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

MVII.2: Decidability issues and links to complexity theory

Period number: 4	Due date of deliverable: 30/12/08
Period covered: from 1/01/05 to 30/12/08	Date of preparation: 18/02/09
	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 Network are identified by an asterisk (*) when first mentioned; Modnet fellows are identified by a double asterisk (**); external experts and collaborators who were identified as having a close involvement with the project in the original proposal are identified by a triple 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.

Hilbert's 10th problem asked to give a procedure which, in a finite number of steps, can determine whether a polynomial equation (in several variables) with integer coefficients has or does not have integer solutions. This was negatively answered by Matiyasevich in 1970, following work of Davis, Putnam and Julia Robinson: no such algorithm can exist.

Similar questions can be raised for domains other than the ring of integers. For instance the analogue of Hilbert 10th problem over the field of rationals is still unanswered. A general picture of the current situation in this framework is given by Thanases Pheidas*** and Karim Zahidi*** in [PhZ], following tutorials presented at American Institute of Mathematics and at Newton Institute of Mathematical Sciences at the beginning of the Modnet program. This report surveys both (a) and (b). Besides their history, it also provides a new formulation, in terms of logic, of several geometrical questions of a computational character, which could have an impact on computational geometry and number theory in the future.

A contribution to the solution of Hilbert's 10th problem over the rationals can be found in [CZ], proving that a conjecture about elliptic curves provides an interpretation of $\mathbf{Z}$ in $\mathbf{Q}$ with quantifier elimination $\forall\exists$ involving only one universally quantified variable. This implies that the Π_2-theory of the field of rationals is undecidable (recall that Hilbert's 10th problem for the rationals is basically the question whether the Σ_1-theory of $\mathbf{Q}$ is undecidable).

However something stronger holds. In fact Jochen Koenigsmann* recently improved these results and provided a direct proof that $\mathbf{Z}$ is definable in $\mathbf{Q}$ just by an $\forall\exists$-formula with only one universal quantifier (so avoiding any additional assumption). Actually Koenigsmann even showed that $\mathbf{Z}$ is universally definable in $\mathbf{Q}$, indeed there is a polynomial $g(t, x_1, \ldots, x_{58})$ with 59 unknowns and integer coefficients such that, for every rational number t, t is an integer if and only if $\forall x_1 \ldots \forall x_{58} g(t, x_1, \ldots, x_{58}) \neq 0$. This implies that the $\forall\exists$-theory of the field of rationals is undecidable. Hilbert's 10th problem over $\mathbf{Q}$ is basically the question whether the $\exists$-theory of $\mathbf{Q}$ is decidable. As said, this is still open. However Koenigsmann also proved that $\mathbf{Z}$ is not existentially definable in $\mathbf{Q}$ under a rather mild arithmo-geometric conjecture (much weaker than Mazur's),
A preliminary report of Koenigsmann's results can be found in [Ko].
Pheidas also proposed some years ago a program which might give an existential definition of $\mathbf{Z}$ in K where K is any global field. The so called *Existential Divisibility Lemma* is a key step in this program. A generalization of this Lemma to all global fields of characteristic not 2 (and to other settings) is given by Demeyer*** and Van Geel in [DeVG].
Papers of Demeyer [De1, 2] also consider Hilbert's 10th problem over rings of polynomial over finite fields.
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 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 regards 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 a wide range of computational aspects on rings.
A negative answer to the analogue of Hilbert's 10th 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 [PhV1]. 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.
Actually [PhV1] deals with Büchi's problem asking whether, for large enough M, the only integer solutions of the system of equations $x_n^2+x_{n-2}^2 = 2x_{n-1}^2+2$ $(1 < n < M)$ satisfy $\pm x_n = \pm x_{n-1}^2 + 1$ and gives a positive answer for polynomial rings of characteristic 0 or greater than 17, and for rational function fields of characteristic 0 or greater than 19 (under some additional assumptions in the positive characteristic case).
Büchi's problem –more precisely a generalization of it over a polynomial ring $K[t]$ with K a field of characteristic 0– is considered in [PhV2]. It is shown that a sequence of 92 or more cubes in $K[t]$, not all constanct, with third difference constant and equal to 6, is of the form $(f+n)^3$ $(n < 92)$ for some polynomial $f \in K[t]$. This result is used, in conjunction to the negative answer of the analogue of Hilbert's 10th Problem for $K[t]$ in order to show that the solvability of systems of degree 1 equations, where some of the variables are assumed to be cubes and (or) non-constant, is an unsolvable problem over $K[t]$.
Work of Prunescu[*/***] can be also subscribed to task VII.1 and a). In [Pru5] the Hilbert 10th Problem is studied relatively to subsets of $\mathbf{Z}$. It is proven for example that it is undecidable if diophantine equations have solutions which consist of prime numbers. Undecidability is proven for sets of integers which are images of an interval of integers through polynomials. However, similar images through exponential functions like 2^k lead to decidable decision problems.
Titles [Pru6]-[Pru9] also refer to this task, but in a wide way. These articles study recurrent double sequences of the following form. One has a *finite* structure $(A, f(.,.,.), 1)$ and forms sequences $a(i,j)$ by putting $a(0,j) = a(i,0) = 1$ and $a(i,j) = f(a(i-1,j), a(i-1,j-1), a(i,j-1))$.
Then [Pru6] and [Pru7] prove that in the special case where $A = F$ is a finite field and $f(x,y,z) = x + my + z$ there are self-similar recurrent double sequences. In the case when F is a prime field all the obtained patterns are self-similar. There are very strong connections between the arithmetic of the finite field and the symmetry structure of the pattern, which are described and proved. A byproduct is the discovery of a combinatorial identity, another one the description of a class of aperiodic tilings.
The paper [Pru8] studies the general recurrent double sequence $a(i,j) = f(a(i-1,j), a(i,j-1))$ over commutative finite structures. It is shown that those structures interpret Turing machines, so there are a lot of undecidable

