ISSN 1880-2818

数理解析研究所講究録1759

RIMS共同研究

数式処理研究の新たな発展

京都大学数理解析研究所

2011年9月

RIMS Kôkyûroku 1759

Developments in Computer Algebra Research

July 7～9, 2010

edited by Akira Terui

September, 2011

Research Institute for Mathematical Sciences

Kyoto University, Kyoto, Japan

はじめに

筑波大学 数理物質科学研究科
照井　章

本講究録は，2010 年 7 月 7 日から 9 日にかけて，京都大学数理解析研究所で開催された RIMS 共同研究 “数式処理研究の新たな発展” の報告集である．

本共同研究は，数式処理（計算代数 [Computer Algebra] や，より広い意味で，計算機で数式・数学情報を扱う技術や方法論）の算法・システム開発・応用の各分野で活躍する研究者が，未解決問題の提起，萌芽的アイデアの紹介，最新の実装状況の報告，他分野との連携等に関する討論を行い，数式処理研究の今後の展望と方向性を検討することを目的として企画された．

数式処理に関する研究は，これまでに，数学，計算機科学に関連した分野で成果を挙げており，最近では，その成果が工学や生物学，教育等の分野にも広まりつつある．これら異分野との交流は，各分野に新しいテーマをもたらし，研究の幅を広げる有意義なものであり，研究交流の今後のさらなる発展が望まれている．本共同研究は，これら異分野の研究者と数式処理の若手研究者が，より密接に情報を共有し，研究の今後の展望と方向性を検討する機会になることを目指した．

本共同研究では，2 件のチュートリアルを企画した．池上大介氏には，“21 世紀の数式処理に対する三つの新機軸：ディペンダビリティ・ユーザビリティ・分散処理” と題し，関数型プログラミング言語 Haskell による数式処理の可能性について講演いただいた．長坂耕作氏には，“国際研究集会を開くまで — CASC 2009 開催までの道のり —” と題し，国際的な研究交流や情報発信の促進の観点から，国際研究集会の開催および運営の経験について講演いただいた．多忙な中講演をお引き受けいただき，有益な講演を下さった両氏に感謝する．

一般講演は，13 件の講演が行われた．内容は，数学，理工学，情報科学の各分野にわたり，活発な討論が行われた．講演者および討論に参加された共同研究参加者各位に感謝する．

京都大学数理解析研究所には，本共同研究の開催にあたり，研究協力者への旅費の助成や，共同研究開催への助力をいただいた．ここに感謝申し上げる．

Preface

This volume of collection of research reports contains invited and contributed papers which have been presented at the RIMS Workshop on Developments in Computer Algebra Research, held at Research Institute for Mathematical Sciences, Kyoto University, on July 7–9, 2010.

We have organized this workshop for examining prospects and future direction of computer algebra research through discussions on various topics, such as raising a new open problem, introduction of exploratory ideas, reporting latest implementation, application to other areas, by researchers in computer algebra and/or those who are working on algorithms, system developments and applications in handling mathematics or mathematical information on a computer in broader sense.

Researches on computer algebra have contributed new results in fields related to mathematics and computer science so far. Furthermore, recent development of researches have enlarged their focus to broader range of applications including engineering, biology, education. Such interaction brings new themes and broaden the scope of computer algebra research, thus it is desired to increase communication between researchers in computer algebra and application fields. Therefore, we have aimed to make this workshop an opportunity to share their research ideas more closely between especially young researchers in computer algebra and researchers from different fields to examine the prospects and future research directions.

In the workshop, a tutorial session was organized with two invited talks. Daisuke Ikegami presented his talk titled "Towards a reliable computer algebraic system: dependability, usability and distributed processing," discussing effectiveness of functional programming language Haskell in computer algebra. Kosaku Nagasaka presented his talk titled "Holding International Scientific Meetings — A Case of CASC 2009 —," discussing experience in holding and management of an international workshop from the viewpoint of promoting international research and information dissemination and exchange. We are grateful to both speakers for accepting our invitations and presenting valuable talks at the workshop.

We also had 13 contributed talks which contain various topics in mathematics, physical and chemical science, engineering and informatics, each of which followed by active discussions. Thanks to all the contributors for their talks and the participants for valuable discussions.

