Feng, Xiutao; **Lin, Dongdai**; **Wang, Liping**; **Wang, Qiang**
Further results on complete permutation monomials over finite fields. (English) Zbl 07067778
Finite Fields Appl. 57, 47-59 (2019).

Summary: In this paper, we construct several new classes of complete permutation monomials $a^{-1}x^d$ over a finite field $\mathbb{F}_{q^n}$ with exponents $d = \frac{q^n-1}{q-1} + 1$, $\frac{q^{p-1}-1}{q-1} + 1$, and $\frac{q^{q-1}-1}{q-1} + 1$, respectively, where $q = p^k$ is a power of a prime number p. Our approach uses the AGW criterion (the multiplicative case) together with Dickson permutation polynomials and a class of exceptional polynomials respectively. One of our results confirms Conjecture 4.18 by G. Wu, N. Li, T. Helleseth, Y. Zhang in [42] under the assumption that the characteristic p is primitive modulo a prime number $n + 1$. Moreover, we show that Conjecture 4.18 is false in general using our approach and a counterexample is provided. We also re-confirm Conjecture 4.20 in [42] that was proved recently in [24], and extend some of these recent results to more general n's and more general a's.

MSC:

11T06 Polynomials over finite fields
05A05 Permutations, words, matrices
11T55 Arithmetic theory of polynomial rings over finite fields

Keywords:

finite fields; permutation polynomials; complete permutation polynomials; monomials

Full Text: DOI arXiv

References:

[1] Akbary, A.; Alaric, S.; Wang, Q., On some classes of permutation polynomials, Int. J. Number Theory, 4, 1, 121-133, (2008) · Zbl 1218.11108

[2] Akbary, A.; Ghioca, D.; Wang, Q., On permutation polynomials of prescribed shape, Finite Fields Appl., 15, 195-206, (2009) · Zbl 1220.11145

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

[4] Akbary, A.; Wang, Q., On some permutation polynomials, Int. J. Math. Math. Sci., 16, 2631-2640, (2005) · Zbl 1092.11046

[5] Akbary, A.; Wang, Q., A generalized Lucas sequence and permutation binomials, Proc. Am. Math. Soc., 134, 1, 15-22, (2006) · Zbl 1137.11355

[6] Akbary, A.; Wang, Q., On polynomials of the form $x^r f(x^{(q - 1) / l})$, Int. J. Math. Math. Sci., 2007, Article 23408, (2007), 7 pages · Zbl 1135.11341

[7] Bartoli, D.; Giulietti, M.; Zini, G., On monomial complete permutation polynomials, Finite Fields Appl., 41, 3, 132-158, (2016) · Zbl 1372.11107

[8] Bartoli, D.; Giulietti, M.; Quoos, L.; Zini, G., Complete permutation polynomials from exceptional polynomials, J. Number Theory, 176, 46-66, (2017) · Zbl 1364.11150

[9] Bassalygo, L. A.; Zinoviev, V. A., On one class of permutation polynomials over finite fields of characteristic two, Mosc. Math. J., 15, 4, 703-713, (2015) · Zbl 1393.11079

[10] Bassalygo, L. A.; Zinoviev, V. A., Permutation and complete permutation polynomials, Finite Fields Appl., 33, 198-211, (2015) · Zbl 1368.11126

[11] Bhargava, M.; Zieve, M. E., Factoring Dickson polynomials over finite fields, Finite Fields Appl., 5, 103-111, (1999) · Zbl 0929.11060

[12] Chou, W.-S., The factorization of Dickson polynomials over finite fields, Finite Fields Appl., 3, 84-96, (1997) · Zbl 0910.11052

[13] Evans, A. B., Orthomorphism Graphs of Groups, Lecture Notes in Mathematics, vol. 1535, (1992), Springer-Verlag · Zbl 0796.05001

[14] Fried, M. D.; Guralnick, R.; Saxl, J., Schur covers and Carlitz's conjecture, Isr. J. Math., 82, 1-3, 157-225, (1993) · Zbl 0855.11063

[15] Hou, X., Permutation polynomials over finite fields—a survey of recent advances, Finite Fields Appl., 32, 82-119, (2015) · Zbl

1325.11128

[16] Hou, X., A survey of permutation binomials and trinomials over finite fields, (Topics in Finite Fields. Topics in Finite Fields, Contemp. Math., vol. 632, (2015), Amer. Math. Soc.: Amer. Math. Soc. Providence, RI), 177-191 · Zbl 1418.11153

[17] Hou, X., Permutation polynomials of $\mathbb{F}_{q^2}$ of the form $a X + X^{r(q - 1) + 1}$, (Contemporary Developments in Finite Fields and Applications, (2016), World Sci. Publ.: World Sci. Publ. Hackensack, NJ), 74-101 · Zbl 1371.11151

[18] Lee, J. B.; Park, Y. H., Some permutation trinomials over finite fields, Acta Math. Sci., 17, 250-254, (1997) · Zbl 0921.11062

[19] Li, K.; Qu, L.; Chen, X., New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl., 43, 69-85, (2017) · Zbl 1351.11078

[20] Li, K.; Qu, L.; Wang, Q., New constructions of permutation polynomials of the form $x^r h(x^{q - 1})$ over $\mathbb{F}_{q^2}$, Des. Codes Cryptogr., 86, 10, 2379-2405, (2018) · Zbl 06933694