problems related to their properties.
The paper [Pru9] studies the ideal of polynomials in fundamental symmetric functions over a finite field, representing the polynomial function 0. The dimension of this ideal is computed and an algorithm to find a basis of this ideal is described and studied. This research occured in the context of the recurrent double sequences.
The paper [Pru10] contains also a flavor of decidability. It is proven that the functional equation given in the title has solutions if and only if $g(x, y)$ is a symmetric cocycle. Moreover, if g is of class C^k ($k \geq 0$) then there are solutions f of this class. The most difficult proof is for $k = 0$ (continuous functions) — which has also a connection with the decidability: if f is algorithmically approximable, then there are such solutions f.
The decidability theme is also considered by the paper of Franoise Point* [Pn], dealing with some expansions of Presburger arithmetic by exponentiation or related functions.

Task VII.2: Algebraic complexity a) Examine the $P = NP$ question in important rings.
The Millennium problem $P = NP$ is one of the top questions in Theoretical Computer Science and contemporary Mathematics. Roughly speaking, it asks whether it is easier to verify a proof or finding this proof (provided that it exists). One generally expects a positive answer, so that $P \neq NP$, but an ultimate theorem confirming this intuition still seems far from being proved. Due to the extreme difficulty of the general problem, some hopefully easier algebraic versions have been proposed, in particular by Valiant, or by Blum-Shub-Smale. A common feature of these models is to deal with real numbers, or with complex numbers. Indeed, in the Poizat* generalization of the Blum-Shub-Smale BSS approach [Po], arbitrary structures M are regarded, and a $P_M = NP_M$ question is raised for each of them. In this perspective the originary $P = NP$ question is that corresponding to $M = \mathbf{Z}/2\mathbf{Z}$, and so to *Boolean* complexity.
In Valiant's model and in BSS, when dealing with real and complex numbers the cost of a computation refers to the arithmetical operations of addition and multiplication it involves; in BSS comparison tests are also considered and counted. Valiant's model is interested in calculating polynomials such as the permanent or the determinant of a matrix, while BSS is mainly concerned in deciding whether a given system of polynomial equations has a solution over the reals, or over the complex numbers. Just as in the originary Boolean

setting, even in the Valiant and BSS models confirming $P = NP$ or negating it, or separating other notable classes such as P itself and $PSPACE$, are related to several intriguing algebraic questions. For instance, $P = NP$ over the reals in the Valiant model means to compute the permanent of a matrix in a number of mathematical operations (additions and multiplications) polynomial with respect to the matrix size. On the other hand the key question towards the solution of $P = NP$ over the field of reals in BSS is to decide, for any polynomial of degree 4 in n unknowns, whether it admits a real root in a number of steps –now involving even comparisons– polynomial in n.

