Covering radius of $RM(4, 8)$

Valérie Gillot & Philippe Langevin

ALCOCRYPT 2023
CIRM Luminy- February 20-24 2023

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

Introduction

Covering radius for Reed-Muller codes of length 2^7

- 2019 : Wang & Stănică find the covering radius of $RM(2,7)$ is 40
- 2022 : Gao, Kan, Li & Wang find the covering radius of $RM(3,7)$ is 20

All covering radii are known for Reed-Muller codes of this length

Results of Dougerthy, Mauldin & Tiefenbruck

- 2022 : bounds for covering radius of $RM(m-4,m)$ in $RM(m-3,m)$
- Covering radius of $RM(4,8)$ in $RM(5,8)$ is 26

Present work (VG & PL)

- 202x : Classification of some cosets of the Reed-Muller codes
- Determine the covering radius of $RM(4,8)$ is 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}

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

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

Nonlinearity & covering radii

- $f \in B(m)$, space of boolean functions in m variables
- the Hamming weight of f is the number of 1 in $\big(f(0), f(1), \ldots, f(2^m - 1)\big)$

Nonlinearity of order k

$$\mathrm{NL}_k(f) = \min_{g \in RM(k,m)} \mathrm{wt}\,(f + g) = \mathrm{distance}\big(f, RM(k,m)\big)$$

Covering radius $\rho(k,m)$ of $RM(k,m)$

$$\rho(k,m) = \max_{f \in B(m)} \mathrm{NL}_k(f)$$

Covering radius of $RM(k,m)$ into $RM(t,m)$ $\quad (k \leq t)$

$$\rho_t(k,m) = \max_{f \in RM(t,m)} \mathrm{NL}_k(f)$$

Bounds for covering radii in 8 variables

Table: Updated table of Handbook of coding theory

k	1	2	3	4	5	6	7	8
$\rho(k,8)$	120	$88^a - 96$	$50^b - 67$	$26^c - 28^d$	10	2	1	0
				26^e				

(a) J.-P. Zanotti, PL (1998)

(b) G. Leander, PL (2005)

(c) R. Dougherty et al. (2022)

$$\rho_5(4,8) = 26$$

(d-e) The present work gives

$$\rho_6(4,8) = 26 \quad \text{and also} \quad \rho(4,8) = 26$$

How to deduce $\rho_6(4,8)$ from $\rho_5(4,8) = 26$

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

It is sufficient to check that for all $f \in RM(6,8)$

$$\mathrm{NL}_4(f) \leq 26$$

To check $\mathrm{NL}_4(f) \leq 26$

We search for a function of weight ≤ 26 in the translate $f + RM(4,8)$ by randomly generating functions of weight $\leq 256 - 163 = 93$

$\sharp RM(6,8)/RM(4,8) = 2^{84}$ rather huge !

We have to reduce the search space...

random reduced generator matrix of $RM(k,m)$

$$\left[\begin{array}{ccccccccc}
1 & 0 & 0 & \cdots & 0 & * & \cdots & * \\
0 & 1 & 0 & \cdots & 0 & * & \cdots & * \\
0 & 0 & 1 & \cdots & 0 & * & \cdots & * \\
\vdots & & & \ddots & 0 & * & \cdots & * \\
0 & 0 & 0 & \cdots & 1 & * & \cdots & *
\end{array}\right]$$

$$\underbrace{\begin{bmatrix} * & * & * & \cdots & * \end{bmatrix}}_{k=163} \underbrace{\begin{bmatrix} * & \cdots & * \end{bmatrix}}_{n-k=93} f$$

$$\underbrace{\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \end{bmatrix}}_{k=163} \underbrace{\begin{bmatrix} * & \cdots & * \end{bmatrix}}_{n-k=93}$$

