ON THE COMPLEXITY OF COMPUTING GRÖBNER BASES IN CHARACTERISTIC 2

Vincenzo Acciaro

TR-232, DECEMBER 1993

School of Computer Science, Carleton University
Ottawa, Canada, KIS 5B6

On the complexity of computing Gröbner Bases in characteristic 2

Vincenzo Acciaro*†

Abstract

The computation of a Gröbner basis over a field F is characterized by a space complexity which grows doubly exponentially with the number of variables. Existing proofs of this fact use nonelementary results from commutative algebra and algebraic geometry. In this paper we use an elementary argument to show that, when $char(F) = 2$, and the number of variables is unbounded, the problem of computing a Gröbner basis is NP-hard.

1 Introduction

Let $f_1, \ldots, f_k$ polynomials in the polynomial ring $F[x_1, \ldots, x_n]$, over an arbitrary field F. Let $(f_1, \ldots, f_k)$ denote the ideal generated by $f_1, \ldots, f_k$ – we recall that it consists of all the linear combinations of $f_1, \ldots, f_k$ with coefficients in $F[x_1, \ldots, x_n]$:

$$(f_1, \ldots, f_k) := \{\sum_{i=1}^{k} f_i h_i \ \mid \ h_i \in F[x_1, \ldots, x_n]\}$$

A well known algorithm, due to Buchberger [3, 2], allows one to construct a standard basis for the ideal I generated by $f_1, \ldots, f_k$ in $F[x_1, \ldots, x_n]$. This basis is known as a *Gröbner basis* for the ideal, and, among other things, it allows us to answer in polynomial time the following decision problem [3]:

ideal membership: *does $g \in F[x_1, \ldots, x_n]$ belong to I?*

*School of Computer Science, Carleton University, Ottawa, ONT, K1S 5B6, Canada.
†Research supported in part by NSERC Grant A2415

Unfortunately, the space requirement for the computation of a Gröbner basis grows, in the worst case, doubly exponentially in n, the number of variables [2, pp. 511–514].

The existing complexity analyses – for fields of characteristic 0 or p – use methods from algebraic geometry and commutative algebra.

We shall show below that, when F is a field of characteristic 2, a very simple argument can be given to prove that the ideal membership problem is NP-hard, and hence that the computation of Gröbner bases is also NP-hard.

2 The result

We recall some concepts from the theory of Boolean algebras.

A ring $(R, +, \cdot)$ is called a *Boolean ring* if, for all $a \in R : a^2 = a$; that is, each element of R is an idempotent. It can be shown that any finite boolean ring is commutative, has characteristic 2, and is isomorphic to Z_2^k, for some positive integer k, where Z_2 denotes the ring of residue classes modulo 2.

A distributive lattice $(R, \vee, \wedge)$ is called a *Boolean algebra* if it has a zero element, denoted by $\hat{0}$, a unity element, denoted by $\hat{1}$, and every element of R has a complement. It can be shown [4, p.192] that:

LEMMA 1 *Given a Boolean algebra $(R, \vee, \wedge)$ we can associate to it a Boolean ring $(R, +, \cdot)$ by letting $a + b := (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$ and $a \cdot b := a \wedge b$, for all $a, b \in R$. Conversely, to any Boolean ring $(R, +, \cdot)$ it is possible to associate a Boolean algebra $(R, \vee, \wedge)$ by letting $a \vee b := a + b + a \cdot b$ and $a \wedge b := a \cdot b$.*

The previous lemma easily implies that $\hat{0} = a \wedge \overline{a}$ corresponds to 0, and $\hat{1} = a \vee \overline{a}$ corresponds to 1.

A Boolean algebra $(B, \vee, \wedge)$ is said to be *free of rank n* if it contains n elements $y_1, \ldots, y_n$ and each element of B can be written in one and only one way in disjunctive normal form:

$$(y'_{1,1} \wedge \ldots \wedge y'_{n,1}) \vee \ldots \vee (y'_{1,m} \wedge \ldots \wedge y'_{n,m})$$

where $m = 2^n$ and, for each i and j, either $y'_{i,j} = y_i$ or $y'_{i,j} = \overline{y_i}$. In particular, $|B| = 2^{2^n}$.