It is also natural to compare these models (Boolean, Valiant and BSS) and to wonder whether some separation result transfers from one of them to the other ones. Connections of this kind were observed between Valiant's model and the Boolean one, or between the latter and BSS. On the other hand, almost nothing is known directly BSS and Valiant's model under this point of view.

Pascal Koiran*** and his group in Lyon have been considering all these topics. In particular Koiran and Perifel*** obtain several noteworthy transfer results, proving that separations theorems are harder in BSS that in the Valiant model. For instance [KP4] shows that separating P and NP in BSS by a problem of NP without multiplication (a natural candidate in this framework) implies to separate P and NP even in the Valiant model. On the other hand [KP2] shows that separating P and $PSPACE$ over the complex field in BSS implies to separate P and $PSPACE$ also in the Valiant model.

The paper [KP3] extends this kind of results also over the field of reals. Even in this setting separating P and $PSPACE$ is more difficult for decision problems than for valuation problem. The proof is based on some algorithmic results obtained by Koiran and Perifel in a paper to appear in *Journal of Complexity* (a parallel algorithm is proposed to find a vector orthogonal to about half a family of vectors over the field with two elements, by a sort of derandomization ensuring that an aleatory vector satisfies the required condition with high probability).

Other connections with the Boolean complexity are illustrated in [KP4], where various consequences of the hypothesis $P = SPACE$ are obtained in the setting of valuation problems, supporting the conjecture that the two classes may be different in the Valiant model. Further results (still to be published) connect the separation of P and NP in the Valiant model and

the question whether the existence of a Boolean algorithm working in polynomial time to compute the value of a polynomial implies the existence of an arithmetical circuit of polynomial size for that polynomial.
Even [KP1] deals with Boolean complexity, more precisely studies how to handle by Boolean Turing machines certain polynomials given in terms of arithmetical circuits. Lower and under bounds are provided for the computation of the degree of a polynomial and of the coefficient of a monomial.
Finally [FKL] studies the complexity of valuating some "difficult" polynomials (like permanent, hamiltonian and so on) for certain classes of graphs: planar graphs and bounded treewidth graphs. It shows how to characterize the complexity of valuating the corresponding polynomials by certain families of arithmetical circuits (formulas, or *"skew circuits"*.
Also the work of Malod$^{**/*}$ [MP1,2] [M1, 2, 3] is concerned with the $P = NP$ problem in different rings. However, following the lead of Poizat [Po], it focuses on studying arithmetic circuit computations, first looking at circuit computations in the most basic manner, by starting with two operations and no properties and then adding properties towards the common arithmetic operations. The basic question in this perspective is the comparison of the computational power of circuits and formulas of polynomial size. What is shown is that elementary parameters of the circuit let us classify easily when the operations are "free", but as we add more properties to the operations interesting questions arise quickly.
The use of specific constants for computation is also studied. For instance, the completeness proof of the permanent uses the constants $-\frac{1}{2}, -1, 0, 1$. It is very unlikely that the permanent could be complete with just the constants $-1, 0, 1$ as it would imply an equality of the type $P = \oplus P$. However, the Hamiltonian is complete with these constants. Malod defines a notion of *auto-reducibility* and shows that the matrix product, the determinant and the Hamiltonian are all auto-reducible with the constants $0, 1$ whereas this is not clear with regard to the permanent. This raises an interesting open question, because it is related to the completeness of the permanent for the class $\sharp P$, and would help to answer questions raised in [DHK].
Another aspect Malod has been considering is to find an intuitive meaning to some of the main circuit classes. In a first series of results the classes are linked to matrix and tensor computations [M3]. A simple, yet still not natural, complete problem has been defined for VP, one of the most important classes. With the help of this result the main classes are characterized as "counting" injective homomorphisms between adequate classes of graphs.

