Characteristic polynomial of linearized polynomials

Luca Bastioni
University of South Florida, USA

30th Applications of Computer Algebra - ACA 2025

Let q be a prime power, and $\mathbb{F}_q$ be the finite field with q elements. Let m, n, r be positive integers. A polynomial of the form $L(Z) = \sum_{i=0}^{r} a_i Z^{q^i} \in \mathbb{F}_{q^m}[Z]$ is called a linearized polynomial. This type of polynomials is particularly important in coding theory, specifically for the theory of rank-metric codes, where they are used to construct a fundamental family of maximum rank-distance (MRD) codes, called Gabidulin codes. Linearized polynomials are also deeply connected to Drinfeld module's theory and recently, as shown in [1], such connection has been used to construct a new infinite family of optimal rank-metric codes with rank-locality, improving some previous parameters and divisibility conditions present in the construction of [3]. Therefore, it comes natural to investigate properties of linearized polynomials in more depth and in terms of Drinfeld modules. An obvious property is that each linearized polynomial can be seen as an $\mathbb{F}_q$-linear map, and so it makes sense to talk about the characteristic polynomial of a linearized polynomial. In this talk, we show how the theory of Drinfeld modules, together with the theory of linear recurrence sequences, can be used to compute the characteristic polynomial $C_L^{(n)}$ of the $\mathbb{F}_q$-linear map associated to a linearized polynomial $L \in \mathbb{F}_{q^m}[Z]$ acting on an extension $\mathbb{F}_{q^{mn}}$ of $\mathbb{F}_{q^m}$. Then, we provide a new algorithm to compute $C_L^{(n)}$, and we show that its running time is $O(n \log^2(n))$ in terms of $\mathbb{F}_q$ operations. This means that, when $n \gg 0$, our algorithm outperforms any other standard algorithm known in literature, since they instead have a running time of $O(n^\omega \log(n))$ where $2 \leq \omega \leq 3$ (see for example [4] **??**).
This is a joint work with Giacomo Micheli and Shujun Zhao.

References

[1] Luca Bastioni, Mohamed O. Darwish, Giacomo Micheli. Optimal Rank-Metric Codes with Rank-Locality from Drinfeld Modules. *arXiv:2407.06081*, 2024.

[2] Ran Duan, Hongxun Wu, Renfei Zhou. Faster matrix multiplication via asymmetric hashing. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2129–2138, 2023.

[3] Swanand Kadhe, Salim El Rouayheb, Iwan Duursma, Alex Sprintson. Rank-metric codes with local recoverability. In *54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, Sept. 2016.

[4] Walter Keller-Gehrig. Fast algorithms for the characteristics polynomial. *Theoretical computer science*, 36:309–317, 1985.

[5] Clément Pernet, Arne Storjohann. Faster algorithms for the characteristic polynomial. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 307–314. Association for Computing Machinery, 2007.

[6] Vincent Neiger, Clément Pernet. Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *Journal of Complexity*, 67:101572, 2021.