MRTN-CT-2004-512234
MODNET
Model Theory and Applications

MVII.1: Decidability issues and links to complexity theory

Period number: 2	Due date of deliverable: 30/12/06
Period covered: from 1/01/05 to 30/12/06	Date of preparation: 07/02/07
	Date of submission: (SESAM)
Start date of project: 1/01/05	Duration: 48 months

Project coordinator name: David Evans

Project coordinator organization name:
UEA, Norwich, UK.

Organization name of lead contractor for this deliverable:
University of Camerino.

Project Co-Funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination in level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Report on Workpackage VII: Decidability issues and links to complexity theory

In the following, members of the Network are identified by an asterisk (*) when first mentioned; external experts and collaborators who were identified as having a close involvement with the project in the original proposal are identified by a double asterisk (**).

Results of task VII.1

Task VII.1: Finitely generated fields and connections with arithmetic (Hilbert's 10th problem) a) Investigate existential definition of the integers in the rationals, or in rings of algebraic integers b) Prove Diophantine undecidability of the rationals).

a) In a series of papers, J.Koenigsmann** (Freiburg/MPI Bonn) showed that almost any perfect field K (in the language of fields) is biinterpretable with the Galois group of the rational function field $K(X)$ over K (in the language of profinite groups due to Cherlin, van den Dries, Macintyre** and Chatzidakis*). In particular, K is (existentially) decidable iff this Galois group is. This gives rise to an altogether new approach to Hilbert's 10th problem for $\mathbf{Q}$, as well as to the question of decidability of $\mathbf{F}_p((t))$ and undecidability of $\mathbf{C}(t)$. A detailed survey of these results can be found in the extended abstract [K1] on Koenigsmann's homepage

http://home.mathematik.uni-freiburg.de/koenigsm/papers.html,

where the series of papers will also shortly appear. The paper [K2], published in 2006, is also part of this research program.

Again about a), a characterization has been given of the meromorphic maps from the torus minus a point to itself. This is a joint result of Thanases Pheidas** with Kourouniotis and Vidaux [KPV], and can be viewed as a first step towards proving that the existential theory of the ring of analytic functions of two variables, in the language of rings augmented by names for the variables, is undecidable. This addresses Task (a), as said, but is also important independently, because analytic functions are used throughout mathematics and its applications and almost all results on the complexity of

computation of that ring have immediate consequences on the computational aspects of these rings.

b) A negative answer to the analogue of Hilbert's tenth problem for the operation of addition and the property of "being a square" was proved for fields of rational functions of any characteristic again by Pheidas and Vidaux in [PV]. This improves earlier results of Vojta and can be seen as a strong indication that the analogous problem for the field of rationals has a similar (negative) answer. The techniques do not seem transferable to the case of the rationals, due to difficulties arising also for problems such as Mordell's Conjecture (for instance, the use of differentiation), but there is currently a vast amount of machinery on similar situations and there seems to be hope for this transfer in the not-so-long future.

Finally, a survey was presented in meetings and summer schools and for publication [PZ] by Pheidas and Zahidi** on aspects of both questions, (a) and (b), which, besides its historical nature, presents a new formulation, in terms of logic, of geometrical questions of a computational character. This could have an impact on computational geometry and number theory in the future.

Christian Michaux* (Mons) is also developing the study of the structure $< N, +, V_2 >$ where $V_2(x)$ is the largest power of two which divides x. This extension of Presburger Arithmetic was studied from the 1960's because its definable subsets of n are exactly the sets of nonnegative integers which, written in base 2, are recognizable by finite automata. Recently new interest in this structure occurs as a complete automatic structure, i.e. all first-order structures with an automatic presentation can be interpreted in it and only those ones. The project is to re-examine this structure in the light of the new developments which occurred during the last years on automatic structures. In particular one can show that $< N, +, V_2 >$ has independence property and quantifier elimination in some (not too unnatural) extension of the original language. Some results about this project were presented during the Modnet workshop in Lyon.

Task VII.2: Algebraic complexity a) Examine the $P = NP$ question in important rings.

A significant headway in the $P = NP$ problem over arbitrary structures has been made Prunescu* (in Freiburg until the end of october 2005) in his papers [Pr1, 2], proving that there are structures where deciding the truth of

pure existential formulas with parameters in the structure can be done in a uniform polynomial time in the sense of unit-cost complexity. According to this notion of computation, the structure has the property P = NP, which shows that there is no philosophical obstacle in achieving this for infinite structures. This solves an open question put by Bruno Poizat* (Lyon 1) in his book "Les Petits Cailloux" in the early 1990's. The construction and the proof are model-theoretic and use properties of the totally free algebras: locality, quantifier-elimination, super-stability; also some special properties of predicates called sparse and generic. The construction goes over a consistent TRUTH-PREDICATE that can be quickly accessed in the structure (this means: by making polynomially many operations in the structure).

General results concerning classical complexity are shown by Malod* and Fournier in [FM], where the structure of $\#P$-complete problems is studied according to the technique introduced by Agrawal and Biswas for the class NP. This is based on replicating the structure of $\#3SAT$ for arbitrary $\#P$-complete problems, or rather for the relations with which they are defined.

