Some Criteria for Permutation Binomials over Finite Fields.

A Permutation Binomial $f = x^r + Bx^s$ over a finite field with $p$ elements, $p$ prime, is a function that permutes the elements of the field. Criteria to determine when a binomial is a Permutation Binomial are scarce. Due to its applications, including to cryptography, we want to focus to find criteria for a family of binomials of the form $f = x^{p-4} + Bx^{p-7}$, to be Permutation Binomials. We proved that no such binomials can be found if $p$ is of the form $3k + 4$, moreover we found a relationship between the distribution of quadratic residues over the field and the capacity of $f$ to permute its elements. That is, we found criteria for $f$ to be a Permutation Binomials in terms of the position of $B$ among such quadratic residues. Also we found a suitable formula for the inverse of $f$. We will present such results and future plans involving the inverse of $f$. (Received September 17, 2018)