Again in relation to counting, Malod and Hervé Fournier give a different treatment of their results on $\sharp P$-completeness in a journal version [FM2] of their conference article [FM1].
Further algebraic aspects of the $P = NP$ problem are also considered in papers of Prunescu ([Pru1]-[Pru4]). They were already illustrated in our mid-term report.
Other papers linked to algebraic complexity in some "non standard models of computation" are [B], [BBR], [BDLM] (by Brihaye*, Da Costa Lopes**, Render** and the Mons group).

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*** continued their study of quadratic forms in bounded arithmetic (following [DM1]). In [DM2] the authors develop a theory of local equivalence of quadratic forms over completions of models of $I\Delta_0 + \Omega_1$, as an essential step in proving a version of Gauss' classical result of Quadratic Reciprocity Law in $I\Delta_0 + \Omega_1$. As in previous work on the global investigation of integral quadratic forms over $I\Delta_0 + \Omega_1$, the inspiration is the analysis by Cassels. The local groups associated to quadratic forms of fixed discriminant are constructed as well as a group structure is defined on the product of these.
Also [DKS] partly deals with this task, as it studies integer parts of real closed fields in connection with recursive saturation. It is shown that if a real closed field has an integer part which is a model of Peano Arithmetic then the field is recursively saturated. Moreover, any countable recursively saturated real closed field has an integer part which is a model of Peano Arithmetic and whose real closure coincides with the starting field.

References.

[B] T. Brihaye, Words and bisimulations of dynamical systems, Discrete Mathematics and Theoretical Computer Science, 9 (2007), 11-31.

[BBR] T. Brihaye, V. Bruyre and E. Render, Formal languages properties of o-minimal hybrid systems, submitted

[BDLM] T. Brihaye, A. Da Costa Lopes, F. Laroussinie and N. Markey, ATL with Strategy Contexts and Bounded Memory, LFCS'09, Lectures Notes in Computer Sciences 5407, 92-106, Springer

[CZ] G. Cornelissen and K. Zahidi, Elliptic divisibility sequences and undecidable problems about rational points, J. Reine Angew. Math. 213 (2007), 1-33

[De1] J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra 310 (2007), 801-828

[De2] J. Demeyer, Recursively enumerable sets of polynomials over a finite field are Diophantine, Invent. Math. 170 (2007), 655-670

[DeVG] J. Demeyer and J. Van Geel, An existential divisibility lemma for global fields, Monatsh. Math. 147 (2006), 293-308

[DHK] A. Durand, M. Hermann and P. G. Kolaitis, Subtractive reductions and complete problems for counting complexity classes, Theor. Comput. Sci. 340 (2005), 496-513

[DK] P. D'Aquino and J. Knight, Strong initial segments of models of $I\Delta_0 + \Omega_1$, Fund. Math. 195 (2007), 155-176

[DKS] P. D'Aquino, J. Knight and S. Starchenko, Real closed fields and models of Peano Arithmetic, preprint 2008

[DM1] P. D'Aquino and A. Macintyre, Quadratic forms in models of $I\Delta_0+\Omega_1$, part I, Ann. Pure Applied Logic 148 (2007), 31-48

[DM2] P. D'Aquino and A. Macintyre, Quadratic forms in models of $I\Delta_0+\Omega_1$, part II, preprint 2008

[FKL] U. Flarup, P. Koiran and L. Lyaudet, On the expressive power of planar perfect matching and permanents of bounded treewidth matrices, Proceedings of ISAAC 2007

[FM1] H. Fournier and G. Malod, Universal Relations and $\#P$-completeness, in T. Calamoneri, I. Finocchi and G. F. Italiano (eds.), Algorithms and Complexity, Proceedings of CIAC 2006, Lecture Notes in Computer Science, 368-379, Springer, 2006

[FM2] H. Fournier and G. Malod, Universal Relations and $\#P$-completeness, Theor. Comput. Sci. 407 (2008), 97-109

[Ko] J. Koenigsmann, Defining $\mathbf{Z}$ in $\mathbf{Q}$, 2009 Oberwolfach Reports, Arithmetic of fields, February 1-7, 2009

[KP1] P. Koiran and S. Perifel, The complexity of two problems on arithmetic circuits, Theoretical Computer Science 389, 172–181, 2007

