Fan, Xiang
Permutation polynomials of degree 8 over finite fields of characteristic 2. (English)
Zbl 1444.11239
Finite Fields Appl. 64, Article ID 101662, 20 p. (2020).

Let $\mathbb{F}_q$ denote the finite field of characteristic $p$ and order $q = p^r$, $r$ a positive integer. We call $f \in \mathbb{F}_q[x]$ a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced map $a \mapsto f(a)$ permutes $\mathbb{F}_q$. An exceptional polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ which is PP over infinite many extensions $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. It is known that permutation polynomials of $\mathbb{F}_q$ of degree $d < \sqrt{q}$ are in particular exceptional polynomials.

Permutation polynomials of small degree have been completely classified: in [L. E. Dickson, Ann. Math. 11, 65–120, 161–183 (1896; JFM 28.0135.03)] for $d \leq 5$ and any $q$, and for $d = 6$, $q$ odd; in [J. Li et al., Finite Fields Appl. 16, No. 6, 406–419 (2010; Zbl 1206.11145)] for $d = 6, 7$, $q \geq 8$ even; in [X. Fan, Finite Fields Appl. 59, 1–21 (2019; Zbl 1444.11238)] for $d = 7$, $q$ odd; in [X. Fan, Bull. Aust. Math. Soc. 101, No. 1, 40–55 (2020; Zbl 1456.11227)] for $d = 8$, $q$ odd.

In this paper the author classifies permutation polynomials of degree 8 over $\mathbb{F}_{2^r}$, $r > 3$, up to linear transformations.

Since the whole set of exceptional polynomials of degree 8 over fields of even characteristic have been already determined in [D. Bartoli et al., J. Number Theory 176, 46–66 (2017; Zbl 1364.11150)], to complete the classification of PPs of degree 8 over $\mathbb{F}_{2^r}$, $r > 3$, it suffices to search for the non-exceptional ones. In particular, the search can be focused only on the cases $r \leq 9$.

The classification of permutation polynomials has been done with the help of the open-source computer algebra system SageMath. Most of the efforts in this paper are devoted to prune the search space, by proving necessary conditions on the coefficients of a polynomial to be a permutation.

Reviewer: Daniele Bartoli (Perugia)

MSC:
11T06 Polynomials over finite fields

Keywords:
Permutation polynomial; exceptional polynomial; Hermite’s criterion

Software:
SageMath

Full Text: DOI arXiv

References:
This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.