Yuan, Pingzhi; **Ding, Cunsheng**

Further results on permutation polynomials over finite fields. (English) Zbl 1297.11148

Finite Fields Appl. 27, 88-103 (2014).

Let $\mathbb{F}_{q^n}$ be a finite field. The main result of the paper is: Suppose $g(x) \in \mathbb{F}_{q^n}[x]$ satisfies $g(x)^q = g(x)$ for all $x \in \mathbb{F}_{q^n}$, and let $L(x)$ be a linearized polynomial. For every $\delta \in \mathbb{F}_{q^n}$,

$$f(x) = g(x^q - x + \delta) + L(x)$$

permutes $\mathbb{F}_{q^n}$ if and only if $L(x)$ does. The authors use this to unify some previous constructions of permutation polynomials and to construct new ones.

Typos have been corrected in the corrigenda [ibid. 30, 153–154 (2014; Zbl 1297.11150)].

Reviewer: Robert Fitzgerald (Carbondale)

MSC:

11T06 Polynomials over finite fields
05B10 Combinatorial aspects of difference sets (number-theoretic, group-theoretic, etc.)

Keywords:

permutation polynomials; linearized polynomials; skew Hadamard difference sets

Full Text: DOI arXiv

References:

[1] Akbary, A.; Ghioca, D.; Wang, Q., On constructing permutations of finite fields, Finite Fields Appl., 17, 51-67, (2011) · Zbl 1281.11102

[2] Carlet, C.; Ding, C.; Yuan, J., Linear codes from highly nonlinear functions and their secret sharing schemes, IEEE Trans. Inf. Theory, 51, 6, 2089-2102, (2005) · Zbl 1192.94114

[3] Cao, X.; Hu, L., New methods for generating permutation polynomials over finite fields, Finite Fields Appl., 17, 493-503, (2011) · Zbl 1245.11114

[4] Charpin, P.; Kyureghyan, G., When does $F(X) + \operatorname{Tr}(H(X))$ permute $\mathbb{F}_{p^n}$?, Finite Fields Appl., 15, 5, 615-632, (2009) · Zbl 1229.11153

[5] Charpin, P.; Kyureghyan, G., On a class of permutation polynomials over $\mathbb{F}_{2^n}$, (SETA 2008, Lect. Notes Comput. Sci., vol. 5203, (2008), Springer-Verlag), 368-376 · Zbl 1180.11038

[6] Ding, C.; Helleseth, T., Optimal ternary cyclic codes from monomials, IEEE Trans. Inf. Theory, 59, 9, 5898-5904, (2013) · Zbl 1364.94652

[7] Ding, C.; Yin, J., Signal sets from functions with optimum nonlinearity, IEEE Trans. Commun., 55, 5, 936-940, (2007)

[8] Ding, C.; Yuan, J., A family of skew Hadamard difference sets, J. Comb. Theory, Ser. A, 113, 1526-1535, (2006) · Zbl 1106.05016

[9] Ding, C.; Xiang, Q.; Yuan, J.; Yuan, P., Explicit classes of permutation polynomials over GF($3^{3 m}$), Sci. China, Ser. A, 53, 639-647, (2009) · Zbl 1215.11113

[10] Kyureghyan, G., Constructing permutations of finite fields via linear translators, J. Comb. Theory, Ser. A, 118, 1052-1061, (2010) · Zbl 1241.11136

[11] Laigle-Chapuy, Y., Permutation polynomials and applications to coding theory, Finite Fields Appl., 13, 58-70, (2007) · Zbl 1107.11048

[12] Li, N.; Helleseth, T.; Tang, X., Further results on a class of permutation polynomials over finite fields, Finite Fields Appl., 22, 16-23, (2013) · Zbl 1285.05004

[13] Hou, X., Two classes of permutation polynomials over finite fields, J. Comb. Theory, Ser. A, 118, 2, 448-454, (2011) · Zbl 1230.11146

[14] Hou, X.; Mullen, G. L.; Sellers, J. A.; Yucas, J. L., Reversed dickson polynomials over finite fields, Finite Fields Appl., 15, 6, 748-773, (2009) · Zbl 1228.11174

[15] Lidl, R.; Müller, W. B., Permutation polynomials in RSA-cryptosystems, (Advances in Cryptology, (1984), Plenum New York), 293-301

[16] Lidl, R.; Niederreiter, H., Finite fields, Encycl. Math. Appl., vol. 20, (1997), Cambridge University Press Cambridge

[17] Lidl, R.; Niederreiter, H., Introduction to finite fields and their applications, (1986), Cambridge University Press Cambridge · Zbl 0629.12016

[18] Marcos, J. E., Specific permutation polynomials over finite fields, Finite Fields Appl., 17, 105-112, (2011) · Zbl 1261.11080

[19] Mullen, G. L., Permutation polynomials over finite fields, (Proceedings of the Conference on Finite Fields and Their Applications, Lect. Notes Pure Appl. Math., vol. 141, (1993), Marcel Dekker), 131-151 · Zbl 0808.11069

[20] Mullen, G. L.; Wang, Q., Permutation polynomials in one variable, (Mullen, G. L.; Panario, D., Handbook of Finite Fields, (2013), CRC Press), 215-229

[21] Rivest, R. L.; Shamir, A.; Adelman, L. M., A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, 21, 120-126, (1978) · Zbl 0368.94005

[22] Schwenk, J.; Huber, K., Public key encryption and digital signatures based on permutation polynomials, Electron. Lett., 34, 759-760, (1998)

[23] Wang, Q., Cyclotomic mapping permutation polynomials over finite fields, (Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, Los Angeles, CA, USA, May 31-June 2, 2007, Lect. Notes Comput. Sci., vol. 4893, (2007)), 119-128 · Zbl 1154.11342

[24] Yuan, J.; Carlet, C.; Ding, C., The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, 52, 2, 712-717, (2006) · Zbl 1192.94128

[25] Yuan, P.; Ding, C., Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl., 17, 560-574, (2011) · Zbl 1258.11100

[26] Zeng, X.; Zhu, X.; Hu, L., Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Eng. Commun. Comput., 21, 145-150, (2010) · Zbl 1215.11116

[27] Zha, Z.; Hu, L., Two classes of permutation polynomials over finite fields, Finite Fields Appl., 18, 781-790, (2012) · Zbl 1288.11111

[28] Zieve, M. E., Some families of permutation polynomials over finite fields, Int. J. Number Theory, 4, 851-857, (2008) · Zbl 1204.11180

[29] Zieve, M. E., Classes of permutation polynomials based on cyclotomy and an additive analogue, (Additive Number Theory, (2010), Springer), 355-361 · Zbl 1261.11081