We also appreciate the Research Institute for Mathematical Sciences, Kyoto University for financial assistance of travel expense of contributors in part and other help for holding the workshop.

Akira Terui, *Organizer*
University of Tsukuba

RIMS共同研究

数式処理研究の新たな発展

日程: 2010年7月7日(水)13:30～7月9日(金)12:30
場所: 京都大学数理解析研究所 111号室 (京都市左京区北白川追分町)
研究代表者: 照井 章 (筑波大学 数理物質科学研究科)
Webサイト: http://sites.google.com/site/dcar2010/

プログラム

7月7日 (水)		
オープニング	13:30 ～ 13:35	
セッション1	13:40 ～ 14:20	種々の行列を利用した整数係数近似GCD計算法 讃岐 勝 (筑波大学)
	14:20 ～ 14:50	有理関数近似を用いた秘密分散法 甲斐 博 (愛媛大学)
	14:50 ～ 15:20	近似GCD算法GPGCDの複数入力多項式への拡張 照井 章 (筑波大学)
セッション2	15:40 ～ 16:40	What for, why and how to get bit-size estimates for polynomial systems over Q: a few answers Eric Schost (University of Western Ontario, ORCCA lab), Abdulilah Kadri (University of Western Ontario), Xavier Dahan (九州大学)
7月8日 (木)		
セッション3	9:30 ～ 10:10	積分の満たす非斉次微分方程式系を与えるアルゴリズム 中山洋将, 西山絢太 (神戸大学, JST CREST)
	10:10 ～ 10:50	半代数的集合から代数的集合への変換に伴うスラック変数の個数について 吉田一星 (日本アイ・ビー・エム(株) 東京基礎研究所)
セッション4	11:10 ～ 11:50	多項式補間法の並列実装について 木村欣司 (京都大学)
	11:50 ～ 12:20	USB起動 KNOPPIX/Math/2010 について 濱田龍義 (福岡大学 / JST CREST)
チュートリアル1	13:40 ～ 14:40	21 世紀の数式処理に対する三つの新機軸: ディペンダビリティ・ユーザビリティ・並列/並行計算 池上大介 (産業技術総合研究所)
チュートリアル2	15:00 ～ 16:00	国際研究集会を開くまで - CASC 2009 開催までの道のり - 長坂耕作 (神戸大学)
情報交換	16:00 ～ 16:30	国際会議等の情報交換

7月9日（金）		
セッション5	9:30 ～ 10:00	**Böttcher 関数の構成による Julia 集合の可視化** 吉田怜史, 藤村雅代, 後藤泰宏 (防衛大学校)
	10:00 ～ 10:40	**電子相関理論のための数式処理システムに向けて** 小副川健, 望月祐志, 横山和弘 (立教大学)
	10:40 ～ 11:10	**An improvement of Voloch's rational point attack on improved algebraic surface cryptosystem** 岩見真希 (大阪経済法科大学)
セッション6	11:30 ～ 12:00	**準同型暗号と整数及び整数多項式の近似GCD** 長坂耕作 (神戸大学)
	12:00 ～ 12:30	**境界多項式について** 北本卓也 (山口大学)

開催目的

本共同研究は、数式処理(計算代数 (Computer Algebra) や、より広い意味で、計算機で数式・数学情報を扱う技術や方法論)の算法・システム開発・応用の各分野で活躍する研究者が、未解決問題の提起、萌芽的アイデアの紹介、最新の実装状況の報告、他分野との連携等に関する討論を行い、数式処理研究の今後の展望と方向性を検討することを目的として開催するものです。

数式処理に関する研究は、これまでに、数学、計算機科学に関連した分野で成果を挙げており、最近では、その成果が工学や生物学、教育等の分野にも広まりつつあります。これら異分野との交流は、各分野に新しいテーマをもたらし、研究の幅を広げる有意義なものであり、研究交流の今後のさらなる発展が望まれます。

本共同研究では、これら異分野の研究者と数式処理の若手研究者が、より密接に情報を共有し、研究の今後の展望と方向性を検討することを目指します。

RIMS Workshop on

Developments in Computer Algebra Research

Date: from July 7, 2010, 13:30 to July 9, 2010, 12:30

Place: Room 111, Research Institute for Mathematical Sciences, Kyoto University, Kyoto, Japan

