Chapter 7

Conclusions and Scope for Future Work

7.1 Conclusions

The thesis solves the open problem of enumeration of n-variable homogeneous rotation symmetric Boolean functions over the finite field $\mathbb{F}_{p^m}$ by giving an explicit formula for the number of homogeneous rotation symmetric functions using Polya's enumeration theorem. This result simplifies the proof and the nonexplicit counting formula given by Shaojing Fu et al. over the field $\mathbb{F}_p$.

We derived an explicit count for n-variable balanced rotation symmetric Boolean functions with $n = pq$, where p and q are distinct primes and calculated the weight of MRS functions generated by $x_1x_2....x_d$ of degree greater than $\frac{n}{2}$. We also studied the affine equivalence of simplest rotation symmetric Boolean functions called MRS Boolean functions and give the enumeration for the number of affine equivalent MRS Boolean functions using Pólya's enumeration theorem.

The thesis also contributes to the enumeration of homogeneous k-rotation symmetric Boolean functions by giving an explicit formula using Polya's enumeration theorem and characterizes the exact weight and nonlinearity of quadratic 2-MRS Boolean functions.

7.2 Related Open Problems

We give a short list of open problems and areas of further research.

- Enumeration of n-variable balanced rotation symmetric Boolean functions for general n.
- Characterization of weight and nonliearity of quadratic MRS Boolean functions in n-variables with SANF x_0x_s, $0 < s \leq n-1$ has been well studied. But the similar results for the functions with SANF having more than one term is not known.
- In the case of cubic MRS Boolean functions, relation between weight and nonlinearity of the functions with SANF $x_0x_1x_2$ and $x_0x_ax_{2a}$ has been well studied. But for the general cubic MRS Boolean functions such results are not known. Based on the numerical examples and observations, Cusick conjectured that the nonlinearity of cubic MRS Boolean functions with SANF $x_0x_ax_b$; $(b > a > 0)$ is same as its Hamming weight in the case of odd number of variables.
- We have enumerated the equivalence class of MRS Boolean functions under the action of permutations which preserve rotation symmetry. But the result for general permutations is to be studied further.