[KP2] P. Koiran and S. Perifel, VPSPACE and a transfer theorem over the complex field, Proceedings of MFCS 2007, Lecture Notes in Computer

Science 4709, Springer

[KP3] P. Koiran and S. Perifel, VPSPACE and a transfer theorem over the reals, Proceedings of STACS 2007

[KP4] P. Koiran and S. Perifel, Valiant's model: from exponential sums to exponential products, Proceedings of MFCS 2006, Lecture Notes in Computer Science 4708, Springer

[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

[M1] G. Malod, Circuits arithmétiques et calculs tensoriels, to appear in the Proceedings of the conference Logicum Lugdunensis

[M2] G. Malod, The complexity of polynomials and their coefficient functions, IEEE Conference on Computational Complexity 2007, 193-204, IEEE Computer Society, 2007

[M3] G. Malod, Circuits arithmétiques et calculs tensoriels. J. Inst. Math. Jussieu 7 (2008), 869-893

[MP1] G. Malod and N. Portier, Characterizing Valiant's algebraic complexity classes, in MFCS 2006, Proceddings of the 31st International Symposium on Mathematical Foundations of Computer Science, Lecture Notes in Computer Science 4162, 704-716, Springer, 2006

[MP2] G. Malod and N. Portier, Characterizing Valiant's algebraic complexity classes, J. Complexity 24 (1), 16-38, 2008

[PhV1] T. Pheidas-X. Vidaux, The analogue of Buchi's problem for rational functions, J. London Mathematical Society (2) 74 (2006), 545-565

[PhV2] T. Pheidas-X. Vidaux, The analogue of Buchi's problem for cubes in rings of polynomials, Pacific J. Math. 238 (2008), 349-366

[PhZ] T. Pheidas-K. Zahidi, Decision problems in algebra and analogues of Hilbert's tenth problem, Model theory with applications to algebra and analysis 2, 207-235, London Mathematical Society Lecture Note Series 350, Cambridge University Press, Cambridge 2008

[Pn] F. Point, On the expansion ($\mathbf{N}$, $+$, 2^x) of Presburger arithmetic , in H. Friedman, Boolean relation theory and incompleteness, ASL, to appear

[Po] B. Poizat, Les petits cailloux, Aléas, Lyon, 1995

[Pru1] M. Prunescu, Two situations with unit-cost: ordered abelian semigroups and some commutative rings, J. Complexity, 21, 4, 579-592, 2005.

[Pru2] M. Prunescu, The symmetric subset-sum problem over the complex numbers, in Dolzmann, Seidl and Sturm (eds.), Algorithmic Algebra

and Logic. Proceedings of the A3L Conference in the Honour of the 60-th Birthday of Volker Weispfenning, Passau, 2005, 201 - 207, 2005

[Pru3] M. Prunescu, Structure with fast quantifier elimination, J. Symbolic Logic, 71, 321–328, 2006

[Pru4] M. Prunescu, Fast elimination of quantifiers means $P = NP$, in A. Beckmann, U. Berger, B. Löwe and J. V. Tucker (eds.), Logical Approaches to Computational Barriers, Lecture Notes in Computer Science 3988, 459–471, 2006,

[Pru5] M. Prunescu, Undecidable and decidable restrictions of Hilbert's Tenth Problem: images of polynomials vs. images of exponential functions, Math. Logic Quarterly, 52, 14–19, 2006.

[Pru6] M. Prunescu, Self-similar carpets associated with the odd primes, Proceedings of the conference "Computability in Europe", CiE 2007, Siena, Italy

[Pru7] M. Prunescu, Self-similar carpets over all finite fields, to appear in European J. Combinatorics, 2008. Published online by the European J. Combinatorics at: http://dx.doi.org/10.1016/j.ejc.2008.08.002

[Pru8] M. Prunescu, An undecidable property of recurrent double sequences, Notre Dame J. Formal Logic, 49, 143–153, 2008

[Pru9] M. Prunescu, Symmetric functions over finite fields, submitted, 2008

[Pru10] M. Prunescu, Concrete algebraic cohomology for the group $(\mathbb{R}, +)$ or how to solve the functional equation $f(x + y) - f(x) - f(y) = g(x, y)$, CUBO 9, 39–45, 2007