–29.