

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

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

Valuation and degree

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

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

Reed-Muller code

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

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

Evaluation

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

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 $(f(0), f(1), \dots, f(2^m - 1))$

Nonlinearity of order k

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

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

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

Covering radius of $\text{RM}(k, m)$ into $\text{RM}(t, m)$ ($k \leq t$)

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

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. Zanolli, 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 $f \in RM(6, 8)$

$$NL_4(f) \leq 26$$

To check $NL_4(f) \leq 26$

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

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

We have to reduce the search space...

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

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & * & \cdots & * \\ 0 & 1 & 0 & \cdots & 0 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & 0 & * & \cdots & * \\ \vdots & & & \ddots & & & & \\ 0 & 0 & 0 & \cdots & 1 & * & \cdots & * \end{bmatrix}$$

$$\begin{bmatrix} * & * & * & \cdots & * \end{bmatrix} \begin{bmatrix} * & \cdots & * \end{bmatrix} f$$

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

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:

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

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

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

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

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

Reduce the search space

Using $AGL(m)$ action

$$\begin{aligned}\rho_t(s-1, m) &= \max_{\deg(f) \leq t} NL_{s-1}(f) \\ &= \max_{f \in B(s, t, m)} NL_{s-1}(f) \\ &= \max_{f \in \tilde{B}(s, t, m)} NL_{s-1}(f)\end{aligned}$$

$$\rho_6(4, 8) = \max_{f \in \tilde{B}(5, 6, 8)} NL_4(f)$$

By Burnside Lemma

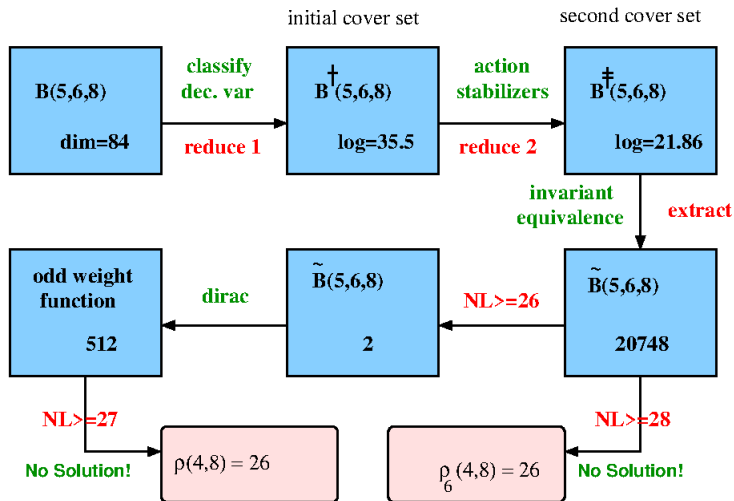
$$\#\tilde{B}(5, 6, 8) = 20748$$

To summarize

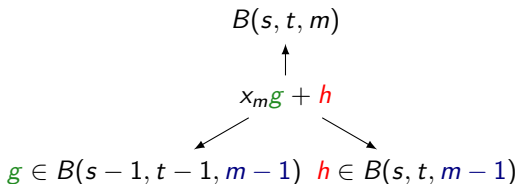
- Classify
 - Determine a **cover set** of $B(5, 6, 8)$ of reasonable size
 - Use **invariants** and **equivalence** to extract the 20748 classes of $\tilde{B}(5, 6, 8)$
- Check for all $f \in \tilde{B}(5, 6, 8)$ that

$$NL_4(f) \leq 26$$

leitfaden



First reduction : decrement number of variables



intermediate set

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

\cup

Cover Set

\cup

$$\tilde{B}(s, t, m)$$

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

AGL($m-1$) acts on $B(s, t, m)$ by

$$x_m g + h \mapsto x_m g \circ s + h \circ s$$

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

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

Second reduction : action of stabilizers

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

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 $\tilde{B}(s, t, m)$

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

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

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

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

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

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

$$B(5, 6, 8) = B(4, 5, 7) \times B(5, 6, 7)$$

$$\#B(5, 6, 8) = 2^{56} \times 2^{28} = 2^{84}$$

Initial cover set

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

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

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

$$\#B^\dagger(5, 6, 8) = 2^{56} \times 8 = 2^{59}$$

Second cover set

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

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

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

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

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

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

Lemma J is an invariant

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

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

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

A more discriminating invariant

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

For $A \in GL(m)$, 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 $B(t - 1, t, m)$.
- $A \in \text{GL}(m)$
- $\Delta(f) = \{\text{Der}_v(f) \mid v \in \mathbb{F}_2^m\}$ a subspace of $B(t - 2, t - 1, m)$

Affine equivalence Lemma

There exists $a \in \mathbb{F}_2^m$ such that $f' \equiv f \circ (A, a) \pmod{RM(t - 2, m)}$ 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 :

- NotEquiv, all potential candidates A were tested, so $f \not\sim f'$;
- Equiv, there exists a such that (A, a) to prove $f \sim f'$;
- Undefined, iter is too small to conclude.

✓ 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 $\tilde{B}(5, 6, 8)$ with invariant approach and equivalent algorithm
 - 40 GB of memory (invariant)
 - several weeks of computation (equivalence test)
- We finally check

$$NL_4(f) \leq 26, \quad \forall f \in \tilde{B}(5, 6, 8),$$

- 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

$$\exists f \in B(8), \quad NL_4(f) = 28 \implies \exists g \in B(8), \quad NL_4(g) = 27$$

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 :

$$\max NL_4(f + \delta_a), \quad a \in \mathbb{F}_2^8, \quad f \in B(5, 6, 8) \text{ such that } NL_4(f) = 26$$

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 $\deg(f) = 8 \implies NL_4(f) \leq 25$ and consequently

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



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