Solving Systems of Algebraic Equations Over Finite Commutative Rings and Applications

Hermann Tchatchiem Kamche
hermann.tchatchiem@gmail.com

Join work with: Hervé Talé Kalachi

LAGA Seminar 2024 (www.eral-cm.org)

Abstract: Several problems in algebraic geometry and coding theory over finite rings are modeled by systems of algebraic equations. Among these problems, we have the rank decoding problem, which is used in the construction of public-key cryptosystems. A finite chain ring is a finite ring admitting exactly one maximal ideal and every ideal being generated by one element. In 2004, Nechaev and Mikhailov proposed two methods for solving systems of polynomial equations over finite chain rings. These methods used solutions over the residue field to construct all solutions step by step. However, for some types of algebraic equations, one simply needs partial solutions. In this paper, we combine two existing approaches to show how Gröbner bases over finite chain rings can be used to solve systems of algebraic equations over finite commutative rings. Then, we use skew polynomials and Plücker coordinates to show that some algebraic approaches used to solve the rank decoding problem and the MinRank problem over finite fields can be extended to finite principal ideal rings.

References

[1] Kamche, H.T., Kalachi, H.T. Solving systems of algebraic equations over finite commutative rings and applications. AAECC (2024). https://doi.org/10.1007/s00200-024-00652-8

[2] Mikhailov, D., Nechaev, A.A.: Solving systems of polynomial equations over Galois–Eisenstein rings with the use of the canonical generating systems of polynomial ideals. Discrete Math. Appl. (2004)