

COE Lecture Note Series

Volume No. : 35

Title : 計算機代数システムの進展 Progress in Computer Algebra Systems

Editors : 横山俊一、夫 紀江、林 卓也

Written In : Japanese

ISSN : 1881-4042

Published In : 2011年11月30日

Contents:

8 月 29 日 (月) 計算機数論セッション

PARI-GP AND SOME PROBLEMS CONCERNING DISTRIBUTION OF NUMBER FIELDS
..... 1

木村 巖 (富山大学大学院理工学研究部)

Sage for Number Theorists 12

横山俊一 (九州大学数理学研究院) .

円文体の相対類数の高速計算 24

谷口哲也 (学習院大学 客員研究員)

ある2次無理数の連分数展開について 40

岸 康弘 (愛知教育大学教育学部)

Lehmerの5次多項式に関するいくつかの問題について 64

木田雅成 (電気通信大学数学教室)

数論システムNZMATHの使い方

巨大な自然数の高速計算にすぐ使えるプログラム 77

中村 憲 (首都大学東京理工学研究科)

8 月 30 日 (火) 計算機代数セッション

解析的既約曲線に付随する半群の計算アルゴリズム 90

渋田敬史 (立教大学/JST CREST)

Structure of lexicographic Gröbner bases in dimension zero 95

Xavier Dahan (九州大学数理学研究院)

グレブナー基底を用いたパラメトリック整数計画アルゴリズム 109

夫 紀恵 (東京大学情報理工学系研究科)

量子化学計算のための数式処理システムQC²AS の開発 122

小副川 健 (立教大学)

KNOPPIX/Math に見る数学ソフトウェアの世界 131
濱田龍義 (福岡大学 / JST CREST)

限量記号消去のアルゴリズムとその応用 135
穴井宏和 (株式会社富士通研究所 / マス・フォア・インダストリ研究所)

8 月 31 日 (水) 暗号・セキュリティセッション

数論アルゴリズムと暗号の安全性 160
伊豆哲也 (株式会社富士通研究所)

暗号システムの安全性証明とその自動化技術 185
花谷嘉一 (株式会社東芝 研究開発センター)

Bilinear Group に関する困難性仮定への攻撃導出 206
吉田真紀 (大阪大学大学院情報科学研究科)