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 $\mathrm{AGL}(m)$

Reduce the search space

Using $\mathrm{AGL}(m)$ action

$$\begin{aligned}\rho_t(s-1,m) &= \max_{\deg(f)\le t} \mathrm{NL}_{s-1}(f)\\ &= \max_{f\in B(s,t,m)} \mathrm{NL}_{s-1}(f)\\ &= \max_{f\in \widetilde{B}(s,t,m)} \mathrm{NL}_{s-1}(f)\end{aligned}$$

$$\rho_6(4,8) = \max_{f\in \widetilde{B}(5,6,8)} \mathrm{NL}_4(f)$$

By Burnside Lemma

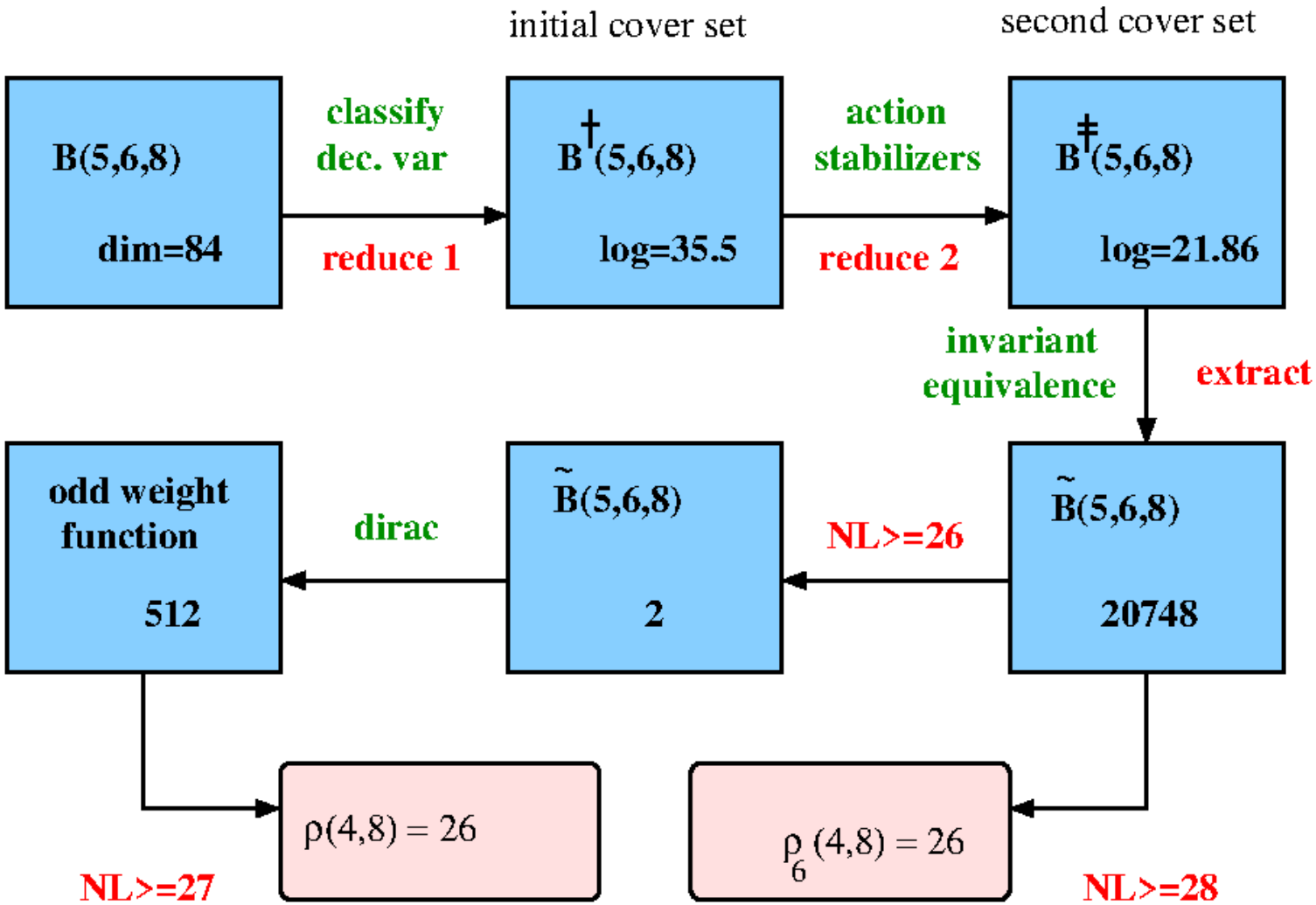
$$\sharp\widetilde{B}(5,6,8) = 20748$$

To summarize

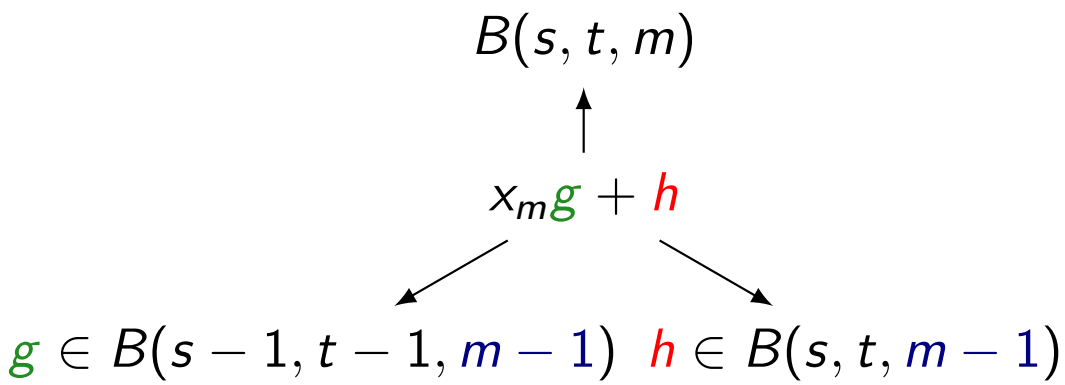
- Classify
  - Determine a cover set of $B(5,6,8)$ of reasonable size
  - Use invariants to extract the 20748 classes of $\widetilde{B}(5,6,8)$
- Check for all $f \in \widetilde{B}(5,6,8)$ that

$$\mathrm{NL}_4(f) \le 26$$

leitfaden


initial cover set
second cover set
B(5,6,8)
dim=84
classify
dec. var
reduce 1
B†(5,6,8)
log=35.5
action
stabilizers
reduce 2
B‡(5,6,8)
log=21.86
invariant
equivalence
extract
odd weight
function
512
dirac
B̃(5,6,8)
2
NL>=26
B̃(5,6,8)
20748
ρ(4,8) = 26
NL>=27
ρ6(4,8) = 26
NL>=28

First reduction : decrement number of variables



intermediate set

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

