Anbar, Nurdagül; **Odžak, Almasa**; **Patel, Vandita**; **Quoos, Luciane**; **Somoza, Anna**; **Topuzoğlu, Alev**

On the difference between permutation polynomials. (English) Zbl 1374.11089

Finite Fields Appl. 49, 132-142 (2018).

Summary: The well-known Chowla and Zassenhaus conjecture, proved by Cohen in 1990, states that if $p > (d^2-3d+4)^2$, then there is no complete mapping polynomial f in $\mathbb{F}_p[x]$ of degree $d \geq 2$. For arbitrary finite fields $\mathbb{F}_q$, a similar non-existence result was obtained recently by Işık, Topuzoğlu and Winterhof in terms of the Carlitz rank of f.

Cohen, Mullen and Shiue generalized the Chowla-Zassenhaus-Cohen Theorem significantly in 1995, by considering differences of permutation polynomials. More precisely, they showed that if f and $f+g$ are both permutation polynomials of degree $d \geq 2$ over $\mathbb{F}_p$, with $p > (d^2-3d+4)^2$, then the degree k of g satisfies $k \geq 3d/5$, unless g is constant. In this article, assuming f and $f+g$ are permutation polynomials in $\mathbb{F}_q[x]$, we give lower bounds for the Carlitz rank of f in terms of q and k. Our results generalize the above mentioned result of Işık et al. We also show for a special class of permutation polynomials f of Carlitz rank $n \geq 1$ that if $f + x^k$ is a permutation over $\mathbb{F}_q$, with $\gcd(k+1, q-1) = 1$, then $k \geq (q-n)/(n+3)$.

MSC:

11T06 Polynomials over finite fields
14H05 Algebraic functions and function fields in algebraic geometry

Keywords:

Carlitz rank; Chowla-Zassenhaus conjecture; curves over finite fields; permutation polynomials

Full Text: DOI

References:

[1] Aksoy, E.; Çeşmelioğlu, A.; Meidl, W.; Topuzoğlu, A., On the Carlitz rank of a permutation polynomial, Finite Fields Appl., 15, 428-440, (2009) · Zbl 1232.11124

[2] Carlitz, L., Permutations in a finite field, Proc. Am. Math. Soc., 4, 538, (1953) · Zbl 0052.03704

[3] Chowla, S.; Zassenhaus, H., Some conjectures concerning finite fields, Nor. Vidensk. Selsk. Forh. (Trondheim), 41, 34-35, (1968) · Zbl 0186.09203

[4] Cohen, S. D., Proof of a conjecture of chowla and Zassenhaus on permutation polynomials, Can. Math. Bull., 33, 230-234, (1990) · Zbl 0722.11060

[5] Cohen, S. D.; Mullen, G. L.; Shiue, P. J.-S., The difference between permutation polynomials over finite fields, Proc. Am. Math. Soc., 123, 2011-2015, (1995) · Zbl 0827.11074

[6] Hirschfeld, J. W.P.; Korchmáros, G.; Torres, F., Algebraic curves over a finite field, (2013), Princeton University Press · Zbl 1200.11042

[7] L. Işık, A. Topuzoğlu, A note on value set of polynomials over finite fields, preprint.

[8] Işık, L.; Topuzoğlu, A.; Winterhof, A., Complete mappings and Carlitz rank, Des. Codes Cryptogr., 85, 121-128, (2017) · Zbl 1408.11115

[9] Laywine, C. F.; Mullen, G., Discrete mathematics using Latin squares, Wiley-Interscience Series in Discrete Mathematics and Optimization, A Wiley-Interscience Publication, (1998), John Wiley \& Sons, Inc. New York · Zbl 0957.05002

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

[11] Niederreiter, H.; Robinson, K. H., Complete mappings of finite fields, J. Aust. Math. Soc. A, 33, 197-212, (1982) · Zbl 0495.12018

[12] Schulz, R.-H., On check digit systems using anti-symmetric mappings, (Numbers, Information and Complexity, Bielefeld, 1998, (2000), Kluwer Acad. Publ. Boston, MA), 295-310 · Zbl 0967.94030

[13] Shaheen, R.; Winterhof, A., Permutations of finite fields for check digit systems, Des. Codes Cryptogr., 57, 361-371, (2010) · Zbl 1248.11100

[14] 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, 4064-4072, (2012) · Zbl 1365.94684

[15] Stichtenoth, H., Algebraic function fields and codes, Graduate Texts in Mathematics, vol. 254, (2009), Springer-Verlag · Zbl 1155.14022

[16] Topuzoğlu, A., Carlitz rank of permutations of finite fields: a survey, J. Symb. Comput., 64, 53-66, (2014) · Zbl 1332.11106

[17] Winterhof, A., Generalizations of complete mappings of finite fields and some applications, J. Symb. Comput., 64, 42-52, (2014) · Zbl 1332.11107