International Journal of Mathematics Trends and Technology
ISSN: 2231-5373/ https://doi.org/10.14445/22315373/IJMTT-V72I1P108

Volume 72 Issue 1, 143-145, January 2026
© 2026 Seventh Sense Research Group®

Review Article

Recent Advances in Polynomial Factorization over Finite Fields and Its Application

Rasha Thnoon Taieb Alrawi

Department of Mathematics, Open Educational College, Kirkuk, Iraq.

Corresponding Author : rashaalrawi99@gmail.com

Received: 23 November 2025 Revised: 30 December 2025 Accepted: 18 January 2026 Published: 30 January 2026

Abstract - *Polynomial factorization is a crucial problem in Abstract Algebra, which has significant theoretical and practical applications. During the recent decades, considerable progress has been made in the theoretical parts and fast algorithms for factoring polynomials over finite fields. The recent outcomes of the Conventional Algorithms and their expansions are summarized in the review. This also investigates the situation when one variable is of low degree, and the polynomial is monic. The discussion commences with covering finite fields and the irreducibility of the polynomials before laying down the necessary conditions. Następnie zbadano klasyczne technique, why metodę kroneckera, algorithm berlekampa i algorytm cantor zassenhausa, które mają swoje mocne i słabe strony. This review illustrates recently generalized and computational techniques inspired by the observation of algorithm efficiency and scalability improvement for the factoring of high-degree integer polynomials. Due to advances in computer algebra systems and optimization of algorithms, polynomial factorization algorithms have become much more effective and practical. As a result of these advancements, the use of factorization algorithms has spread in practice. The impact of breakthroughs in these areas on applied areas, including Modern Cryptography, Error-Correcting Codes, and Information Security, is also discussed, such as the role of polynomial factorization over finite fields. In conclusion, challenges and open research questions in the contemporary world and new directions are the main topics of discussion in this paper. This paper highlights the continuous importance of polynomial factorization over finite fields as a central topic in abstract algebra and its many uses by fusing traditional ideas in algebra with modern computational and applied perspectives.*

Keywords - *Polynomial Factorization, Finite Fields, Abstract Algebra, Computational Algebra, Irreducible Polynomials, Kronecker Method, Berlekamp Algorithm, Coding Theory, Cryptography, Error-correcting Codes.*

1. Introduction

The problem of polynomial factorization over finite fields is a classical problem in computational algebra with applications to cryptography, coding theory, and symbolic computation [1]. Factoring a polynomial over a finite field into irreducible components can shed light on both the polynomial itself and the field [2, 3]. Historically, conventional algorithms like Berlekamp's method combine linear algebraic techniques with probabilistic ideas. Similarly, they provide effective solutions for univariate polynomial factorization. There has been much theoretical and practical progress in recent years in the area [4,5]. Recent deterministic algorithms with better performance have been developed, along with improved probabilistic approaches that enhance their reliability and efficiency [6]. Furthermore, fast matrix multiplication and modular composition techniques and Galois theory-inspired methods have significantly quickened factorization procedures and expanded their use to polynomials of high degree and of a greater complexity [1]. The recent progressions have lowered the computation burdens of polynomial factorization algorithms and increased the efficacy of these algorithms in large-scale computations and for high-degree polynomials over large finite fields [7]. One important current research direction is the design of deterministic algorithms that do not rely on heuristic assumptions such as GRH [8]. Insights into how polynomials look and how the factors decompose give new strategies for designing algorithms and more refined complexity analyses. By approaching such issues, we will clarify our understanding and efforts here. The efficient factorization of polynomials is essential in many practical applications [9]. The security of lots of protocols and cryptosystems based on discrete logarithm is based on this problem [10]. It is a cryptographic assumption where the security is linked to related factorization problems. In coding theory, factorization over finite fields is required for the construction and decoding of BCH and Reed–Solomon (RS) error-correcting codes [11]. Moreover, factorization algorithms play a central role in the symbolic computation of polynomial equations, the construction of field extensions, etc. [12] With increasing computational needs and the emergence of new applications such as cloud computing, post-quantum cryptography, and large-scale symbolic computation, it is important to comprehend the latest polynomial factorization advancements[13]. Consequently, the objective of the study is to present an overview of the existing algorithms, theoretical underpinnings, and uses, and identify challenges and future directions of research for algorithmic developments. [14].

