Abstracts from RIMS Workshop on Developments in Computer Algebra Research

Communicated by Akira Terui

The RIMS Workshop on Developments in Computer Algebra Research (https://sites.google.com/site/dcar2010/) has been held at Research Institute for Mathematical Sciences, Kyoto University, Kyoto, Japan, on July 7–9, 2010.

This workshop has been organized mainly for young researchers of computer algebra in Japan (besides another RIMS conference annually held that is one of the most traditional one in computer algebra community in Japan), for communicating new ideas, interaction with other research areas and/or sharing resource of research communications (including how to organize an international conference, as shown below). We had two invited talks as tutorials and 13 contributed talks which contain various topics in mathematics, physical and chemical sciences, engineering and informatics.

Following are the abstracts presented at the workshop. Full papers of contributed talks along with abstracts of tutorials will be published as Volume 1759 of “RIMS Kôkyûroku” (collection of research reports), which will also be accessible at Kyoto University Research Information Repository (KURENAI; http://hdl.handle.net/2433/24851).

1 Tutorials (invited talks)

Title: Towards a reliable computer algebraic system: dependability, usability and distributed processing
Speaker: Daisuke Ikegami (Information Technology Research Institute, AIST)

Computer algebraic systems (CASs) have a long history of being used for computation. One aspect of the systems which makes them powerful as a mathematical language is that they mix efficient algorithms with computation. Other is graphical user interfaces, literally. This talk is concerned related topics; dependability, usability, and distributed computations for CASs. To describe these features, I will introduce a modern programming language, called Haskell, and show what the language enables to work with CASs briefly.

Title: Holding International Scientific Meetings — A Case of CASC 2009 —
Speaker: Kosaku Nagasaka (Kobe University)

There are several international workshops, symposiums and conferences in Symbolic and Algebraic Computation hence holding such meetings in Japan is important especially for graduate students and young researchers. In this report, for potential local organizers in Japan, we describe backstage administration works on CASC 2009 from my experience (on behalf of the chair of local organizing committee of CASC 2009).
2 Contributed talks

Title: Computing Approximate Polynomial GCD over Integers via Various Matrices  
Speaker: Masaru Sanuki (University of Tsukuba)  
We study the computation of approximate polynomial GCD over integers, which is based on the lattice methods on several matrices such as the Bezout and the Hankel matrices. Additionally, we propose an optimization of “monic” approximate GCD over integers. We show that our methods are efficient.

Title: A Secret Sharing Scheme Using Rational Approximation  
Speaker: Hiroshi Kai (Ehime University)  
In this paper, a method to detect cheaters on the Shamir’s \((k, n)\) threshold secret sharing scheme is proposed using rational interpolation. When a rational interpolant is computed for \(l\) shares \(D_i, i = 1, \ldots, l\), where \(l > k\), then unattainable points of the rational interpolant may detect the cheaters.

Title: GPGCD, an Iterative Method for Calculating Approximate GCD, for Multiple Univariate Polynomials  
Speaker: Akira Terui (University of Tsukuba)  
We present an extension of our GPGCD method, an iterative method for calculating approximate greatest common divisor (GCD) of univariate polynomials, to multiple polynomial inputs. For a given pair of polynomials and a degree, our algorithm finds a pair of polynomials which has a GCD of the given degree and whose coefficients are perturbed from those in the original inputs, making the perturbations as small as possible, along with the GCD. In our GPGCD method, the problem of approximate GCD is transferred to a constrained minimization problem, then solved with the so-called modified Newton method, which is a generalization of the gradient-projection method, by searching the solution Newton iteratively. In this paper, we extend our method to accept more than two polynomials with the real coefficients as an input.

Title: On bit-size estimates of triangular systems  
Speaker: Eric Schost (University of Western Ontario, ORCCA Lab), Abdulilah Kadri (University of Western Ontario), Xavier Dahan (Kyushu University)  
When solving polynomial equations over an infinite field like \(Q\), in an exact manner, that is without approximation, coefficients usually become very large. This survey presents some upper-bounds on the size of coefficients of some specific Gröbner bases. They concern still quite limited families of such systems, but are among the first of this kind. A special emphasize is put on the element representation by a fundamental tool, height theory for measuring the complexity in term of space of a polynomial system.

Title: An algorithm of computing inhomogeneous differential equations for definite integrals  
Speaker: Hiromasa Nakayama, Kenta Nishiyama (Kobe University)  
We give an algorithm to compute inhomogeneous differential equations for definite integrals with parameters. The algorithm is based on the integration algorithm for \(D\)-modules by Oaku. The main tool of the algorithm is the Gröbner basis method in the ring of differential operators. We give
some examples of our algorithm which has been implemented as the package \texttt{nk\_restriction.rr} on the Risa/Asir.

Title: On the number of slack variables used in representation of semi-algebraic sets  
Speaker: Issei Yoshida (IBM Research - Tokyo)

In real algebraic geometry, slack variables play a fundamental role in transforming a semi-algebraic set into an algebraic set. Specifically, for a semi-algebraic set $S \subset \mathbb{R}^n$, there exists an algebraic set $\tilde{S} \subset \mathbb{R}^{n+k}$ such that the natural projection of $\tilde{S}$ onto $\mathbb{R}^n$ is $S$, where $k$ slack variables are used to convert inequalities to equations.

