Hou, Xiang-Dong
A new approach to permutation polynomials over finite fields. (English) Zbl 1273.11169
Finite Fields Appl. 18, No. 3, 492-521 (2012).

Summary: Let p be a prime and $q = p^\kappa$. We study the permutation properties of the polynomial $g_{n,q} \in \mathbb{F}_p[x]$ defined by the functional equation $\sum_{a \in \mathbb{F}_q}(x + a)^n = g_{n,q}(x^q - x)$. The polynomial $g_{n,q}$ is a q-ary version of the reversed Dickson polynomial in characteristic 2. We are interested in the parameters $(n, e; q)$ for which $g_{n,q}$ is a permutation polynomial (PP) of $\mathbb{F}_{q^e}$. We find several families of such parameters and obtain various necessary conditions on such parameters. Initial results, both theoretical and numerical, indicate that the class $g_{n,q}$ contains an abundance of PPs over finite fields, many of which are yet to be explained and understood.

MSC:
11T06 Polynomials over finite fields

Cited in **2** Reviews
Cited in **15** Documents

Keywords:
finite field; permutation polynomial; reversed Dickson polynomial

Full Text: DOI

References:

[1] Carlitz, L., On certain functions connected with polynomials in a Galois field, Duke math. J., 1, 139-158, (1935) · Zbl 61.0127.01

[2] Dillon, J.F., Geometry, codes and difference sets: exceptional connections, (), 73-85 · Zbl 1032.94013

[3] Goss, D., Basic structures of function field arithmetic, (1996), Springer-Verlag Berlin-Heidelberg · Zbl 0874.11004

[4] K. Hicks, X. Hou, G.L. Mullen, Sums of reciprocals of polynomials over finite fields, Amer. Math. Monthly, in press. · Zbl 1266.11129

[5] Hollmann, H.D.L.; Xiang, Q., Kloosterman sum identities over $\mathbf{F}_{2^m}$, Discrete math., 279, 277-286, (2004) · Zbl 1099.11040

[6] Hou, X., Two classes of permutation polynomials over finite fields, J. combin. theory ser. A, 118, 448-454, (2011) · Zbl 1230.11146

[7] Hou, X., Third power of the reversed dickson polynomial over finite fields

[8] Hou, X.; Ly, T., Necessary conditions for reversed dickson polynomials to be permutational, Finite fields appl., 16, 436-448, (2010) · Zbl 1209.11103

[9] Hou, X.; Mullen, G.L.; Sellers, J.A.; Yucas, J.L., Reversed dickson polynomials over finite fields, Finite fields appl., 15, 748-773, (2009) · Zbl 1228.11174

[10] Lidl, R.; Niederreiter, H., Finite fields, (1997), Cambridge Univ. Press Cambridge

[11] Nyberg, K., Differentially uniform mappings for cryptography, (), 55-64 · Zbl 0951.94510

[12] Thakur, D.S., Function field arithmetic, (2004), World Scientific Publishing Co. River Edge, NJ · Zbl 1061.11001

[13] Yuan, J.; Ding, C.; Wang, H.; Pieprzyk, J., Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, Finite fields appl., 14, 482-493, (2008) · Zbl 1211.11136

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.