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

$\mathbb{F}_{q^{15}}$ Paris

Valérie Gillot & Philippe Langevin

Fq15 - June 19-23 2023 -

Institut de Mathématiques de Toulon

website : https://langevin.univ-tln.fr/project/

Introduction

main objective : classification of $RM(6,8)/RM(4,8)$

- Provide a set of orbit representatives under the action $\mathrm{AGL}(8)$

20748 class

classification of RM quotients are useful namely for

- analysis of cryptographic parameters of Boolean functions
- estimation covering radius of Reed-Muller code

ALCOCRYPT : covering radius of $RM(4,8)$: $\rho(4,8) = 26$

Boolean functions

- $\mathbb{F}_2$ the finite field of order 2, m a positive integer
- $B(m)$ the set of Boolean functions in m variables

$$f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$$

Algebraic Normal Form

$$f(x_1, x_2, \ldots, x_m) = f(x) = \sum_{S \subseteq \{1,2,\ldots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2,\ X_S(x) = \prod_{s \in S} x_s.$$

Valuation and degree

- $\mathtt{val}(f)$ is the minimal cardinality of S for which $a_S = 1$
- $\deg(f)$ is the maximal cardinality of S for which $a_S = 1$

By convention $\mathtt{val}(0) = \infty$

Reed-Muller code

Reed-Muller space $RM(k, m)$

- $RM(k, m) = \{f \mid \deg(f) \leq k\}$

Evaluation

$$B(m) \ni f \longrightarrow \big(f(0), f(1), \ldots, f(2^m - 1)\big)$$

Reed-Muller code of order k in m variables

- length : 2^m
- dimension : $\sum_{i=0}^{k} \binom{m}{i}$
- minimum distance : 2^{m-k}
- automorphism group : $\mathrm{AGL}(m)$

$$\begin{array}{c} RM(m, m) \\ \cup \\ RM(m-1, m) \\ \cup \\ \vdots \\ \cup \\ RM(1, m) \\ \cup \\ RM(0, m) \\ \cup \\ (0) \end{array}$$

We identify Reed-Muller space (functions) and Reed-Muller code (codewords)

Reed-Muller quotient

We denote $B(s, t, m)$

the space of Boolean functions of valuation $\geq s$ and degree $\leq t$

$$B(s, t, m) := RM(t, m)/RM(s-1, m)$$

The affine general linear group acts naturally on Boolean functions:

$$\forall \mathfrak{s} \in \mathrm{AGL}(m) \quad \forall f \in B(m) \quad f \circ \mathfrak{s}(x) = f(\mathfrak{s}(x))$$

It acts on $B(s, t, m)$:

$$f \circ \mathfrak{s}(x) \equiv f(\mathfrak{s}(x)) \mod RM(s-1, m)$$

We denote $\widetilde{B}(s, t, m)$

a set of orbit representatives of $B(s, t, m)$ under the action of $\mathrm{AGL}(m)$

classification in dimension 7 and 8

Table: Class numbers of $B(s,t,7)$

$s\backslash t$	1	2	3	4	5	6	7
0	3	12	3486	$10^{13.5}$	$10^{19.8}$	$10^{21.9}$	$10^{22.2}$
1	2	8	1890	$10^{13.1}$	$10^{19.5}$	$10^{21.6}$	$10^{21.9}$
2		4	179	$10^{11.0}$	$10^{17.3}$	$10^{19.5}$	$10^{19.8}$
3			12	**68443**	$10^{11.0}$	$10^{13.1}$	$10^{13.5}$
4				12	**179**	1890	3486
5					4	8	12
6						2	3
7							2

