Preface

Massimiliano Sala

In the period February–July 2006 a major research event took place in Linz (Austria): the Special Semester in Gröbner Bases and Related Areas.[1] Organized by RICAM (in close cooperation with RISC) and funded by the Austrian Academy of Sciences, it saw the involvement of hundreds of people working in Gröbner bases theory and their applications. In particular, a workshop (D1[2]) was held, co-chaired by Mikhail Klin (algebraic combinatorics), Ludovic Perret (cryptography) and me (coding theory). The aim of the workshop was twofold: to present possible applications of the theory to experts in Gröbner bases (so that they could explore new research fields) and to present Gröbner bases as an attractive tool to people working in other areas. Therefore, the invited talks were mainly tutorials and surveys, while posters and contributed talks outlined specific research results.

Workshop D1 was a success, with a large audience coming from different backgrounds. It was suggested that some[3] of the best D1 presentations related to cryptography and codes would be collected in a book of the RISC Book Series. The invited talks would become book *chapters*. The posters and contributed talks would become short *notes* at the end of the book. I was appointed Managing Editor, with an Editorial Board composed of Teo Mora (Gröbner bases related papers), Ludovic Perret (cryptography), Shojiro Sakata (AG codes) and Carlo Traverso (Gröbner bases and coding). To cover some interesting aspects not presented at Workshop D1, we invited a few more papers and notes.

I would like to thank all of them for their great help and assistance in planning, shaping and editing this book. The Board and I would like to express our gratefulness for their supervision to Bruno Buchberger and the series editor Peter Paule.

[1] http://www.ricam.oeaw.ac.at/specsem/srs/groeb/index.htm.

[2] "Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics".

[3] Other D1 presentations will appear in a special issue of Journal of Symbolic Computation, edited by D. Augot, J.-C. Faugère and L. Perret.

M. Sala
Univ. of Trento, Trento, Italy
e-mail: sala@science.unitn.it

http://www.springer.com/978-3-540-93806-4

Gröbner Bases, Coding, and Cryptography
Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.)
2009, XVI, 430 p.,
ISBN: 978-3-540-93806-4