On the difference between permutation polynomials over finite fields

The well-known Chowla and Zassenhaus conjecture, proven 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 is obtained recently by I¸sök, Topuzo˘glu 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 \( k \) in terms of the Carlitz rank of \( f \) and \( q \). Our results generalize the above mentioned result of I¸sık et al. We also show for a special class of 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 \( k \geq (q - n)/(n + 3) \).

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Mathematics, University of Sarajevo, University of Warwick, Universidade Federal do Rio de Janeiro, Leiden University, Sabancı University
Contributors: Anbar Meidl, N., Odzak, A., Patel, V., Quoos, L., Somoza, A., Topuzoglu, A.
Number of pages: 12
Publication date: 2017
Peer-reviewed: Yes

Publication information
Journal: arXiv
Original language: English
Electronic versions: difference_of_permutation_polynomials.pdf
Source: PublicationPreSubmission
Source-ID: 134439140
Research output: Research - peer-review > Journal article – Annual report year: 2017