Abstract

Boolean functions play an important role in modern cryptography. Despite its conceptual simplicity, what makes the research in Boolean functions challenging is how quickly the number of functions grow as the number of inputs increases, rendering it impossible to make an exhaustive search on the entire space. Boolean functions which are invariant under the action of cyclic rotation of the input variables are known as rotation symmetric Boolean functions. This class of functions were proved to be extremely rich with good cryptographic Boolean functions. Homogeneous rotation symmetric Boolean functions have been extensively studied in recent years due to their applications in cryptography. We give an explicit formula for the number of homogeneous rotation symmetric functions over the finite field $\mathbb{F}_{p^m}$ using Polya's enumeration theorem, which completely solves the open problem proposed by Yuan Li in 2008. This result simplifies the proof and the nonexplicit counting formula given by Shaojing Fu et al. over the field $\mathbb{F}_p$. Much work has been done on counting special types of Boolean functions which are balanced. We derive an explicit count for n-variable balanced rotation symmetric Boolean functions with $n = pq$, where p and q are distinct primes. Another important area of study in the class of rotation symmetric Boolean functions is affine equivalence. Two Boolean functions are affine equivalent if one can be obtained from the other by applying some affine transformation to the input variables. We study the affine equivalence of simplest rotation symmetric Boolean functions called MRS Boolean functions which are generated by the cyclic permutations of the single monomial. Using Pólya's enumeration theorem, we compute the number of affine equivalent MRS Boolean functions. We also concentrated on the generalized class of rotation symmetric Boolean functions called k-rotation symmetric functions. We give an explicit formula for the number of homogeneous k-rotation symmetric Boolean functions using Polya's enumeration theorem and characterize the exact weight and nonlinearity of quadratic 2-MRS Boolean functions.