We consider the number of slack variables necessary for the transformation that corresponds to the auxiliary dimension $k$ in $\mathbb{R}^{n+k}$. In general such $k$ depends on the Boolean expression of a given semi-algebraic set. It is known that if a semi-algebraic set consists of only inequalities, then just one slack variable is sufficient for the transformation. We show that for a general semi-algebraic set expressed by a disjunctive normal form (DNF), $\lfloor \frac{m}{2} \rfloor$ variables are sufficient for the transformation where $m$ is the maximal number of inequalities appeared in a single conjunctive clause which comprises the DNF.

Title: About a parallel implementation of the polynomial interpolation method  
Speaker: Kinji Kimura (Kyoto University)

We propose an efficient method for parallel implementation of the Newton interpolation method. The first idea is use of inner product to reduce the number of modular arithmetic operations in the Newton interpolation over finite fields, and another one is a clever definition of the weight on the variables to reduce the number of evaluation points for the interpolation. As an application of the method, we show an efficient calculation of the discriminant of a polynomial of degree 27 with coefficients with 6 indeterminates, which appears in a problem in construction of elliptic curves.

Title: USB bootable KNOPPIX/Math/2010  
Speaker: Tatsuyoshi Hamada (Fukuoka University / JST CREST)

KNOPPIX/Math offers many documents and mathematical software packages. Once you run the live DVD system, you can enjoy a wonderful world of mathematical software without installing anything yourself. KNOPPIX/Math/2010, the newest one, supports to make a bootable USB-medium. In order to create a bootable USB-medium, the program “flash-knoppix” can be used on the running KNOPPIX/Math/2010 system. Having copied the system to USB-medium, you can store files permanently with the persistent KNOPPIX image in live mode. This paper is an introduction of how to make USB-KNOPPIX/Math.

Title: On the construction of Böttcher functions and visualization of Julia sets  
Speaker: Satoshi Yoshida, Masayo Fujimura, Yasuhiro Gotoh (National Defense Academy)

DEM (Distance Estimate Method) is an algorithm that draws the connected Julia set for quadratic maps $P_c(z) = z^2 + c$ introduced by Y. Fisher. We construct two revisions of DEM; the first one can be applied to the sequence of conformal maps $\varphi_n$, which converges to the Böttcher map $\varphi$, and the other one can be applied to disconnected Julia set. We implement these algorithms on Risa/Asir.

Title: Toward a Computer Algebra System for Electron Correlation Theory  
Speaker: Takeshi Osoekawa, Yuji Mochizuki, Kazuhiro Yokoyama (Rikkyo University)
The aim of this research is to develop a computer algebra system for quantum chemistry. The system is designed to manipulate algebraic formulas that appeared in electron correlation theory. We present the architecture of the system and the progress of the development in this paper. This paper also reports some benchmarks of the implementation of a module of the system.

Title: An improvement of Voloch’s rational point attack on improved algebraic surface cryptosystem
Speaker: Maki Iwami (Osaka University of Economics and Law)

There are trials to attack on improved algebraic surface cryptosystem (ASC07) such as rational point attack by Voloch and substitution of series solution by Iwami, but they are not effective because a certain polynomial has too many candidates and cannot be determined uniquely in the realistic calculation. In this paper, we try to improve these attacks. The idea is based on a monomial reduction which increases the number of the system of equations and decreases the number of candidates of a certain polynomial. It can be reduced to the combinatorial optimization problem by lattice basis reduction. Unfortunately, after further investigation, it was found that we couldn’t improve these attacks by the suggested algorithm because ASC07 has some conditional equations w.r.t. degrees in the public key and encryption step, and the restrictions prevent the suggested algorithm from increasing the number of the system of equations and decreasing the the number of candidates of a certain polynomial. However, we see that the suggested algorithm in this paper would be useful if there weren’t such a degree restriction in ASC07.

Title: Homomorphic Encryption and Approximate GCD of Integers and Polynomials over Integers
Speaker: Kosaku Nagasaka (Kobe University)

We briefly review the article published in Communications of the ACM, about homomorphic encryption and approximate GCD of integers, and a known algorithm for approximate GCD of polynomials over integers. Extending algorithms for polynomials over integers to integers by mapping the variable to the base number is not easy since the integer arithmetic causes carry and bellow digits while the polynomial arithmetic does not have this property. In this preliminary report, we introduce a way to overcome this problem.

Title: On the boundary polynomial
Speaker: Takuya Kitamoto (Yamaguchi University)

Recently, Computer algebra system (CAS) such as Maple, Mathematica is gaining its popularity in various fields of science, education and engineering. Symbolic computation, one of their features, provides us new applications of computer systems that conventional numerical packages can not. Control engineering, where unknown parameters play important roles as design parameters and uncertain indeterminates, has a lot of such applications.

In this paper, we define “boundary polynomial” and show its applications to the stability analysis of a control system. Given a system with a parameter $k$, roughly speaking, boundary polynomial is a polynomial of $k$ that vanishes when the system is on the verge of instability. The boundary polynomial has a close relationship with well-known “Hurwitz criterion” for the stability analysis, and can be used to compute the range of parameter $k$ where the system is stable.