Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Foreword

Daniel Augot[a], Jean-Charles Faugère[b], Ludovic Perret[b,1]

[a] *INRIA Saclay –Île-de, France*

[b] *SALSA Project, INRIA, Centre Paris-Rocquencourt, UPMC, Univ Paris 06, LIP6, CNRS, UMR 7606, LIP6, 104, avenue du Président Kennedy, 75016 Paris, France*

ARTICLE INFO

Article history:
Received 3 November 2008
Accepted 3 November 2008
Available online xxxx

This issue of the Journal of Symbolic Computation is a follow-up event of the successful workshop D1[2] "Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics" of the Special Semester on Gröbner Bases and Related Methods,[3] supported by the RICAM Institute of the Austrian Academy of Science in Linz and held at RICAM and at the RISC Institute of the Johannes Kepler University in Hagenberg, April 30–May 06, 2006. Bruno Buchberger and Heinz Engl organized the Special Semester, which resulted in a series of meetings and events from February to July 2006.

This special issue aims at offering a selection of research articles deploying algebraic techniques in coding theory or cryptography. We hope that this selection of articles will illustrate the benefits of using standard techniques of symbolic computation in applicative domains such as coding theory and cryptography. Besides, we believe that such domains of applications give raise to new and challenging problems for the symbolic computation community.

Gröbner bases have become a major tool for dealing with algebraic equations over finite fields, or for describing ideals over these fields. This has been demonstrated by the development of the so-called algebraic attacks in cryptography, and by the use of Gröbner solving tools for decoding algebraic codes.

E-mail addresses: Daniel.Augot@inria.fr (D. Augot), Jean-Charles.Faugere@inria.fr (J.-C. Faugère), ludovic.perret@lip6.fr (L. Perret).

URLs: http://www-rocq.inria.fr/~augot (D. Augot), http://fgbrs.lip6.fr/jcf/ (J.-C. Faugère), http://www-salsa.lip6.fr/~perret/ (L. Perret).

[1] Tel.: +33 1 44 27 88 35; fax: +33 1 44 27 75 41.

[2] Another publication related to D1 is a book "Bases, Coding, and Cryptography", RISC Book Series, edited M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso.

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

0747-7171/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.11.004

In these two domains, the approach is the same: model the problem, transform it into a system of algebraic equations; then apply a symbolic method for solving (or evaluating the difficulty of solving) the system of equations. Very often the solving step is not straightforward. To make the computation efficient, we usually have to deeply study the structural properties of the systems (using symmetries for instance). In addition, you have also to check the consistency of the zeros of the algebraic system with respect to the desired solutions of the natural problem. Of course, all these steps must be constantly checked against the natural problem, which in many cases serves as lantern to guide the researcher for finding an efficient method for solving the algebraic system.

In *Coding Theory*, there are two major goals: construction of good codes, that is to say codes which both are large and have a large correction capacity (minimum distance); the second goal is to design algorithms for decoding efficiently existing error correcting codes. Boucher and Ulmer have followed the trend of constructing good codes. To do so, they have used skew polynomials and they found a $[38, 19, 11]_4$ self dual codes which improves on previously known records. Note that finding such self dual codes over $GF(4)$ is longstanding problem which relates to combinatorics. Here Gröbner bases are an ingredient for finding the generator polynomial of these codes.

In the context of decoding, another trend has been followed by Augot, Bardet and Faugère and Bulygin and Pellikaan. They both try to write the decoding problem of codes (which is well known to be a difficult one) in terms of algebraic systems. Augot et al. technique relies on Newton's identities for writing the algebraic system, while Bulygin and Pellikaan use determinantal ideals. Both methods are heavily related on the efficiency of algorithms for computing Gröbner bases to recover the original message.

Still in the decoding domain, a big boom in coding theory was the introduction of the Guruswami–Sudan list decoding algorithm, which has a large decoding radius. This algorithm applies to the classical Reed–Solomon codes, but also to more elaborate algebraic-geometry codes. But this algorithm is described in general terms, and suffers of a complexity penalty. Both Das and Sikdar, and Lee and O'Sullivan use the theory of Gröbner bases for the Guruswami–Sudan algorithm for AG codes: Das and Sikdar for long codes which are asymptotically good, and Lee and O'Sullivan for the quite popular Hermitian codes.

In *Cryptography*, the situation is very similar : we have mainly two faces of Gröbner bases: the positive (design of new cryptosystems), and a darkest part (attacks of cryptosystems).

Multivariate public key cryptosystems are a target of choice for Gröbner bases. A multivariate public key cryptosystem is a cryptographic primitive whose public key is given by a system of algebraic equations. To encrypt, we have simply to evaluate the message on the polynomials of public key. To attack the system, you have then to solve an algebraic system derived from the polynomials of the public key. Faugère and Perret have investigated the security of a multivariate public key cryptosystem whose public polynomials are obtained from the composition of two systems of quadratic equations. An algorithm for decomposing a system of multivariate polynomials of an arbitrary degree is described in Faugère and Perret ; in a second step, applying this general method lead to an efficient attack against the scheme considered.

In cryptanalysis, a fundamental problem is to find the cost of solving the discrete logarithm problem over various abelian varieties over finite fields. Gaudry addresses this problem using the well known index calculus principle, but dealing with a special representation of the abelian variety based on triangular sets. Also, index calculus relies on finding relations, that is to say, decomposing random elements of the group into the factor base, whose elements are defined using these triangular sets. In Gaudry's approach, decomposition is obtained by a Gröbner basis computation (for each relation to be found). For some elliptic curves and hyperelliptic curves, this method improves on previous results.

On the other face, Gröbner bases theory can be also used to design secure cryptographic systems. A notable example is Berbain, Gilbert and Patarin. They proposed a stream cipher whose security is proven to be related to the difficulty of solving a generic system of overdetermined quadratic equations. This is a major breakthrough in the design of schemes based on multivariate polynomials which were so far mainly based on heuristic arguments.

All the submissions were reviewed by experts in the relevant areas and according to the usual JSC refereeing process; papers submitted by the guest editors have been referred under the supervision of the journal editor-in-chief . We want to thank the reviewers for their help in providing timely and informative feedback to the authors.

Last, but not least, we would like to express our thanks to Bruno Buchberger, and all the members of the scientific board of the Special Semester, for having included an event related to Cryptography and Coding Theory. This was an important step toward the development of these areas.

Please cite this article in press as: Augot, D., et al., Foreword. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.11.004