STARTPAGE

PEOPLE
MARIE CURIE ACTIONS

International Outgoing Fellowships (IOF)
Call: FP7-PEOPLE-IOF-2008

Publishable Summary

“PACCAP”

Problems in Algebraic Complexity and Complexity of Algebraic Problems

The "P $\neq$ NP ?" problem is widely recognized as one of the most important and challenging open problems in contemporary mathematics and computer science. Is it easier to check the proof of a statement than to find such a proof when it exists? The general belief is that this question admits a positive answer, i.e., that P is strictly included in NP. Unfortunately, this intuition is still not supported by a proof in spite of 35 years of intensive research. Given the difficulty of this problem, algebraic versions of "P $\neq$ NP ?" have been proposed. The hope is that these algebraic versions of the problem should be easier to solve than the original one.

One of the main algebraic versions of "P$\neq$ NP ?" is due to Valiant. Valiant's model does not deal with decision problems (i.e., problems admitting a "yes or no" answer) but with polynomial evaluation. The permanent polynomial

$$\mathrm{per}(x_{11}, \ldots, x_{nn}) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

is a prominent example of a VNP-complete family of polynomials. The algorithmic content of the "VP = VNP ?" problem is thus as follows: is it possible to evaluate the permanent of a matrix in a number of arithmetic operations which is polynomial in the size of this matrix? It is widely believed that the permanent is not computable by arithmetic circuits of size polynomial in n.

It is known that this much coveted lower bound for the permanent would follow from a so-called *real τ-conjecture* for sums of products of sparse polynomials. Those are polynomials of the form $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(x)$, where the sparse polynomials f_{ij} have at most t monomials. According to the real τ-conjecture, the number of real roots of such an expression should be polynomially bounded in k, m and t. The original τ-conjecture by Shub and Smale deals with integer roots of arbitrary (constant-free) straight-line programs. As a first step towards the real τ-conjecture in [GKPS], we considered the family of sums of products of powers of sparse polynomials. Those polynomials are of the form $\sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$. They are best viewed as sums of products of sparse polynomials where the total number m of distinct sparse polynomials is "small", but each polynomial may be repeated several times. We obtain a $O(t^{m(2^{k-1}-1)})$ upper bound on the number of real roots of such a polynomial, where t is the maximum number of monomials in the f_j's. In particular, the bound is polynomial in t when the "top fan-in" k and the number m of sparse polynomials in the expression are both constant. Note also that the bound is independent of the magnitude of the integers α_{ij}.

Bounds on the number of real zeros for systems of sparse polynomials were abundantly studied by Khovanskiĭ in his "fewnomial theory". His results on fewnomials imply an upper bound exponential in k, m and t. In a new work ([KPT]) we gave a bound in $t^{O(k^2 m)}$, thereby removing the double exponential while staying polynomial in t. Moreover, our results extend well to some other families of functions. We remarked first that finding the roots of a product of polynomials is easy: it is the union of the roots of the corresponding polynomials. But finding the roots of a sum is difficult: for example how to bound the number of real roots of $fg + 1$ where f and g are t-sparse? It is an open question to decide if this bound is linear in t. Our main tool to tackle the sum is the Wronskian. We recall that the Wronskian of a family of functions $f_1, \ldots, f_k$ is the determinant of the matrix of the derivatives. More formally,

$$W(f_1, \ldots, f_k) = \det\left(\left(f_j^{(i-1)}\right)_{1 \leq i,j \leq k}\right)$$

This tool has been widely studied in linear differential equations: for a given homogeneous differential equation of order k and a family of solutions $f_1, \ldots, f_k$, the Wronskian $W(f_1, \ldots, f_k)$ is identically zero (the family is dependent) or has no real root (the family is a basis of the solutions). In our case, we have to use other tools because the considered Wronskians are non zero polynomials with some real roots. In particular, we use the classical and very useful Descartes' rule of signs.

