
QIANG WANG, Carleton University
Ambiguity and Deficiency of Permutations

We introduce the concepts of weighted ambiguity and deficiency, which measures the injectivity and surjectivity of difference mappings respectively, for a given mapping f between two finite Abelian groups of the same size. Then we obtain certain optimal constructions using permutation polynomials over finite fields. Furthermore, we explain their connections with Costas Arrays and Almost Perfect Nonlinear (APN) functions which are employed in some cryptosystems. (joint work with D. Panario, A. Sakzad, and B. Stevens).