2. Discussion

Recently, there has been a vast improvement in the theory and practice of polynomial factorization over finite fields [1]. Faster deterministic and probabilistic algorithms have been discovered to greatly lower the price of the calculations of high-degree polynomials over big finite fields [13,1]. Such improvements **as** fast modular composition, Galois-theoretic methods, and more modern linear algebra methods have led to performance improvements in modern factorization algorithms [13,1]. The most notable consequence of these happenings is, possibly, to cryptography, in which the majority of cryptosystems founded on the public key rely on the presumption that the elements of the polynomials and other functions are hard to separate. [15]. Algorithms with high speed are more effective, but the cryptographers need to reconsider their security parameters and assumptions. [16]. The thing is that the truth is that we will need to strike a golden mean between algorithmic efficiency and having a sound security guarantee [17]. Coding theory Construction and decoding of error-correcting codes in coding theory, including BCH and Reed Solomon error-correcting codes, is more effectively done with the aid of the polynomial factorization [17]. The factoring also provides the opportunity to use longer codes and larger finite fields, which is an advantage to the existing system of communication. [18]. Moreover, their use in symbolic computations and computer algebra systems allows them to be used in a variety of algebraic computations, including the factoring of polynomials, extensions of fields, and the study of algebraic structures. The algorithms of factorizing polynomials have theory and practice flourishing side by side, whereby both facets of the research or industrial and scalability uses are applicable [13,1]. However, it has difficulties. Deterministic unconditional polynomially time algorithms are rare and operate on a broad class of polynomials. Many methods are still based on heuristic speculations, e.g., the Generalized Riemann Hypothesis [14]. The current processes discussed in the previous paragraph can be attacked by the degree reduction attacks. All in all, the latest developments of the poly factorization theory in finite fields indicate a tight cooperation between the theory and practice. [13,1]. The mathematical efficiency of algorithms and the expansion of the efficiency of an algorithm in the areas of cryptography, coding theory, and symbolic computation demonstrate that this direction is still topical nowadays, and the further development of this field can be considered in the future[13,1].

3. Conclusion

The process of polynomial factorization over finite fields is a major subject in computational algebra and has many applications in cryptography, coding theory, and symbolic computation. In recent decades, there have been significant advances in deterministic and probabilistic algorithms that are becoming ever more efficient, scalable, and can now even deal with high-degree polynomials over very large finite fields. Techniques that rely on quick modular composition, sophisticated linear algebra, or Galois-theoretic ideas yield better theoretical complexity results and also more efficient implementations in computer algebra systems like magma and singulak. These advances have wide implications. The security assumption of public-key cryptosystems is impacted by the improvement of factorization algorithms, thus requiring constant reassessment of parameters. In coding theory, efficient polynomial factorization builds error-correcting codes and helps in the decoding of error-correcting codes. Additionally, advanced factorization techniques in symbolic computation have equipped researchers with powerful tools to solve algebraic equations, construct field extensions, and reconcile polynomial structures. Challenges continued to exist despite progress. A major open problem is to devise a fully deterministic algorithm that operates efficiently for all classes of polynomials. Another interesting open problem is to develop current methods towards multivariate polynomials and extremely large finite fields—constraints on Future Investigations. Future investigation is likely to deal with the factorization methods resistant to quantum computing, in addition to these limitations. Also, the future research involves extending the area of application to include cloud systems and post-quantum cryptography. All in all, the polynomial factorization over finite fields is a lively area of research in recent times. This research connects theory with practice. This continuous evolution remains instrumental in offering computational tools, while simultaneously fostering new developments within mathematics and computer science.