An expression $S(y_1, \ldots, y_n)$ obtained by recursively applying the operations $\vee, \wedge$ and $\overline{}$ to the free generators $y_1, \ldots, y_n$ is called a *Boolean expression* in the variables $y_1, \ldots, y_n$. Two Boolean expression are considered equal if they can be represented in the same disjunctive normal form.

When we let $\vee$ stand for *logical or*, $\wedge$ stand for *logical and*, and $\overline{}$ stand for *logical negation* we obtain the familiar *algebra of propositions.*

Let $S_3(y_1, \ldots, y_n) \in B$ be an expression of the form:

$$S_3(y_1, \ldots, y_n) = (v_{1,1} \vee v_{1,2} \vee v_{1,3}) \wedge \ldots \wedge (v_{m,1} \vee v_{m,2} \vee v_{m,3})$$

where $v_{i,j} \in \{y_1, \ldots, y_n, \overline{y_1}, \ldots, \overline{y_n}\}$. The 3-Satisfability Problem (3-SAT) asks for an assignment of truth values to the boolean variables $y_1, \ldots, y_n$ which makes $S_3(y_1, \ldots, y_n)$ true. It is well known that 3-SAT is NP-complete [1, p. 384].

Using Lemma 1 and the embedding $y_i \mapsto x_i$, we can associate to $S_3(y_1, \ldots, y_n)$ a polynomial $f(x_1, \ldots, x_n)$ over $GF(2)$, the Galois field of 2 elements.

It is easy to see that $S_3(y_1, \ldots, y_n)$ is satisfiable if and only if $f(x_1, \ldots, x_n) = 1$ is solvable in $GF(2)$, since the element associated to $\hat{1}$ the *tautology of* B, is 1, the *identity of* $GF(2)$, and the element associated to $\hat{0}$, the *contradiction of* B, is 0, the *zero element of* $GF(2)$.

We need now a standard result from commutative algebra [6, p.157]:

LEMMA 2 *Let* $f_1, \ldots, f_k \in F[x_1, \ldots, x_n]$, *Then* $1 \in (f_1, \ldots, f_k)$ *if and only if the system of polynomial equations* $\{f_1 = 0, \ldots, f_k = 0\}$ *admits no solution in* $\overline{F}$, *the algebraic closure of* F.

On the other hand $f(x_1, \ldots, x_n) = 1$ is solvable $GF(2)$ if and only if:

$$f(x_1, \ldots, x_n) = 1, x_1^2 - x_1, \ldots, x_n^2 - x_n$$

has solution in $\overline{GF(2)}$, since

$$(\alpha \in \overline{GF(2)} \text{ and } \alpha^2 = \alpha) \Rightarrow \alpha \in GF(2)$$

Therefore, by Lemma 2, the equation $f(x_1, \ldots, x_n) = 1$ is solvable $GF(2)$ if and only if:

$$1 \notin (f(x_1, \ldots, x_n) - 1, x_1^2 - x_1, \ldots, x_n^2 - x_n) \tag{1}$$

that is, the ideal generated by:

$$f(x_1, \ldots, x_n) - 1, x_1^2 - x_1, \ldots, x_n^2 - x_n \tag{2}$$

is not the full ring $F[x_1, \ldots, x_n]$. Since the Boolean expression S_3 can be mapped to the string (2) in linear time and space, we have proved that:

3-SAT *is reducible to* **ideal membership in characteristic 2**

Therefore the ideal membership problem in characteristic 2 is NP-hard.

3 Conclusion

How does the result of the previous Section relate to the complexity of Buchberger's algorithm? To test if (1) holds we apply the Gröbner basis algorithm, giving as input the string (2). The basis returned consists of the element 1 alone if and only if the original formula is not satisfiable. This proves the reduction:

3-SAT *is reducible to* **Gröbner Bases in characteristic 2**

and therefore shows that, for an unbounded number of variables, the computation of Gröbner bases in characteristic 2 is NP-hard.