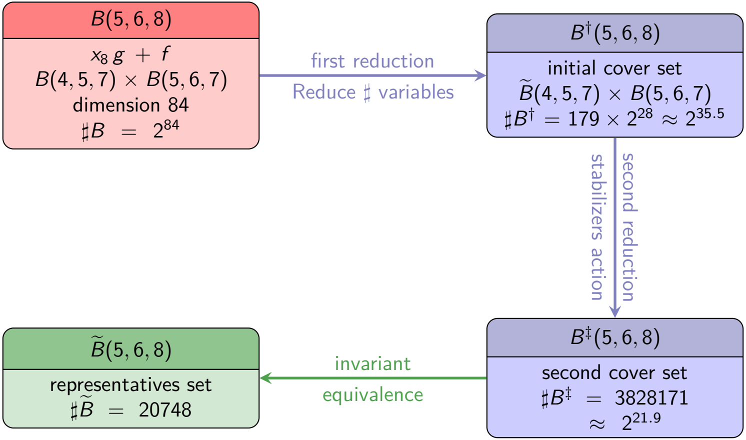
BFA conference

Table: Class numbers of $B(s,t,8)$

$s\backslash t$	1	2	3	4	5	6	7	8
1	2	9	3814830	$10^{27.6}$	$10^{44.5}$	$10^{52.9}$	$10^{55.3}$	$10^{55.6}$
2		5	**20748**	$10^{25.2}$	$10^{42.0}$	$10^{50.5}$	$10^{52.9}$	$10^{53.2}$
3			32	$10^{16.7}$	$10^{33.6}$	$10^{42.0}$	$10^{44.5}$	$10^{44.8}$
4				**999**	$10^{16.7}$	$10^{25.2}$	$10^{27.6}$	$10^{27.9}$
5					32	**20748**	3814830	7611801
6						5	9	14
7							2	3
8								2

$\mathbb{F}_{q^{15}}$ conference

Strategy to classify $B(5,6,8)$



To summarize classification

- Determine a cover set of $B(5,6,8)$ of reasonable size
- Use invariants and equivalence to extract the 20748 classes of $\widetilde{B}(5,6,8)$

First reduction : decrement number of variables

$$B(s,t,m)$$

$$\uparrow$$

$$x_m g + h$$

$$\swarrow \qquad \searrow$$

$$g \in B(s-1,t-1,m-1) \quad h \in B(s,t,m-1)$$

intermediate set

$$B(s,t,m)$$
$$\cup\!\mid$$
Cover Set
$$\cup\!\mid$$
$$\widetilde{B}(s,t,m)$$

$B^\dagger(s,t,m)$ the initial cover set

$m-12$ acts on $B(s,t,m)$ by

$$x_m g + h \mapsto x_m g \circ \mathfrak{s} + h \circ \mathfrak{s}$$

$$B^\dagger(s,t,m) = \left\{ x_m g + h \mid g \in \widetilde{B}(s-1,t-1,m-1), h \in B(s,t,m-1) \right\}$$

$$\sharp B^\dagger(s,t,m) = \sharp \widetilde{B}(s-1,t-1,m-1) \times \sharp B(s,t,m-1)$$

Second reduction : action of stabilizers

- $g \in \widetilde{B}(s-1, t-1, m-1)$
- $\mathfrak{s} \in m-12$ in the stabilizer of g $(g \circ \mathfrak{s} = g)$
- $\alpha \in RM(1, m-1)$

Lemma

1. $x_m g + h$
2. $x_m g + h \circ \mathfrak{s}$
3. $x_m g + h + \alpha g$

are in the same orbit in $\widetilde{B}(s, t, m)$

The $h \mapsto h \circ \mathfrak{s}$ and $h \mapsto h + \alpha g$ make an action on $B(s, t, m-1)$

For each g... $\mathfrak{R}(g)$ denotes an orbit representatives set for the action

$B^{\ddagger}(s, t, m)$ the second cover set

$$B^{\ddagger}(s, t, m) = \bigsqcup_{g \in \widetilde{B}(s-1, t-1, m-1)} \{ \, x_m g + h \mid h \in \mathfrak{R}(g) \, \}$$

$\sharp B^{\ddagger}(s, t, m) = \sum_{g \in \widetilde{B}(s-1, t-1, m-1)} \sharp \mathfrak{R}(g)$

