Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Parametric Polynomial Systems"*

Comprehensive Gröbner systems over finite fields

Ryoya Fukasaku[1]***, Yasuhiko Ikematsu***[2] [fukasaku@math.kyushu-u.ac.jp]

[1] Faculty of Mathematics, Kyushu University, Fukuoka, Japan
[2] Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan

A comprehensive Gröbner system (CGS) is a powerful tool for handling a parametric polynomial system, and plays a role as a Gröbner basis (GB) of a parametric polynomial ideal. By the algorithm introduced in [6] together with its improvements achieved in [3, 4, 5], it is now possible to build an efficient program for computing CGSs. So we have several its application programs. For example, a program for computing CGSs over an infinite field is applied to a real quantifier elimination program such as the one introduced in [2].

Since the theory of GBs allows us to analyze the algebraic structure of a given polynomial system, it is used in the security evaluation of multivariate public key cryptography (MPKC). In MPKC, a parametric polynomial system $\mathcal{P}$ over a finite field is constructed in some way, and a public key is generated by substituting random numbers r into the parameters of $\mathcal{P}$. Then a public key $\mathcal{P}(r)$ is a (non-parametric) polynomial system and varies with the value of r. The security of MPKC is analyzed by computing GBs of $\mathcal{P}(r)$ for some r. However, to our best knowledge, there has been no study to analyze the parametric polynomial system $\mathcal{P}$. We believe that we provide a new perspective in security evaluation of MPKC by computing a CGS of $\mathcal{P}$. Therefore, it is important to be able to compute CGSs over finite fields.

In this talk, we report on our program for computing CGSs over finite fields.

Keywords
Comprehensive Gröbner systems, Multivariate public key cryptography, Finite fields

References
[1] J. DING; A. PETZOLDT; D.S. SCHMIDT, Multivariate Public Key Cryptosystems, Second Edition, Springer, 2020.
[2] R. FUKASAKU; H. IWANE; Y. SATO, Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2015*, pp. 173–180, ACM, 2015.
[3] D. KAPUR; Y. SUN; D. WANG, A New Algorithm for Computing Comprehensive Gröbner Systems. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2010*, pp. 29–36, ACM, 2010.
[4] Y. KURATA, Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation. *Communications of the Japan*

Society for Symbolic and Algebraic Computation, Vol. 1, pp. 39–66, JSSAC, 2011.
[5] K. NABESHIMA, Stability Conditions of Monomial Bases and Comprehensive Gröbner systems. *Lecture Notes in Computer Science*, Vol. 7442, pp. 248–259, Springer, 2012.
[6] A. SUZUKI; Y. SATO, A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2006*, pp. 326–331. ACM, 2006.