1

Classification of RM(6,8)/RM(4,8)

Philippe Langevin
IMATH, UNIVERSITÉ DE TOULON
(Joint work with Valérie Gillot)

Abstract

In our previous work [2], we determined the covering radius of the Reed-Muller code $RM(4,8)$. The numerical result was obtained through several steps. Firstly, we classified the Reed-Muller space $RM(6,8)/RM(4,8)$, denoted as $B(5,6,8)$, and obtained a set of representatives. Details of the results used in obtaining this set are presented in this paper, and the 20748 functions corresponding to this classification are available on the project page [1]. In the second step, we estimated the nonlinearity of the representatives using probabilistic algorithms presented at the ALCOCRYPT conference in February 2023.In this talk, we will focus on the algorithms used to classify $B(5,6,8)$. To this end, we propose new theoretical results that can be used for the classification of quotient spaces of the form $RM(t,m)/RM(t-2,m)$ in general.

Keywords: Affine general linear group, Boolean function, Reed-Müller codes

References

[1] Valérie Gillot and Philippe Langevin. Classification of $B(5,6,8)$. `http://langevin.univ-tln.fr/project/agl8/aglclass.html`, 2023.

[2] Valérie Gillot and Philippe Langevin. Covering radius of $RM(4,8)$. `https://arxiv.org/pdf/2305.03493v1.pdf`, 2023.

*This work is partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012