Konyagin, Sergei; Pappalardi, Francesco

Enumerating permutation polynomials over finite fields by degree. (English) Zbl 1029.11067

Finite Fields Appl. 8, No. 4, 548-553 (2002).

Every permutation on the elements of $\mathbb{F}_q$ ($q > 2$) is uniquely represented by a polynomial over $\mathbb{F}_q$ of degree $\leq q-2$. The authors deal with the problem of enumerating such permutation polynomials having degree $< q-2$. This is equivalent to counting the permutations σ of $\mathbb{F}_q$ for which $\sum_{c\in\mathbb{F}_q} c\sigma(c) = 0$.

Let N denote the number of permutations of $\mathbb{F}_q$ satisfying this condition. By inclusion exclusion,

$$N = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S$$

where n_S is the number of mappings $f\colon \mathbb{F}_q \to S$ with $\sum_{c\in S} cf(c) = 0$. Using an expression for n_S in terms of exponential sums, the authors then show that

$$|N - (q-1)!| \leq \sqrt{2e/\pi}\, q^{q/2}.$$

A similar estimate for a prime q was determined, using a different method, by *P. Das* [Finite Fields Appl. 8, 478–490 (2002; Zbl 1029.11066)].

Reviewer: Astrid Reifegerste (Hannover)

MSC:

11T06 Polynomials over finite fields

Keywords:

permutation polynomials over finite fields; exponential sums

Full Text: DOI arXiv

References:

[1] Grosswald, E., Algebraic inequalities for \textit{π}, solution to a problem proposed by R. E. Shafer, Amer. math. monthly, 84, 63, (1977)

[2] Konyagin, S., A note on the least prime in an arithmetic progression, East J. approx., 1, 403-418, (1995) · Zbl 0855.11045

[3] Lidl, R.; Mullin, G.L., When does a polynomial over a finite field permute the elements of the field?, Amer. math. monthly, 95, 243-246, (1988) · Zbl 0653.12010

[4] Lidl, R.; Mullin, G.L., When does a polynomial over a finite field permute the elements of the field? II, Amer. math. monthly, 100, 71-74, (1993) · Zbl 0777.11054

[5] Lidl, R.; Niederreiter, H., Finite fields, (1983), Addison-Wesley Reading

[6] C. Malvenuto, and, F. Pappalardi, Enumerating permutation polynomials I: Permutations with non-maximal degree, submitted. · Zbl 1029.11068

[7] C. Malvenuto, and, F. Pappalardi, Enumerating permutation polynomials II: \textit{k}-cycles with minimal degree, in preparation. · Zbl 1035.11062