Acknowledgements

The author wishes to thank Prof. J.D. Dixon for his invaluable advice and extremely helpful comments.

References

[1] A.V. Aho, J.E. Hopcroft, J.D. Ullman, *The design and analysis of computer algorithms,* Addison-Wesley Inc., Reading, Mass., 1974.

[2] T. Becker, V. Weispfenning, *Gröbner Bases, A Computational Approach To Commutative Algebra,* Springer-Verlag, Berlin, 1993.

[3] B. Buchberger, 'Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory', in *Recent Trends in Multidimensional System Theory,* (N.K. Bose ed.), D. Reidel Publ. Comp., 1985.

[4] L. Di Martino, M.C. Tamburini, *Appunti di algebra,* CLUED, Milano, 1984.

[5] S. Lang, *Algebra,* Addison-Wesley Inc., Reading, Mass., 1993.

[6] B.L. van der Waerden, *Algebra, volume 2,* Springer-Verlag, Berlin, 1991.

TR-210 **Sorting Permutations with Networks of Stacks**
M.D. Atkinson, August 1992

TR-211 **Generating Triangulations at Random**
Peter Epstein and Jörg-Rüdiger Sack, August 1992

TR-212 **Algorithms for Asymptotically Optimal Contained Rectangles and Triangles**
Evangelos Kranakis and Emran Rafique, September 1992

TR-213 **Parallel Algorithms for Rectilinear Link Distance Problems**
Andrzej Lingas, Anil Maheshwari and Jörg-Rüdiger Sack, September 1992

TR-214 **Camera Placement in Integer Lattices**
Evangelos Kranakis and Michel Pocchiola, October 1992

TR-215 **Labeled Versus Unlabeled Distributed Cayley Networks**
Evangelos Kranakis and Danny Krizanc, November 1992

TR-216 **Scalable Parallel Geometric Algorithms for Coarse Grained Multicomputers**
Frank Dehne, Andreas Fabri and Andrew Rau-Chaplin, November 1992

TR-217 **Indexing on Spherical Surfaces Using Semi-Quadcodes**
Ekow J. Otoo and Hongwen Zhu, December 1992

TR-218 **A Time-Randomness Tradeoff for Selection in Parallel**
Danny Krizanc, February 1993

TR-219 **Three Algorithms for Selection on the Reconfigurable Mesh**
Dipak Pravin Doctor and Danny Krizanc, February 1993

TR-220 **On Multi-label Linear Interval Routing Schemes**
Evangelos Kranakis, Danny Krizanc, and S.S. Ravi, March 1993

TR-221 **Note on Systems of Polynomial Equations over Finite Fields**
Vincenzo Acciaro, March 1993

TR-222 **Time-Message Trade-Offs for the Weak Unison Problem**
Amos Israeli, Evangelos Kranakis, Danny Krizanc and Nicola Santoro, March 1993

TR-223 **Anonymous Wireless Rings**
Krzysztof Diks, Evangelos Kranakis, Adam Malinowski, and Andrzej Pelc, April 1993

TR-224 **A consistent model for noisy channels permitting arbitrarily distributed substitutions, insertions and deletions**
B.J. Oommen and R.L. Kashyap, June 1993

TR-225 **Mixture Decomposition for Distributions from the Exponential Family Using a Generalized Method of Moments**
S.T. Sum and B.J. Oommen, June 1993

TR-226 **Switching Models for Non-Stationary Random Environments**
B. John Oommen and Hassan Masum, July 1993

TR-227 **The Probability of Generating Some Common Families of Finite Groups**
Vincenzo Acciaro, September 1993

TR-228 **Power Roots of Polynomials over Arbitrary Fields**
Vincenzo Acciaro, September 1993

TR-229 **Optimal Parallel Algorithms for Direct Dominance Problems**
Amitava Datta, Anil Maheshwari and Jörg-Rüdiger Sack, October 1993

TR-230 **Uniform Generation of Forests of Restricted Height**
M.D. Atkinson and J.-R. Sack, October 1993

TR-231 **Optimal Elections in Labeled Hypercubes**
Paola Flocchini and Bernard Mans, December 1993