RECURSIVE CONSTRUCTIONS OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

LUCAS REIS

UFMG - CARLETON U

ABSTRACT. Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p. There is a special action of the group $\mathrm{PGL}_2(\mathbb{F}_q)$ on the set of monic irreducible polynomials of degree $n \geq 2$ over $\mathbb{F}_q$ and the invariant polynomials have been explored by many authors (see [1], [2], [3] and [5]). Recently, in [4], it was showed that, for a given element $[A] \in \mathrm{PGL}_2(\mathbb{F}_q)$, the $[A]$-invariant polynomials arise from certain rational transformations of degree D, where D is the order of $[A]$. In this talk we discuss the construction of such $[A]$-invariants as well as constructions of infinite sequences of irreducible polynomials: given a positive integer n and $D > 1$ a divisor of $q - 1, q + 1$ or p, we show how to obtain a sequence of irreducible polynomials f_i of degree $n \cdot D^i$. In particular, this generalizes the construction of irreducible polynomials via quadratic transformations, such as constructions of self-reciprocal polynomials of degree $2^i \cdot n$. We also discuss a probabilistic approach that arises naturally in the construction of $[A]$-invariants.

REFERENCES

[1] T. Garefalakis. On the action of $\mathrm{GL}(2,q)$ on irreducible polynomials over $\mathbb{F}_q$. *J. Pure Appl. Algebra*, 215:1835–1843, 2011.
[2] S. Mattarei, M. Pizzato. Generalizations of self-reciprocal polynomials *Finite Fields Appl.*, 48: 271–288, 2017.
[3] L. Reis. The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited. *J. Pure Appl. Algebra* (in press), 2017. `http://dx.doi.org/10.1016/j.jpaa.2017.06.008`
[4] L. Reis Invariant theory of a special group action on irreducible polynomials over finite fields. Arxiv, 2017.
[5] H. Stichtenoth and A. Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18:108–122, 2012.