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

$\mathrm{AGL}(m-1)$ 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

- $g \in \widetilde{B}(s-1, t-1, m-1)$
- $\mathfrak{s} \in \mathrm{AGL}(m-1)$ 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

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

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

Reduction of $B(5,6,8)$

$$B(5,6,8) = B(4,5,7) \times B(5,6,7)$$
$$\sharp B(5,6,8) = 2^{21} \times 2^{28} = 2^{49}$$

Inital cover set

$$B^{\dagger}(5,6,8) = \widetilde{B}(4,5,7) \times B(5,6,7) \qquad B^{\dagger}(5,6,8) = B(4,5,7) \times \widetilde{B}(5,6,7)$$

$$\sharp B^{\dagger}(5,6,8) = 179 \times 2^{28} \approx 2^{35.5} \qquad \sharp B^{\dagger}(5,6,8) = 2^{56} \times 8 = 2^{59}$$

Second cover set

$$\sharp B^{\ddagger}(5,6,8) = 3828171 \approx 2^{21.9}$$

Now, extract $\sharp\widetilde{B}(5,6,8) = 20748$ orbit representatives from 3828171 functions

Invariant approach to classify $B(s,t,m)$

- $f \in B(s,t,m)$, $v \in \mathbb{F}_2^m$
- $\mathrm{Der}_v(f)(x) \equiv f(x+v) + f(x) \mod RM(s-2,m)$

$$F(f) = \widetilde{\mathrm{Der}_\cdot(f)} : \mathbb{F}_2^m \longrightarrow \widetilde{B}(s-1,t-1,m)$$
$$v \mapsto F(f)(v) = \widetilde{\mathrm{Der}_v(f)}$$