[21] Lidl, R.; Mullen, G. L., When does a polynomial over a finite field permute the elements of the field?, Am. Math. Mon., 95, 243-246, (1988) · Zbl 0653.12010

[22] Lidl, R.; Mullen, G. L., When does a polynomial over a finite field permute the elements of the field? II, Am. Math. Mon., 100, 71-74, (1993) · Zbl 0777.11054

[23] Lidl, R.; Niederreiter, H., Finite Fields, Encyclopedia of Mathematics and Its Applications, (1997), Cambridge University Press

[24] Ma, J.; Zhang, T.; Feng, T.; Ge, G., New results on permutation polynomials over finite fields, Des. Codes Cryptogr., 83, 425-443, (2017) · Zbl 1369.11091

[25] Mullen, G. L., Permutation polynomials over finite fields, (Finite Fields, Coding Theory, and Advances in Communications and Computing, (1993), Marcel Dekker: Marcel Dekker New York), 131-151 · Zbl 0808.11069

[26] Mullen, G. L.; Panario, D., Handbook of Finite Fields, (2013), CRC Press · Zbl 1319.11001

[27] Mullen, G. L.; Wang, Q., Permutation polynomials of one variable, Section 8.1, (Mullen, G. L.; Panario, D., Handbook of Finite Fields, (2013), CRC Press), 215-229

[28] Niederreiter, H.; Winterhof, A., Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, Discrete Math., 295, 161-171, (2005) · Zbl 1078.11068

[29] Nyberg, K., Perfect non-linear S-boxes, (Proc. Advances in Cryptology. Proc. Advances in Cryptology, EUROCRYPT (1991). Proc. Advances in Cryptology. Proc. Advances in Cryptology, EUROCRYPT (1991), LNCS, vol. 547, (1992), Springer: Springer Heidelberg), 378-386 · Zbl 0766.94012

[30] Muratović-Ribić, A.; Pasalic, E., A note on complete polynomials over finite fields and their applications in cryptography, Finite Fields Appl., 25, 306-315, (2014) · Zbl 1302.11096

[31] Stănică, P.; Gangopadhyay, S.; Chaturvedi, A.; Gangopadhyay, A. K.; Maitra, S., Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inf. Theory, 58, 6, 4064-4072, (2012) · Zbl 1365.94684

[32] Tu, Z.; Zeng, X.; Hu, L., Several classes of complete permutation polynomials, Finite Fields Appl., 25, 182-193, (2014) · Zbl 1284.05012

[33] Tuxanidy, A.; Wang, Q., Compositional inverses and complete mappings over finite fields, Discrete Appl. Math., 217, 318-329, (2017), part 2 · Zbl 1372.11111

[34] Wan, Z. X., Lectures on Finite Fields and Galois Rings, (2003), Wolrd Scientific Publishing Co. Pte. Ltd. · Zbl 1028.11072

[35] Wan, D.; Lidl, R., Permutation polynomials of the form $x^r f(x^{(q - 1) / d})$ and their group structure, Monatshefte Math., 112, 149-163, (1991) · Zbl 0737.11040

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

[37] Wang, Q., On generalized Lucas sequences, Combinatorics and Graphs. Combinatorics and Graphs, The Twentieth Anniversary Conference of IPM, May 15-21, 2009. Combinatorics and Graphs. Combinatorics and Graphs, The Twentieth Anniversary Conference of IPM, May 15-21, 2009, Contemp. Math., 531, 127-141, (2010) · Zbl 1246.11039

[38] Wang, Q., Cyclotomy and permutation polynomials of large indices, Finite Fields Appl., 22, 57-69, (2013) · Zbl 1331.11107

[39] Wu, B.; Lin, D., Complete permutation polynomials induced from complete permutations of subfields, (2013), preprint

[40] Wu, B.; Lin, D., On constructing complete permutation polynomials over finite fields of even characteristic, Discrete Appl. Math., 184, 213-222, (2015) · Zbl 1311.05009

[41] Wu, G.; Li, N.; Helleseth, T.; Zhang, Y., Some classes of monomial complete permutation polynomials over finite fields of characteristic two, Finite Fields Appl., 28, 148-165, (2014) · Zbl 1314.11073

[42] Wu, G.; Li, N.; Helleseth, T.; Zhang, Y., Some classes of complete permutation polynomials over $\mathbb{F}_q$, Sci. China Math., 58, 10, 2081-2094, (2015) · Zbl 1325.05013

[43] Yuan, P.; Ding, C., Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl., 17, 6, 560-574, (2011) · Zbl 1258.11100

[44] Yuan, P.; Ding, C., Further results on permutation polynomials over finite fields, Finite Fields Appl., 27, 88-103, (2014) · Zbl 1297.11148

[45] Zha, Z.; Hu, L.; Fan, S., Further results on permutation trinomials over finite fields with even characteristic, Finite Fields Appl., 45, 43-52, (2017) · Zbl 1362.05006

[46] Zheng, Y.; Yuan, P.; Pei, D., Large classes of permutation polynomials over $\mathbb{F}_{q^2}$, Des. Codes Cryptogr., 81, 3, 505-521, (2016) · Zbl 1396.11139

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

[48] Zieve, M., On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q - 1) / d})$, Proc. Am. Math. Soc., 137, 7, 2209-2216, (2009) · Zbl 1228.11177

[49] Zieve, M., Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, (2013)