Equivalence, invariant, collision

Equivalence $f \sim f'$

$\exists \mathfrak{s} \in \mathrm{AGL}(m)$ such that

$$f' \equiv f \circ \mathfrak{s} \mod RM(s-1, m)$$

An invariant $j : B(s,t,m) \to X$

- $f \sim f' \Longrightarrow j(f) = j(f')$

Collision

- $j(f) = j(f')$ and $f \not\sim f' \rightsquigarrow$ collision

Of course $f \mapsto \tilde{f}$ is an invariant

Lift by derivation

$v \in \mathbb{F}_2^m, f \in B(m),$ $\quad \mathrm{d}_v(f)(x) = f(x+v) + f(x).$

Derivative of $f \in B(s,t,m)$ is an element of $B(s-1, t-1, m)$

$$\mathrm{Der}_v f(x) \equiv f(x+v) + f(x) \mod RM(s-2, m)$$

Invariant J

$J(f)$ is the distribution of the values of $\widetilde{\mathrm{Der}_v f}$, for all $v \in \mathbb{F}_2^m$

Class of derivative

$$F(f)(v) = \widetilde{\mathrm{Der}_v f}$$

Action of $\mathfrak{s} = (A, a) \in \mathrm{AGL}(m)$ $\quad \mathfrak{s}(x) = A(x) + a$

- $f \in B(m)$
- $A \in \mathrm{GL}\,(m, 2)$ the linear part of $\mathfrak{s}$
- $a \in \mathbb{F}_2^m$ the affine part of $\mathfrak{s}$

$$F(f \circ \mathfrak{s}) = F(f) \circ A$$

Fourier lift

- Assuming that $F(f)(v) \in \mathbb{Z}$

Invariant $\widehat{J}$

$\widehat{J}(f)$ is the values distribution of $\widehat{F}(f)$

Fourier coefficient

$$\widehat{F}(f)(b) = \sum_{v \in \mathbb{F}_2^m} F(f)(v)(-1)^{b.v}$$

In this context

$\widehat{J}$ is more discriminating than J

A^* is the adjoint of $A \in \mathrm{GL}(m)$

$$F(f') = F(f) \circ A \Longleftrightarrow \widehat{F}(f') \circ A^* = \widehat{F}(f)$$

Periodic function in $B(m)$

- Let be $f \in B(m)$

f is v-periodic if

$$\mathrm{d}_v(f) = 0$$

Clearly

$\mathrm{d}_v(f)$ is v-periodic

E_v a supplementary of v $\quad E_v \oplus v = \mathbb{F}_2^m$

the restriction $f|_{E_v}$ is a function in $m-1$ variables

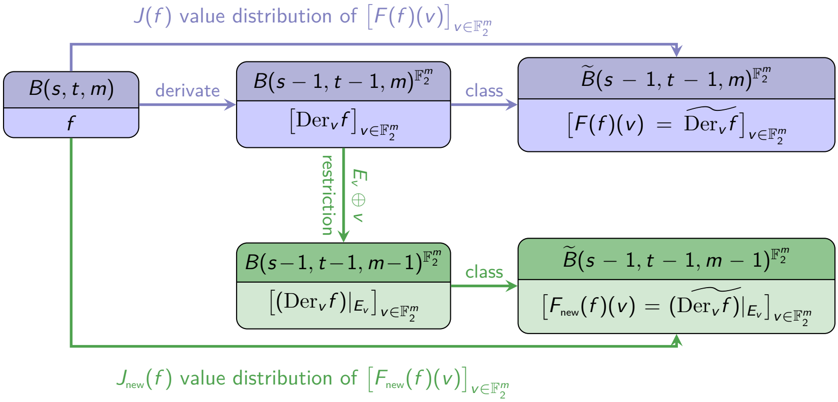
Lemma (Restriction)

f, g two v-periodic functions in $B(m)$.