Another way of approaching the complexity of polynomials is to study how they can be represented by one of the most important, and easy to compute, of them: the determinant. This is a very well studied problem, and one version of it is to ask the considered matrices to be symmetric: given a polynomial f of degre d, can we fin a symmetric matrix A, whose entries are variables or constants, such that $f = \det(A)$? What is the smallest dimension of such a matrix? Quarez answered to this question with a purely algebraic construction that leads to exponential matrix dimensions t. We continued ([GKKP, GKKP11]) this line of work but we proceed differently by symmetrizing the complexity theoretic construction by Valiant. Our construction yields smaller dimensional matrices not only for polynomials represented as sums of monomials but also for polynomials represented by formulas and weakly skew circuits. Our constructions are valid for any field of characteristic different from 2. The case of fields of characteristic 2 was studied later by our student, Bruno Grenet, and other authors.

The last approach we studied in this project ([CGKPS]) is the factorisation and identity testing of lacunary polynomials. The *lacunary*, or *supersparse*, representation of a polynomial

$$P(X_1, \ldots, X_n) = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

is the list of the tuples $(a_j, \alpha_{1,j}, \ldots, \alpha_{n,j})$ for $1 \leq j \leq k$. This representation allows very high degree polynomials to be represented in a concise manner. The factorization of lacunary polynomials has been investigated in a series of papers. Cucker, Koiran and Smale first proved that integer roots of univariate integer lacunary polynomials can be found in polynomial time.This result was generalized by Lenstra who proved that low-degree factors of univariate lacunary polynomials over algebraic number fields can also be found in polynomial time.More recently, Kaltofen and Koiran generalized Lenstra's results to bivariate and then multivariate lacunary polynomials. A common point to these algorithms is that they all rely on a so-called *Gap Theorem*: If F is a factor of $P(\bar{X}) = \sum_{j=1}^{t} a_j \bar{X}^{\bar{\alpha}_j}$, then there exists k_0 such that F is a factor of both $\sum_{j=1}^{k_0} a_j \bar{X}^{\bar{\alpha}_j}$ and $\sum_{j=k_0+1}^{k} a_j \bar{X}^{\bar{\alpha}_j}$. Moreover, the different Gap Theorems in these papers are all based on the notion of height of an algebraic number, and some of them use quite sophisticated results of number theory. In our work, we are interested in more elementary proofs for some of these results. We show how a Gap Theorem that does not depend on the height of an algebraic number can be proved. In particular, our Gap Theorem is valid for any field of characteristic zero. As a result, we get a new, more elementary, algorithm for finding linear factors of bivariate lacunary polynomials over an algebraic number field.

References

[GKKP] B. Grenet, E. Kaltofen, P. Koiran, N. Portier, Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits, to appear in *AMS Contemporary Mathematics Proceedings*

[GKKP11] B. Grenet, E. Kaltofen, P. Koiran, N. Portier, Symmetric Determinantal Representation of Weakly Skew Circuits, *STACS 2011*

[GKPS] B. Grenet, P. Koiran, N. Portier, Y. Strozecki The Limited Power of Powering: Polynomial Identity Testing and a Depth-four Lower Bound for the Permanent, *FSTTCS 2011 (IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, December 12 to 14, 2011, IIT Bombay, Mumbai, India)*

[GKP10] B. Grenet, P. Koiran, N. Portier, The multivariate resultant is NP-hard in any characteristic, *MFCS 2010 (35th International Symposium on Mathematical Foundations of Computer Science)*

[GKP] B. Grenet, P. Koiran, N. Portier, On the Complexity of the Multivariate Resultant, *Submitted*

[KPT] P. Koiran, N. Portier, S. Tavenas Polynomial identity testing using the Wronskian of the polynomial, *In preparation*

[CGKPS] A. Chattopadhyay, B. Grenet, P. Koiran, N. Portier, Y. Strozecki Polynomial identity testing using small valuations of the polynomial, *In preparation*