Involutive Bases as a Tool for Multivariate Polynomials over Finite Fields

Vladimir P.Gerdt

Laboratory of Information Technologies, Joint Institute for Nuclear Research
141980 Dubna, Russia
gerdt@jinr.ru

Abstract

Being the most universal algorithmic tool in investigating and solving systems of multivariate polynomial systems over finite fields, Gröbner Bases, along with the characteristic set method [1], revealed in the first decade of the 21st century their practicality in algebraic cryptanalysis (see [2, 3, 4] and references therein).

The main topic of this talk is Involutive Bases [5] whose origin goes back to the algebraic analysis of systems of partial differential equations [6]. Whereas Gröbner Bases are defined and algorithmically characterized in terms of the conventional monomial division, Involutive Bases are based on the concept of involutive monomial division which is a certain restriction of the conventional division. Due to this restriction an Involutive Basis is generally a superset of the Gröbner Basis, and the latter can be extracted from the former without any extra computation costs [5]. Important features of the Involutive Basis approach is uniqueness of the reduction process and weak dependence on the criteria for detection of useless reductions.

Two specific Involutive Bases called after French mathematicians Janet and Pommaret are to be discussed in details and their application to Boolean multivariate polynomial systems (i.e. over $\mathbb{F}_2$) is to be considered. Although, Janet and Pommaret divisions are distinct, both involutive bases are identical [7]. Unlike any other known algorithmic methods, Boolean Pommaret/Janet Bases, and hence Boolean Gröbner bases can be constructed [8] directly in the underlying Boolean ring without extension of the initial set of Boolean polynomials with quadratic field binomials.

Another attractive feature of Boolean Involutive Bases is their suitability for the counting variant for Boolean polynomials (#SAT) which is $\#\mathcal{P}-$complete. This makes these bases appropriate for simulation of quantum computation on a classical computer. Thus for a quantum circuit built out of the three-qubit Toffoli and one-qubit Hadamard gates, which form a universal gate basis, construction of the circuit unitary matrix fully defining quantum computation is reduced to counting solutions to systems of Boolean polynomials [9].

In the talk we give the cardinality bounds for Boolean Gröbner and also for Janet/Pommaret Bases and explicit formula for the Hilbert function of an ideal in a Boolean ring in terms of the Involutive Basis of the ideal. The current implementation of involutive algorithms for Boolean rings will be illustrated by some standard SAT benchmarks [10] and compared with PolyBoRi 0.6.1 [11] and FGb 1.46 for Maple [12].

References

[1] X.-S.Gao and Z.Huang. *Efficient Characteristic Set Algorithms for Equation Solving in Finite Fields and Application in Analysis of Stream Ciphers*. Cryptology ePrint Archive, 2009/637.

[2] J.-C.Faugère and A.Joux. *Algebraic Cryptanalysis of Hidden Field Equations (HFE) Using Gröbner Bases*. LNCS 2729, Springer-Verlag, 2003, pp.44–60.

[3] J.-C.Faugère. *Interaction between Computer Algebra (Gröbner Bases) and Cryptology*. Proceedings of ISSAC 2009, ACM Press, pp.383–384.

[4] C.Cid and R.-P.Weinmann. *Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases*. Gröbner Bases, Coding, and Cryptography. Springer-Verlag, 2009, pp.307–366.

[5] V.P.Gerdt. *Involutive Algorithms for Computing Gröbner Bases*. Computational Commutative and Non-Commutative Algebraic Geometry. NATO Science Series, IOS Press, 2005, pp. 199–225. arXiv:math.AC/0501111

[6] W.M.Seiler. *Involution: The Formal Theory of Differential Equations and its Applications in Computer Algebra*. Algorithms and Computation in Mathematics 24, Springer, 2010.

[7] V.P.Gerdt. *On the Relation Between Pommaret and Janet Bases*. Computer Algebra in Scientific Computing / CASC 2000. Springer-Verlag, Berlin, 2000, pp.164-171.

[8] V.P.Gerdt and M.V.Zinin. *A Pommaret Division Algorithm for Computing Gröbner Bases in Boolean Rings*. Proceedings of ISSAC 2008, ACM Press, pp.95–102.

[9] C.M.Dawson, H.L.Haselgrove, A.P.Hines, D.Mortimer, M.A.Nielsen and T.J.Osborne. *Quantum computing and polynomial equations over the finite field Z_2*. arXiv:quant-ph/0408129

[10] `http://www.satlib.org/`

[11] `http://polybori.sourceforge.net/`

[12] `http://www-calfor.lip6.fr/~jcf/Software/FGb/`