$$f \sim g \Longrightarrow \forall v \in \mathbb{F}_2^m, \quad f|_{E_v} \sim g|_{E_v}$$

where $\sim$ equivalence in $B(m)$, $\sim$ equivalence in $B(m-1)$

An effective invariant



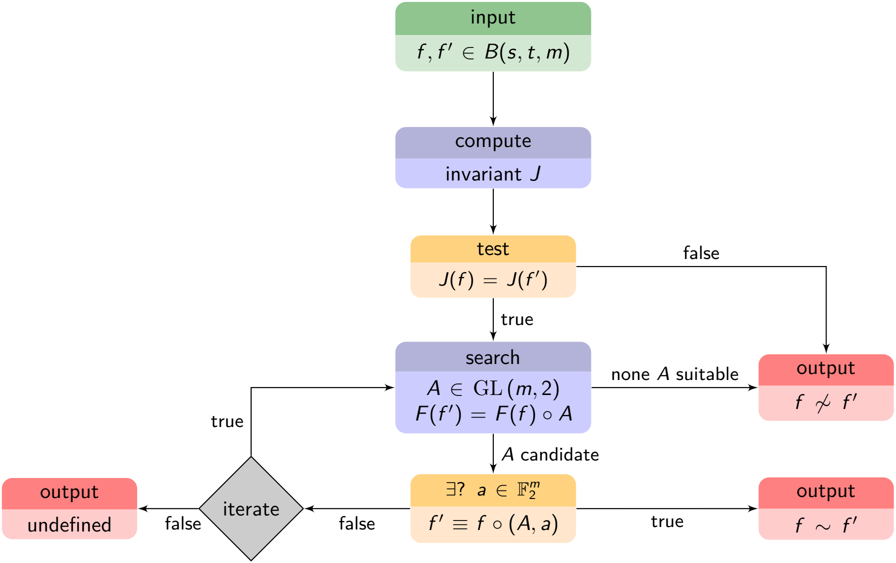
Invariant J_{new}

$J_{\text{new}}(f)$ is the value distribution of $F_{\text{new}}(f)(v)$, for all $v \in \mathbb{F}_2^m$

Derivative restriction class

$$F_{\text{new}}(f)(v) = \widetilde{(\mathrm{Der}_v f)}|_{E_v}$$

Affine equivalence algorithm $\mathfrak{s} = (A, a) \in \mathrm{AGL}(m)$



Existence of $a \in \mathbb{F}_2^m$ in case $s = t - 1$

- f, f' in $B(t-1, t, m)$.
- $A \in \mathrm{GL}(m)$
- $\Delta(f) = \{\mathrm{d}_v(f) \mod RM(t-2, m) \mid v \in \mathbb{F}_2^m\}$

$\Delta(f)$ is a subspace of $B(t-1, t-1, m)$

Affine equivalence Lemma

There exists $a \in \mathbb{F}_2^m$ such that

$$f' \equiv f \circ (A, a) \mod RM(t-2, m) \iff f' \circ A^{-1} + f \in \Delta(f)$$

Target achieved : 20748 classes of $B(5, 6, 8)$

- ✓ We found a cover set $B^{\ddagger}(5, 6, 8)$ of size 3828171
- ✓ The invariant J_{new} finds 20694 distributions (54 collisions)
- ✓ The invariant $\widehat{J_{\text{new}}}$ finds 20742 distributions (6 collisions)
- ✓ The equivalence algorithm detects and solves theses collisions.

Ressources used to extract the 20748 classes of $\widetilde{B}(5, 6, 8)$

- 40 GB of memory (invariant)
- several weeks of computation (equivalence test)

Covering radii of Reed-Muller code of length 256

The classification is a milestone to determine

- covering radius of $RM(4,8)$ into $RM(6,8)$:

$$\rho_6(4,8) = 26$$

- covering radius of $RM(4,8)$:

$$\rho(4,8) = 26$$

website : https://langevin.univ-tln.fr/project/