

数理解析研究所講究録 1268

代数系のアルゴリズムと計算論

京都大学数理解析研究所

2002年6月

まえがき

計算機科学との関わりの中で、代数系のアルゴリズムの重要性が認識され、国内外で関連した研究が活発になっている。代数系の一般的構造論のみならず、具体的計算アルゴリズムを念頭においた研究が盛んである。2001年2月20日～22日に京都大学数理解析研究所で行われた今回の研究集会では、代数、言語理論、暗号理論、計算理論に複合的に関連した広い分野の研究者が集まり、代数系のアルゴリズムの理論的側面と応用的側面からの研究発表が行われた。特に、代数系の組合せ手法による構造論、暗号理論・情報セキュリティへの応用、言語理論・オートマトン理論との関わり、NP問題を含む、計算の論理構造の問題について取り上げられ、活発な討論が行われた。

この報告集には、期間中発表された24件の講演から、22件の報告を収録している。今後のこの分野の研究の発展の一助になれば幸いである。

This volume, the proceedings of Algorithms in Algebraic Systems and Computation Theory, contains 21 articles which were presented in the meeting held from February 20 to 22, 2002 in Kyoto. They discuss subjects widely related to algebraic algorithms, such as cryptography, combinatorial techniques in algebra, formal languages, automata, and logic related to computation.

2002年5月 (May, 2002)

小林ゆう治 (Yuji Kobayashi)

東邦大学理学部 (Toho University)

代数系のアルゴリズムと計算論
Algorithms in Algebraic Systems and Computation Theory
研究集会報告集

2002年2月20日～2月22日
研究代表者 小林 ゆう治(Yuji Kobayashi)

目 次

1.	n-Insertion on Languages-----	1
	京産大・理	伊藤 正美(Masami Ito)
	京産大・理学	杉浦 亮(Ryo Sugiura)
2.	A Language Equation and Its Applications-----	7
	京産大・理	伊藤 正美(Masami Ito)
3.	Some Remarks on Sequence Design for DNA Computing (Abstract)-----	11
	電通大	小林 聡(Satoshi Kobayashi)
	”	近藤 朋大(Tomohiro Kondo)
4.	On Public-Key Cryptosystems against Chosen Cipertext Attack-----	17
	富士通研	小柴 健史(Takeshi Koshiba)
5.	A Parallelized Elliptic Curve Multiplication and its Resistance against Side-Channel Attacks-----	29
	富士通研	伊豆 哲也(Tetsuya Izu)
	ダルムシュタット工科大	高木 剛(Tsuyoshi Takagi)
6.	Formal Language Theoretical Approach to Secret Sharing Schemes-----	40
	通信総合研	山村 明弘(Akihiro Yamamura)
	”	滝澤 修(Osamu Takizawa)
7.	Remarks on locally inverse *-semigroups-----	47
	島根大・総合理工	今岡 輝男(Teruo Imaoka)
	”	藤原 浩示(Koji Fujiwara)
8.	THE NORMAL OPEN SET ALMOST EQUAL TO A REGULAR OMEGA LANGUAGE-----	50
	東邦大・理	竹内 泉(Izumi Takeuti)
9.	On cellular automata-----	59
	東洋大・工	佐藤 忠一(Tadakazu Sato)
10.	Graph Rewriting in Topology IV: Rewriting Based on Algebraic Operators-----	64
	ATR人間情報科学研	Jian-Qin Liu
	”	下原 勝憲(Katsunori Shimohara)
11.	LEXICOGRAPHIC GRÖBNER BASES OF TORIC IDEALS ARISING FROM ROOT SYSTEMS-----	73
	立教大・理	大杉 英史(Hidefumi Ohsugi)

1 2.	Numerical semigroups of toric type of higher dimension-----	77
	神奈川工大	米田 二良(Jiryō Komeda)
1 3.	Average number of connected components and free resolutions of Stanley-Reisner rings-----	81
	佐賀大・文化教育	寺井 直樹(Naoki Terai)
1 4.	On the Unit Group of a Semigroup Ring-----	97
	茨城大・理	松田 隆輝(Ryūki Matsuda)
1 5.	The word problem for the braid inverse monoid-----	105
	東邦大・理	稲田 勇(Isamu Inata)
	〃	片海 直樹(Naoki Kataumi)
	〃	飛田 享俊(Takatoshi Tobita)
1 6.	On the structure of weak interlaced bilattice $\mathcal{K}(L)$ -----	110
	島根大・総合理工	近藤 通朗(Michiro Kondo)
1 7.	λ -Calculus with Lazy Lists – Extended Abstract – -----	118
	島根大・総合理工	藤田 憲悦(Ken-etsu Fujita)
1 8.	Gödel's incompleteness theorem and forcing-----	126
	NTT	河野 泰人(Yasuhito Kawano)
1 9.	On Computable Tree Functions-----	138
	コンパクトコンピュータ(株)	木本 正裕(Masahiro Kimoto)
	国際基督教大	高橋 正子(Masako Takahashi)
2 0.	Model-robustness of equilibrium in game for modal logics-----	151
	茨城工業高専	松久 隆(Takashi Matsuhisa)
2 1.	Algorithmic Analysis of LS-systems: Solving the 3-SAT problems in a logarithmic space-----	155
	ATR人間情報科学研	Jian-Qin Liu
	〃	下原 勝憲(Katsunori Shimohara)
2 2.	On the Regularity of the Power Language of a Regular Language (Extended abstract)-----	156
	Eötvös Loránd Univ.	Sándor Horváth