Tuxanidy, Aleksandr; **Wang, Qiang**

Compositional inverses and complete mappings over finite fields. (English) Zbl 1372.11111
Discrete Appl. Math. 217, Part 2, 318-329 (2017).

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements and $f \in \mathbb{F}_q[x]$ a univariate polynomial. If f induces a permutation of $\mathbb{F}_q$ under evaluation then there exists a unique $f^{-1} \in \mathbb{F}_q[x]$ of degree less than q satisfying $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x}$. The paper under review studies this compositional inverse in case f is a linearized binomial permuting the kernel of the trace map $T_{q^n|q^s} : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^s}$, where s is a positive divisor of n.

In Theorem 2.4 it is shown that for any positive integer r such that $d := \gcd(n, r) = \gcd(r, s)$ and any $c \in \mathbb{F}_{q^s}$ whose norm $N^{q^s|q^d}(c)$ equals 1, the binomial $L_{c,r}(x) := x^{q^r} - cx \in \mathbb{F}_{q^n}[x]$ induces a permutation of $\ker(T_{q^n|q^s})$ if and only if n/s is not divisible by the characteristic p. Theorem 2.4 also contains an explicit formula for $L_{c,r}^{-1}$ when it exists.

This result is used in order to construct a class of complete mappings (i.e., permutation polynomials $f \in \mathbb{F}_q[x]$ such that $f(x) + x$ also permutes $\mathbb{F}_q$) for which the computational inverse is again explicitly obtained. A recursive construction of a set of complete mappings with the property that the difference of any two distinct elements permutes $\mathbb{F}_q$ is also given.

Reviewer: Mihai Cipu (Bucureşti)

MSC:

11T06 Polynomials over finite fields
05B15 Orthogonal arrays, Latin squares, Room squares

Keywords:

permutation polynomials; complete mappings; compositional inverse; linearized polynomials; finite fields; binomial; trace

Full Text: DOI

References:

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

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

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

[4] Cao, X.; Hu, L.; Zha, Z., Constructing permutation polynomials from piecewise permutations, Finite Fields Appl., 26, 162-174, (2014) · Zbl 1288.11109

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

[6] Coulter, R. S.; Henderson, M., The compositional inverse of a class of permutation polynomials over a finite field, Bull. Aust. Math. Soc., 65, 521-526, (2002) · Zbl 1023.11061

[7] Coulter, R. S.; Henderson, M.; Mathews, R., A note on constructing permutation polynomials, Finite Fields Appl., 15, 5, 553-557, (2009) · Zbl 1215.11112

[8] Ding, C., Cyclic codes from some monomials and trinomials, SIAM J. Discrete Math., 27, 4, 1977-1994, (2013) · Zbl 1306.94114

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

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

[11] Fernando, N.; Hou, X., A piecewise construction of permutation polynomial over finite fields, Finite Fields Appl., 18, 1184-1194, (2012) · Zbl 1254.05008

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

[13] Hou, X., A new approach to permutation polynomials over finite fields, Finite Fields Appl., 18, 3, 492-521, (2012) · Zbl 1273.11169

[14] Kyureghyan, G. M., Constructing permutations of finite fields via linear translators, J. Combin. Theory Ser. A, 118, 3, 1052-1061, (2011) · Zbl 1241.11136

[15] Laigle-Chapuy, Y., A note on a class of quadratic permutation polynomials over $\mathbb{F}_{2^n}$, (Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol. 4851, (2007), Springer), 130-137 · Zbl 1195.11159

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

[17] Lidl, R.; Niederreiter, H., (Finite Fields, Encyclopedia Math. Appl., vol. 20, (1997), Cambridge University Press Cambridge)

[18] Marcos, J. E., Specific permutation polynomials over finite fields, Finite Fields Appl., 17, 2, 105-112, (2011) · Zbl 1261.11080

[19] Mullen, G. L.; Wang, Q., Permutation polynomials of one variable, (Handbook of Finite Fields, (2013), Chapman and Hall/CRC), 215-230, Section 8.1

[20] Muratović-Ribić, A., A note on the coefficients of inverse polynomials, Finite Fields Appl., 13, 4, 977-980, (2007) · Zbl 1167.11044

[21] 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

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

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

[24] Sade, A., Groupoides automorphes par le groupe cyclique, Canad. J. Math., 9, 321-335, (1957) · Zbl 0092.01801

[25] S. Samardjiska, D. Gligoroski, Quadratic permutation polynomials, complete mappings and mutually orthogonal Latin squares, Preprint, 2014. · Zbl 1442.11165

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

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

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

[29] Tuxanidy, A.; Wang, Q., On the inverses of some classes of permutations of finite fields, Finite Fields Appl., 28, 244-281, (2014) · Zbl 1360.11134

[30] Wang, Q., On inverse permutation polynomials, Finite Fields Appl., 15, 207-213, (2009) · Zbl 1183.11075

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

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

[33] Wu, B., Linearized and linearized derived permutation polynomials over finite fields and their compositional inverses, (2013), University of Chinese Academy of Sciences, (in Chinese)

[34] B. Wu, The compositional inverses of linearized permutation binomials over finite fields, Preprint, 2013. arXiv:1311.2154v1 [math.NT].

[35] G. Wu, N. Li, T. Helleseth, Y. Zhang, More classes of complete permutation polynomials over $\mathbb{F}_q$, Preprint, 2013. arXiv:1312.4716v2 [cs.IT].

[36] B. Wu, D. Lin, Complete permutation polynomials induced from complete permutations of subfields, Preprint, 2013. arXiv:1312.5502v1 [math.NT].

[37] 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

[38] Wu, B.; Liu, Z., Linearized polynomials over finite fields revisited, Finite Fields Appl., 22, 79-100, (2013) · Zbl 1345.11084

[39] Wu, B.; Liu, Z., The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2, Finite Fields Appl., 24, 136-147, (2013) · Zbl 1286.05005

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

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

[42] Zha, Z.; Hu, L., Two classes of permutation polynomials over finite fields, Finite Fields Appl., 18, 4, 781-790, (2012) · Zbl 1288.11111

[43] Zha, Z.; Hu, L.; Cao, X., Constructing permutations and complete permutations over finite fields via subfield-valued polynomials, Finite Fields Appl., 31, 162-177, (2015) · Zbl 1320.11123

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