Work of Malod* (Mons) –partly with Portier**– deals with Valiant complexity classes. [MP] approaches them via restricted classes of arithmetic circuits. This also answers raised, showing the completeness of several operations of linear algebra for the class capturing the complexity of the Determinant polynomial, and the linear closedness of the Determinant. The paper also deals with the complexity classes VP and VNP, both introduced in terms of sequences of polynomials. A characterization of a uniform version of VNP is provided. [M] studies the links between the complexity of a polynomial and that of its coefficient function, and shows that VNP is stable for "taking coefficients"; while the same property holds for VP if and only if $VP = VNP$ (and thus is unlikely). These questions are also considered for classes of unbounded degree $VPnb$ and $VNPnb$. This leads us to study the computation of big integers. In the case of fields of positive characteristic, this computation can be done, and one gets the same results as above. This also shows that the question of VP vs VNP has the same answer in both bounded degree and unbounded degree cases if the characteristic is positive. Finally one shows that the ability to compute higher order partial derivations on polynomials represented as circuits is also equivalent to VP vs VNP.

Further investigations are planned again about VP and VNP. The question $VP = VNP$ is still open, as are the relations between other complexity classes. Notably the permanent sequence is complete for VNP, and the determinant sequence is complete for a smaller class than VP, called $VPws$.

It turns out that, although the definition of VP is more natural, the natural polynomials seem to live in $VPws$ if they are quickly computable. This seems to contrast Valiant's latest work on holographic algorithms, which shows that some counting problems which would seem intractable (i.e. in the class $\#P$) "fall" in a class lower than P, mostly by elaborate reductions to the Determinant or the Pfaffian.

A $PSPACE$ class has been singled out over rings. In detail, Koiran** and Perifel** introduced the class $VPSPACE$ of sequences of polynomials computable in polynomial parallel time [KP]. In the meantime Poizat* (Lyon) [Po] introduced the class VSP of sequences of polynomials defined by arithmetic circuits with summations inside (and not only at the output gate) of polynomial complexity. VSP arises in a natural way as a class closed for taking Malod's coefficient function. Poizat also realized that VSP equals $VPSPACE$ and clarifies substantially the connections between the complexity classes of polynomial á la Valiant and the classical ones (of boolean functions).

Task VII.3: Models of fragments of arithmetic a) Partners 1, 11: Prove that the residue field in models of $I\Delta_0 + \Omega_1$ are pseudofinite b) Partners 1, 11: Prove existence of infinitely many primes over $I\Delta_0(p)$ where $p(x)$ counts the primes below x c) Partners 1, 11: Study quadratic forms, local/global results, quadratic reciprocity over bounded arithmetic.

Paola D'Aquino** and Angus Macintyre** have concentrated on task c) and have carried an analysis of quadratic forms over models of $I\Delta_0 + \Omega_1$ [DM]. The motivation was to prove quadratic reciprocity law in weak fragments of Arithmetic. Gauss second proof relies on the integral theory of binary quadratic forms. The treatment in [DM] was inspired by Cassel's analysis of integral quadratic forms. Some connections with fundamental solutions of Pell equations were proved, and a global and local analysis of quadratic forms over models of $I\Delta_0 + \Omega_1$ was developed. Due to the lack of exponentiation in models of $I\Delta_0 + \Omega_1$ a finer analysis of the classical proofs had to be carried, and new and subtle arguments had to be found, for example continued fractions approximations in the construction of the global group associated to quadratic forms of fixed discriminant.

[DK] - a joint paper of Paola D'Aquino and Julia Knight - also deals with $I\Delta_0$ and studies certain initial segmente of its models.

References.

[DK] P. D'Aquino-J. Knight, Strong initial segments of models of $I\Delta_0$, submitted.

[DM] P. D'Aquino-A. Macintyre, Quadratic forms over models of $I\Delta_0 + \Omega_1$, I, Ann. Pure Applied Logic, to appear.

[FM] H. Fournier-G. Malod, Universal Relations and $\#P$-completeness, Lecture Notes in Computer Science, 368-379, 2006 (Algorithms and Complexity, Proceedings of CIAC 2006).

[K1] J. Koenigsmann, Recovering fields from Galois groups, extended abstract

[K2] J. Koenigsmann, Projective extensions of fields (with applications to the inverse Galois problem and the Leopoldt conjecture), J. London Math. Soc. (2) 73(3), 2006, 639-656

[KPV] C. Kourouniotis-T. Pheidas-X. Vidaux, Analytic Maps on Elliptic Surfaces and Undecidability in fields of Meromorphic Functions, Proceedings of the "International Conference on Analysis and Applications", Nanjing, China, to appear.

[KS] P. Koiran-S. Perifel, VPSPACE and a transfer theorem over the reals, submitted.

[M] G. Malod, The complexity of polynomials and their coefficient functions, IEEE Conference on Computational Complexity 2007, to appear.

[MP] G. Malod-N. Portier, Characterizing Valiant's algebraic complexity classes, Lecture Notes in Computer Science 4162, 704-716, 2006 (MFCS 2006, Proc. 31st International Symposium on Mathematical Foundations of Computer); an extended version is going to appear in J. Complexity.

[Po] B. Poizat, Une expression de taille polynomiale en n de la factorielle d'un nombre de n chiffres, J. Symbolic Logic, submitted.

[Pr1] M. Prunescu, Structure with fast quantifier elimination J. Symbolic Logic 71, 1, 321 - 328, 2006.

[Pr2] M. Prunescu, Fast quantifier elimination means P = NP Lecture Notes in Computer Science 3988, 459 - 471, 2006 (Logical Approaches to Computational Barriers).

[Pr3] M. Prunescu, Concrete algebraic cohomology over the group (R, +), CUBO, to appear.

[PV] T. Pheidas-X. Vidaux, The analogue of Buchi's problem for rational functions, J. London Mathematical Society (2) 76 (2006), 545-565.

[PZ] T. Pheidas-K. Zahidi, Analogues of Hilbert's tenth problem, Cambridge University Press, London Mathematical Society Lecture Note Series, to appear.