Organizer: Akira Terui (Graduate School of Pure and Applied Sciences, University of Tsukuba)

Web site: http://sites.google.com/site/dcar2010/

Program

Wednesday, July 7

Opening	13:30 ~ 13:35	
Session 1	13:40 ~ 14:20	**Computing Approximate Polynomial GCD over Z via Various Matrices** Masaru Sanuki (University of Tsukuba)
	14:20 ~ 14:50	**A Secret Sharing Scheme Using Rational Approximation** Hiroshi Kai (Ehime University)
	14:50 ~ 15:20	**GPGCD, an Iterative Method for Calculating Approximate GCD, for Multiple Univariate Polynomials** Akira Terui (University of Tsukuba)
Session 2	15:40 ~ 16:40	**What for, why and how to get bit-size estimates for polynomial systems over Q: a few answers** Eric Schost (University of Western Ontario, ORCCA lab), Abdulilah Kadri (University of Western Ontario), Xavier Dahan (Kyushu University)

Thursday, July 8

Session 3	9:30 ~ 10:10	**An algorithm of computing inhomogeneous differential equations for definite integrals** Hiromasa Nakayama, Kenta Nishiyama (Kobe University, JST CREST)
	10:10 ~ 10:50	**On the number of slack variables used in representation of semi-algebraic sets** Issei Yoshida (IBM Research - Tokyo, IBM Japan Ltd.)
Session 4	11:10 ~ 11:50	**About a parallel implementation of the polynomial interpolation method** Kinji Kimura (Kyoto University)
	11:50 ~ 12:20	**On USB bootable KNOPPIX/Math/2010** Tatsuyoshi Hamada (Fukuoka University / JST CREST)

Tutorial 1	13:40 ~ 14:40	**Towards a reliable computer algebraic system: dependability, usability, concurrent and parallel computation** Daisuke Ikegami (National Institute of Advanced Industrial Science and Technology (AIST))
Tutorial 2	15:00 ~ 16:00	**Holding International Scientific Meetings - A Case of CASC 2009 -** Kosaku Nagasaka (Kobe University)
Communication	16:00 ~ 16:30	Communication on information of international conferences, etc.

Friday, July 9		
Session 5	9:30 ~ 10:00	**On the construction of Böttcher functions and visualization of Julia sets** Satoshi Yoshida, Masayo Fujimura, Yasuhiro Gotoh (National Defense Academy)
	10:00 ~ 10:40	**Toward a Computer Algebra System for Electron Correlation Theory** Takeshi Osoekawa, Yuji Mochizuki, Kazuhiro Yokoyama (Rikkyo University)
	10:40 ~ 11:10	**An improvement of Voloch's rational point attack on improved algebraic surface cryptosystem** Maki Iwami (Osaka University of Economics and Law)
Session 6	11:30 ~ 12:00	**Homomorphic Encryption and Approximate GCDs of Integers and Polynomials over Integers** Kosaku Nagasaka (Kobe University)
	12:00 ~ 12:30	**On the boundary polynomial** Takuya Kitamoto (Yamaguchi University)

Aims and scope

We organize this workshop for examining prospects and future direction of computer algebra research through discussions on various topics, such as raising a new open problem, introduction of exploratory ideas, reporting latest implementation, application to other areas, by researchers in computer algebra and/or those who are working on algorithms, system developments and applications in handling mathematics or 'mathematical' informations on a computer in broader sense.

Researches on computer algebra have contributed new results in fields related to mathematics and computer science so far. Furthermore, recent development of researches have enlarged their focus to broader range of applications including engineering, biology, education. Such interaction brings new themes and broaden the scope of computer algebra research. Thus, it is desired to increase communication between researchers in computer algebra and application fields.

Therefore, this workshop aims to communicate between especially young researchers in computer algebra and researchers from different fields to share their ideas more closely to examine the prospects and future research directions.

数式処理研究の新たな発展

Developments in Computer Algebra Research

RIMS 共同研究報告集

２０１０年７月７日～７月９日

研究代表者　照井　章 (Akira Terui)

目　次