Classification of Boolean functions

The 7th International Workshop on Boolean Functions and their Applications

Valérie Gillot & Philippe Langevin

BFA - September 11-16 2022


Institut de Mathématiques de Toulon

Introduction

James Maiorana (1991)

presents a recursive algorithm [a] to classify Boolean functions in 6 variables under the action of the affine general linear group modulo functions of degree ≤ 1.

$$RM(6,6)/RM(1,6) = B(2,6,6)$$

[a] A classification of the cosets of the Reed-Muller code $RM(1,6)$, Mathematics of Computation, 1991

New approach

We present a descending procedure to classify in higher dimensions, namely the 68443 classes of

$$RM(4,7)/RM(2,7) = B(3,4,7)$$

This approach computes the 150357 classes of $B(2,6,6)$ in about 15 seconds !

Orbit - Stabilizer - Classification

- Let $(G, *)$ be a finite group
- Let U be a finite set
- A right group action of G on U is a mapping from $U \times G$ to U denoted by $(u, g) \longmapsto u \circ g$ such that :

$$\begin{aligned} \text{(Identity)} \quad & u \circ e = u, \quad u \in U, e \text{ identity of } G \\ \text{(Compatibility)} \quad & (u \circ g) \circ h = u \circ (g * h), \quad u \in U, g, h \in G \end{aligned}$$

- The orbit of an element u : $\mathcal{O}_u = \{u \circ g \mid g \in G\}$
- The stabilizer of u : $\textsc{stab}(u) = \{g \in G \mid u \circ g = u\}$

A classification consists of the data

- a set of orbit representatives R
- a generator set of the stabilizer of each element of R

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

$\mathbb{F}_2$ the finite field of order 2, m a positive integer, $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$

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 $a_S = 1$

$B(s,t,m)$

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

By convention $\mathtt{val}(0) = \infty$ and $B(s,t,m) = \{0\}$ whenever $s > t$

Actions of affine general linear group

Action of $\mathrm{AGL}(m, 2)$ on Boolean functions

$\mathrm{AGL}(m, 2)$ acts naturally on Boolean functions, for $\mathfrak{s} \in \mathrm{AGL}(m, 2)$ and f a Boolean function :

$$f \circ \mathfrak{s}(x) = f(\mathfrak{s}(x))$$

The Reed-Muller spaces $RM(k, m)$

- $RM(k, m) = \{f \mid \deg(f) \leq k\}$
- $(0) \subset RM(0, m) \subset RM(1, m) \subset \cdots \subset RM(m-1, m) \subset RM(m, m)$

Actions of $\mathrm{AGL}(m, 2)$ on Reed-Muller spaces

- Reed-Muller spaces are invariants under the action of $\mathrm{AGL}(m, 2)$
- $\mathrm{AGL}(m, 2)$ acts on $RM(k, m)/RM(r, m)$, $r \leq k$

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

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

Objects at level r - Action modulo $RM(r, m)$

Equivalence at level r

$$f \underset{r}{\sim} g \Longleftrightarrow \exists \mathfrak{s} \in \mathrm{AGL}(m, 2), \quad g \equiv f \circ \mathfrak{s} \mod RM(r, m)$$

Stabilizer at level r

$$\mathrm{STAB}_m^r(f) = \{\mathfrak{s} \in \mathrm{AGL}(m, 2) \mid f \circ \mathfrak{s} \equiv f \mod RM(r, m)\}$$

$$(f + u) \circ \mathfrak{s} = f \circ \mathfrak{s} + u \circ \mathfrak{s} \equiv f + (f + f \circ \mathfrak{s}) + u \circ \mathfrak{s} \mod RM(r - 1, m)$$

Boundary action

$\mathfrak{s} \in \mathrm{STAB}_m^r(f)$ induces an action on the space of forms $B(r, r, m) \ni u$ by :

$$u \longmapsto u \circ \mathfrak{s} + f \circ \mathfrak{s} + f \mod RM(r - 1, m)$$

Orbit at level $r-1$ from classification at level r.

Lemma (Boundary)

If

- $\mathcal{R}$ *is a set of orbit representatives of degree* k *at level* r,
- *for each* $f \in \mathcal{R}$,
  - $\mathcal{U}(f)$ *denotes a set of orbit representatives of* $B(r, r, m)$ *under the boundary action of* $\mathrm{STAB}_m^r(f)$,

then the set

$$\{f + u \mid \quad f \in \mathcal{R}, \quad u \in \mathcal{U}(f)\}$$

is nothing but a set of orbit representatives with same degree at level $r-1$.

not yet a classification!

The order of $\mathrm{STAB}_m^{r-1}(f+u)$ is known, it remains to find a generators set...

