
BRETT STEVENS, Carleton University

Sequences in Groups: covering arrays, costas arrays and APN permutations

Sequences can be viewed more generally as maps from one group to another, with the standard domain being the Natural numbers or some subset thereof. We survey some common uses of such sequences for constructing orthogonal covering arrays, Costas arrays and APN permutations. The requirements on the sequences in these three cases are similar and lead to two natural definitions: weighted ambiguity and deficiency. We study the optimum lower bounds of these measures for bijections between two groups of the same size and show that optimal ambiguity implies the APN property. We then examine several constructions of mappings which are optimal with respect to these lower bounds.