Funding Statement

There is no funding source for the research. Authors should state how the research and publication of their article was funded, by naming financially supporting bodies, followed by any associated grant numbers in square brackets.

References

[1] Joachim von zur Gathen, and Daniel Panario, "Factoring Polynomials over Finite Fields: A Survey," *Journal of Symbolic Computation*, vol. 31, no. 1-2, pp. 3-17, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rudolf Lidl, and Harald Niederreiter, *Finite Fields*, Cambridge University Press, 1997. [Google Scholar] [Publisher Link]

[3] Victor Shoup, "New Algorithms for Finding Irreducible Polynomials over Finite Fields," *Mathematics of Computation*, vol. 54, pp. 435–447, 1990. [Google Scholar] [Publisher Link]

[4] E.R. Berlekamp, "Factoring Polynomials Over Large Finite Fields," *Mathematics of Computation*, vol. 24, pp. 713–735, 1970. [Google Scholar] [Publisher Link]

[5] David G. Cantor, and Hans Zassenhaus, "A New Algorithm for Factoring Polynomials Over Finite Fields," *Mathematics of Computation*, vol. 36, no. 154, pp. 587–592, 1981. [CrossRef] [Google Scholar] [Publisher Link]

[6] Erich Leo Kaltofen, and Victor Shoup, "Subquadratic-time Factoring of Polynomials Over Finite Fields," *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, 1995. [CrossRef] [Google Scholar] [Publisher Link]

[7] Joris Van der Hoeven, and Gregoire Lecerf, "Univariate Polynomial Factorization Over Finite Fields with Large Extension Degree," *Applicable Algebra in Engineering, Communication and Computing,* vol. 35, pp. 121–149, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zeyu Guo, "Deterministic Polynomial Factoring Over Finite Fields: A Uniform Approach Via P-scheme," *Journal of Symbolic Computation*, vol. 96, pp. 22-61, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] P. Flajolet, X. Gourdon, and D. Panario, "The Complete Analysis of a Polynomial Factorization Algorithm Over Finite Fields," *Journal of Algorithms,* vol. 40, no. 1, pp. 37–81, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[10] Antoine Joux, Andrew Odlyzko, and Cecile Pierrot, "The Past, Evolving Present and Future of Discrete Logarithm," *Open Problems in Mathematics and Computational Science,* pp. 5-36, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[11] S.V. Fedorenko, and P.V. Trifonov, "Finding Roots of Polynomials Over Finite Fields," *IEEE Transactions on Communications*, vol. 50, no. 11, pp. 1709-1711, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[12] Keith O. Geddes, Stephen R. Czapor, and George Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992. [Google Scholar] [Publisher Link]

[13] Joachim von zur Gathen, and Jurgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2013. [Google Scholar] [Publisher Link]

[14] Victor Shoup, "A New Polynomial Factorization Algorithm and Its Implementation," *Journal of Symbolic Computation,* vol. 20, no. 4, pp. 363–397, 1995. [CrossRef] [Google Scholar] [Publisher Link]

[15] Antoine Joux, and Andrew Odlyzko, and Cecile Pierrot, "The Past, Evolving Present and Future of Discrete Logarithms," *Open Problems in Mathematics and Computational Science,* pp. 5-36, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[16] Wikipedia, Chien Search. [Online]. Available: https://en.wikipedia.org/wiki/Chien_search

[17] Oliver Pretzel, *Error-correcting Codes and Finite Fields*, Oxford University Press, 1992. [CrossRef] [Google Scholar] [Publisher Link]

[18] Richard E. Blahut, *Algebraic Codes for Data Transmission (2nd Edition),* Cambridge University Press, 2003. [Google Scholar] [Publisher Link]