Generators set of stabilizer

Let G a group acting on the right over a set U

- L a set of generators of G
- $u \circ s$ the action of $s \in G$ on $u \in U$
- $\mathcal{O}_u$ the orbit of u
- $u \circ R(x) = x,\ x \in \mathcal{O}_u$
- S_u the stabilizer of u
- s_u the order of S_u

$$\begin{tikzcd}
& u \arrow[dr, "R(x)"] & \\
x \circ \lambda \arrow[ur, "R(x\circ\lambda)^{-1}"] & & x \arrow[ll, "\lambda"]
\end{tikzcd}$$

Recall that,

$$s_u := \sharp S_u = \frac{\sharp G}{\sharp \mathcal{O}_u} \qquad \text{(class formula)}$$

Lemma (Schreier)

If $R\colon \mathcal{O}_u \to G$ is a map such that $u \circ R(x) = x$ for all $x \in \mathcal{O}_u$ then $\{R(x)\lambda R(x \circ \lambda)^{-1} \mid \lambda \in L, x \in \mathcal{O}_u\}$ spans the stabilizer S_u of u.

Find a generator set

```
Algorithm generatorSet( u , L, s_u)
// return a generator set of the stabilizer of u under the action of the
     group (G,*) generated by L knowing its order s_u
    S ←∅
    push( u )
    R [ u ] ←id
    Y ←{ u }
    while ( order( <S> ) < s_u) {
        pop( x )
        for λ∈L {
            y ←x ∘ λ
            if y ∉Y {
                push(y)
                R[ y ] ←R[ x ] * λ
                Y← Y  ∪ {y}
            } else {
              s ←R[x] * λ * inverse( R[ y ] )
              if ( s not in <S> )
                 S ←S  ∪ { s }
            }
        }
    return S
```

Classify $RM(k, m)$ by descending procedure

$$B(k+1, k, m) = \{0\}$$
$$\downarrow$$
$$B(k, k, m)$$
$$\downarrow$$
$$B(k-1, k, m)$$
$$\downarrow$$
$$\vdots$$
$$\downarrow$$
$$B(r+1, k, m)$$
$$\downarrow\downarrow$$
$$B(r, k, m)$$
$$\downarrow$$
$$\vdots$$
$$\downarrow$$
$$B(0, k, m) = RM(k, m)$$

Input : classification of $B(r+1, k, m)$

- $\mathcal{R}$ an orbit representatives set at level r
- a generator set of $\mathrm{STAB}^r_m(f)$

Compute boundary orbits

for each $f \in \mathcal{R}$, compute an orbit representatives set $\mathcal{U}(f)$ of the action of $\mathrm{STAB}^r_m(f)$ over $B(r, r, m)$

Apply `generatorSet` algorithm

for each $f \in \mathcal{R}$, for each $u \in \mathcal{U}(f)$: determine a generator set of the stabilizer of $f + u$ at level $r - 1$

Output : classification of $B(r, k, m)$

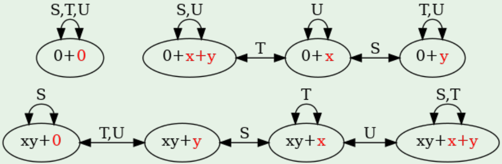
Baby example $m = 2$

- $\sharp\mathrm{AGL}(2,2) = (2^2-1)(2^2-2)\times 2^2 = 24$

Input : $B(3,2,2) = \{0\}$

Boundary action over $B(2,2,2)$: level 1

Boundary action over $B(1,1,2)$: level 0



- $\mathrm{AGL}(2,2) = \langle S, T, U\rangle$, Shift (S), Tranvection (T), translation (U)
-

$\mathrm{AGL}(2,2)$	x	y
S	y	x
T	$x+y$	y
U	$x+1$	y

- at level 1 mod $RM(1,2)$:

$$
\begin{aligned}
xy \circ S &= yx \equiv xy\\
xy \circ T &= (x+y)y = xy + y\\
&\equiv xy\\
xy \circ U &= (x+1)y = xy + y\\
&\equiv xy
\end{aligned}
$$

- at level 0 mod $RM(0,2)$:

$$
\begin{aligned}
(xy + x) \circ S &= yx + y \equiv xy + y\\
(xy + x) \circ T &= (x+y)y + x + y\\
&\equiv xy + x\\
(xy + x) \circ U &= (x+1)y + x + 1\\
&\equiv xy + x + y
\end{aligned}
$$

Numerical results for $m = 7$

Table: Class numbers $\mathrm{n}(s, t, 7)$

$s \backslash t$	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

Full details of results

- Number of classes
- Orbit representatives set
- Generator set of stabilizer

http://langevin/project/agl7/aglclass.html

Input : classification of $B(4, 4, 7)$

12 classes

Compute boundary orbits

- dim $B(3, 3, 7) = 35$
- RAM : 50 GB
- $\approx$ 3 days

genenatorSet

Few minutes

Output : classification of $B(3, 4, 7)$

68443 classes

Conclusion

The descending procedure successfully classifies Boolean functions in 7 variables.

Our detailed numerical results may be used namely for :

- the analysis of cryptographic parameters of Boolean functions
- the estimation of covering radii of Reed-Muller codes

Valérie and Philippe in 1991 when Maiorana classifies $B(2,6,6)$!