- $J(f)$ is the distribution of the values of $F(f)(v)$

Lemma J is an invariant

Considering the linear part $A \in \mathrm{GL}(m)$ of $\mathfrak{s} = (A,a)$, $\mathfrak{s}(x) = A(x) + a$, we have

$$F(f') = F(f) \circ A$$

Recall $f \sim f'$, $\exists \mathfrak{s} \in \mathrm{AGL}(m)$ such that $f' \equiv f \circ \mathfrak{s} \mod RM(s-1,m)$

A more discriminating invariant

- $F(f)(v) \in \mathbb{N}$
- $\widehat{F}(f)(b) = \sum_{v \in \mathbb{F}_2^m} F(f)(v)(-1)^{b.v}$ its Fourier transform
- $\widehat{J}$ the invariant corresponding the values distribution of $\widehat{F}(f)$

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

$$F(f') = F(f) \circ A$$

becomes

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

We use J (or $\widehat{J}$) to determine candidates A (or A^*) for the linear part of an action $\mathfrak{s} = (A, a)$ over $B(s, t, m)$

Now, it remains to verify the existence of an affine part a of $\mathfrak{s} = (A, a)$

Affine equivalence case $s = t - 1$

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

Affine equivalence Lemma

There exists $a \in \mathbb{F}_2^m$ such that $f' \equiv f \circ (A, a) \mod RM(t-2, m)$ if and only if $f' \circ A^{-1} + f \in \Delta(f)$.

`Equivalent(`f`,`f'`,iter)`

An algorithm ending with one of following three values :

$$\begin{cases} \texttt{NotEquiv}, & \text{all potential candidates } A \text{ were tested, so } f \not\sim f'; \\ \texttt{Equiv}, & \text{there exists } a \text{ such that } (A, a) \text{ to prove } f \sim f'; \\ \texttt{Undefined}, & \texttt{iter} \text{ is too small to conclude.} \end{cases}$$

✓ `iter` ranges from 1024 to 2^{23} depending on the situation

Progress report

- ✓ We found a cover set of $B(5, 6, 8)$ of size 3828171
- ✓ We extracted the 20748 classes of $\widetilde{B}(5, 6, 8)$ with invariant approach and `equivalent` algorithm
  - 40 GB of memory (invariant)
  - several weeks of computation (equivalence test)
- We finally check

$$\mathrm{NL}_4(f) \leq 26, \quad \forall f \in \widetilde{B}(5, 6, 8),$$

  - 48 processors
  - 1 day of computation (checking nonlinearity)

Consequences for the covering radii

Covering radius of $RM(4,8)$ into $RM(6,8)$

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

Covering radius of $RM(4,8)$

$$\rho(4,8) \leq \rho_6(4,8) + \rho(6,8) = 28$$

Easy but very Important remark

$$\exists f \in B(8), \quad \mathrm{NL}_4(f) = 28 \Longrightarrow \exists g \in B(8), \quad \mathrm{NL}_4(g) = 27$$

Nonlinearity of odd weight functions

An odd weight function is at distance one from $RM(6,8)$.

In order to prove the non existence of odd weight function at distance 27 from $RM(4,8)$, we have to estimate :

$$\max \mathrm{NL}_4(f+\delta_a), \qquad a \in {\mathbb{F}_2}^8, \quad f \in B(5,6,8)$$

Only two classes of $B(5,6,8)$ have non linearity ≥ 26 :

$$abcdf + abcef + abdeg + abcdeh + bcefh + adefh + bcdgh + acegh + abfgh$$

$$abcef+acdef+abcdg+abdeg+abcfg+acdeh+abcfh+bdefh+bcdgh+abegh+adfgh+cefgh$$

covering radius

It is easy to check $\deg(f) = 8 \Longrightarrow \mathrm{NL}_4(f) \leq 25$ and consequently

$$\rho(4,8) = \rho_6(4,8) = \rho_5(4,8) = 26$$

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