A Parallel Approach to the Minimal Involutive Basis Algorithm

Vladimir A. Mityunin
Moscow State University
Department of Mechanics and Mathematics
Laboratory of Computing Methods
Vorobjovy Gory, Moscow, 119899, Russia
vmit@metric.ru

Alexandr S. Semenov
Moscow State University
Department of Mechanics and Mathematics
Laboratory of Computing Methods
Vorobjovy Gory, Moscow, 119899, Russia
semyonov@mccme.ru

ABSTRACT

In the paper [2] the probabilistic algorithm to obtain the reduced Gröbner Basis of an algebraic ideal over the ring of integers was presented. This algorithm leaves a place for a possibility that the basis obtained is not valid Gröbner one (with certain, but very small probability). The idea behind is to perform computation of the reduced Gröbner Basis for the integer ideal I and for its projection I_p over the modular field Z_p simultaneously. If one obtains zero as the reduction result in the modular case, the integer reduction can be omitted. In this paper this idea was extended for the Minimal Involutive Basis algorithm [4, 5]. Using the method described in [2], it was shown that this algorithm is also inherently sequential. The results obtained were compared with the results of [9, 10]. This work is the extension of the paper [6]

1. INTRODUCTION

In this work an attempt to parallelize the algorithm of computation of the minimal involutive bases is presented. In the paper [2] J.C.Faugère has shown that the task of the standard basis computation is inherently sequential and, therefore, every attempt to parallelize it essentially breaks the original algorithm. The main reason is that the result of the polynomial reduction often depends on the other polynomials, in particular on the last reduced one.

In integer computations probabilistic approach plays a significant role. The word "probabilistic" means that after termination of the algorithm it is necessary to check whether the obtained polynomial system is the standard basis of the initial ideal. In the case of the failure the standard basis construction algorithm should be run again.

In this paper a pseudo-probabilistic Faugère-style version of the computation method of the minimal involutive basis of the ideal is presented. For example it is necessary to execute the Minimal Involutive Basis algorithm [4, 5] on an integer system. Usually most of the time will be spent in the involutive reductions of the unnecessary polynomials (which have zeros as normal form). Instead of the true integer computation its modular analog can be performed and some hints on the redundant involutive prolongations can be obtained. Having the modular involutive reduction protocol the corresponding integer involutive reductions can be performed step by step. This algorithm is not correct everywhere, however, it gives the valid minimal involutive basis with very high probability. Upon completion of this part one have to check the involutive basis property. In the case of failure it is necessary to perform the slow integer computation.

Surprisingly, for most systems it is possible to obtain a correct minimal involutive basis using this method without slow integer computation and in many cases the check phase is very quick, and the parallel checking using all available processors is also possible. The detailed analysis shows that the involutive reduction of the redundant prolongations (the prolongations with zero normal form) takes a lot of running time. The only way to eliminate them correctly is to use criteria, for example described in papers [3, 1], but some zero prolongations will be undetected. For the integer computations, the cost of one involutive reduction is rather expensive, and the elimination of the redundant prolongations is very important.

Let I be an initial integer polynomial system and I_p its modular projection. The algorithm consists of three steps:

- Sequential calculation of the minimial involutive basis of I_p and recording the non-zero involutive reductions into the list RL
- Parallel re-execution of RL-reductions on the set I and construction of the integer system $RL(I)$
- Parallel checking whether $RL(I)$ is an involutive basis of the initial ideal

The results of the theoretical estimation of the maximum possible parallelization quality for number of test systems are presented. This is done using Faugère's technique, for detailed description refer to [2].

The program complex [8], [7] supports both integer and modular bases computations. It is implemented using Microsoft Visual C++ 6.0 and can be easily ported. Parallelization is supported by means of the MPI 1.1 standard.

2. REFERENCES

[1] J. Apel and R. Hemmecke, *Detecting unnecessary reductions in an involutive basis computation*, Risc linz report series 02-22, Research Institute for Symbolic Computation, Johannes Kepler Universität, 4040 Linz, Austria, Europe, October 2002, Appeared also as SFB F013 Report 02-13.

[2] J. C. Faugère, *Parallelization of Gröbner basis*, Proceedings of PASCO 1994, World Scientific Publ. Comp., 1994.

[3] V. P. Gerdt, *Involutive division technique: Some generalizations and optimizations*, Journal of Mathematical Sciences **108** (2002), no. 6, 1034–1051.

[4] V. P. Gerdt, Yu. A. Blinkov, and D. A. Yanovich, *Computation of Janet bases. i. monomial bases*, Computer Algebra in Scientific Computing / CASC 2001 (Berlin) (V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, eds.), Springer-Verlag, pp. 233–247.

[5] ———, *Computation of Janet bases. ii. polynomial bases*, Computer Algebra in Scientific Computing / CASC 2001 (Berlin) (V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, eds.), Springer-Verlag, pp. 249–263.

[6] V.A. Mityunin and A.S. Semenov, *An estimation of the parallelization quality of the involutive basis computation algorithm*, Proc. of CASC'2002 (Garching, Germany) (V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov, eds.), Technische Universität München, 2002, pp. 221–226.

[7] ———, *Parallel implementation of honey strategy Buchberger algorithm*, Proc. of Workshop on Under- and Overdetermined Systems of Algebraic or Differential Equations (Karlsruhe, Germany) (J. Calmet, M. Hausdorf, and W.M. Seiler, eds.), 2002, pp. 221–225.

[8] V.A. Mityunin, A.I. Zobnin, A.I. Ovchinnikov, and A.S. Semenov, *Involutive and classical Gröbner bases construction from the computational viewpoint*, Proc. of CAAP'2001 (Dubna, Russia) (V.P. Gerdt, ed.), Dubna JINR, 2002, pp. 221–230.

[9] D. A. Yanovich, *On parallelization of involutive Janet bases construction algorithm*, Programming and Computer Software **27** (2001).

[10] ———, *Parallelization of an algorithm for computation of involutive Janet bases*, Programming and Computer Software **28** (2002), no. 2.