Classification of the boolean cubics of 9 variables

Eric BRIER

Gemplus

Security Technology Dpt.

eric.brier@gemplus.com

Philippe LANGEVIN

Université de Toulon

GRIM

langevin@univ-tln.fr

Arithmétique et combinatoire

Luminy, 23–27 septembre 2002

Reed-Muller codes

Let f be a boolean function mapping $\mathbf{F}_2^m$ to $\mathbf{F}_2$.

$$f(X_1, X_2, \ldots, X_m) = \sum_{S \subset \{1,2,\ldots,m\}} a_S X_S$$

$$X_S = \prod_{i \in S} X_i$$

$$\deg(f) = \sup\{\mathrm{card}(S) \mid a_S = 1\}$$
$$\mathrm{wt}(f) = \mathrm{card}\{x \in \mathbf{F}_2^m \mid f(x) = 1\}$$

$\diamond$ The set of boolean functions of degree $\leq r$ is the Reed-Müller code $\mathrm{RM}(r, m)$ of order r with m variables, or length 2^m.

Reed (1954), Müller, (1954).

$\mathrm{RM}(1, 5)$ used on Mariner '69.

The standard parameters of $\mathrm{RM}(r,m)$ are well known : length 2^m, dimension $\sum_{i=0}^{r}\binom{m}{i}$, minimal distance 2^{m-r}, divisibility of the weights (Ax 1962, McEliece 1972) and automorphisms group.

$$\mathrm{RM}(r,m)^{\perp} = \mathrm{RM}(m-r-1,m)$$

There exists formulas for weight distribution of the Reed-Müller codes of order 0, 1 and 2, and by duality $m-3$, $m-2$, $m-1$, m.

The weight distribution of the $\mathrm{RM}(r,m)$ unknown.

▷ The record : Sugita, Kasami, Fujiwara, The weight distribution of the third-order Reed-Muller code of length 512 (1996).

i.e. $\mathrm{RM}(3,9)$.

Classification of boolean Functions

The linear group $\mathrm{GL}(m,2)$ acts over the Reed-Müller codes thus on the quotient space $\mathrm{RM}^*(r,m) := \mathrm{RM}(r,m)/\mathrm{RM}(r-1,m)$.

classification in $\mathrm{RM}^*(3,m)$ $\approx$ distribution of $\mathrm{RM}(3,m+1)$

◇ Let $n(r,m)$ be the number of orbits in $\mathrm{RM}^*(r,m)$

Let A_1, A_2, ... , A_t representatives of the conjugacy classes of $\mathrm{GL}(m,2)$.

$$n(r,m) = \sum_{i=1}^{t} \frac{2^{\binom{m}{r} - \mathrm{rank}\left(C_r(A_i) - \mathrm{Id}\right)}}{\sharp\mathrm{cent}_{\mathrm{GL}(m,2)}(A_i)}$$

Xiang-Dong Hou, (1996).

$C_r(A)$ is the r-compound matrix of A.

What can be done ?

For the linear and quadratic forms :

$$n(1,m) = 2, \quad n(2,m) = \lfloor \frac{m}{2} \rfloor + 1.$$

Hou formula gives

r/m	6	7	8	9	10
3	6	12	32	349	3691561
4	4	12	999	10^{15}	∞

For small m,

$m = 5$, Berlekamp-Welch (1971)

$m = 6$, Rothaus (1976)

$m = 7$, Hou (1993)

$m = 8$, Hou (1996) ....used by Kasami, Fujiwara, Sugita.

Invariants

- Let $A.f$ the action of $A \in \mathrm{GL}(m,2)$ on $f \in \mathrm{RM}^*(r,m)$.

  $$g \sim f \iff \exists A \in \mathrm{GL}(m,2), \quad A.f \equiv g \pmod{\mathrm{RM}(r-1,m)}$$

- An invariant is a map χ s. t. $f \sim g \Longrightarrow \chi(f) = \chi(g)$.
- The **complementary map**

$$\mathrm{comp}\colon \mathrm{RM}^*(r,m) \to \mathrm{RM}^*(m-r,m)$$
$$f \mapsto \sum_S a_S X_{\{1,2,\dots,m\}\setminus S}$$

if χ is an invariant of degree r then $\chi \circ \mathrm{comp}$ is an invariant of degree $m-r$, denoted χ^c.

The naive algorithm

```
val := {}
rep := {}
repeat
      f := random of degree <=  r
      t := chi( f )
      if t  is not in val then
         append t to val
         append f to rep
      fi
until :-)
```

We need **good** invariants ! Splitting the space. Easy to compute.

Examples of invariants

Let i, j be integers such that $i+j=r$. Let $f \in \mathrm{RM}^*(r,m)$. We construct a $\binom{m}{i} \times \binom{m}{j}$-matrix $M(f)$ indexed by ordered pairs (x,y) of subsets of order i, j such that $\mathrm{card}(x \cup y) = r$.

$$M(f)[x,y] = a_{x \cup y}.$$

$\mathrm{inv}_{i,j}(f) := \mathrm{rank}\big(M(f)\big)$ is an invariant.

$\mathrm{inv}_{1,2}$	7 values	5 classes
$\mathrm{inv}^c_{2,2}$	7 values	4 classes
both		6 classes

— 6 of the 12 classes in 7 variables.

The derivation

- ◇ The **derivation** of f in the **direction** of $u \in \mathbf{F}_2^m$ is

$$\mathrm{der}_u(f)(x) := f(x+u) + f(x)$$

- ▷ The derivation is bilinear on $\mathbf{F}_2^m \times \mathrm{RM}^*(r, m)$.

$$\mathrm{der}_{u+v} f = \mathrm{der}_u f + \mathrm{der}_v f$$

$$\mathrm{der}_u A.f = \mathrm{der}_{Au} f$$

An invariant χ of degree $r-1$ lifts to an invariant of degree r

$$\chi' := \text{distribution of } [\chi(\mathrm{der}_u f)]_{u \in \mathbf{F}_2^m}$$

The $\mathrm{inv}'_{1,1}$ splits completely the set of cubics of 7 variables.

—

$\mathrm{inv}_{1,2}$	8 values	6 classes
$\mathrm{inv}^{c}_{2,3}$	28 values	11 classes
both		13 classes
$\mathrm{inv}'_{1,1}$		27 classes
all		29 classes

— 29 of the 32 classes in 8 variables.

A Fourier trick

Let $F\colon \mathbf{F}_2^m \to \mathbf{C}$ be a complex function. The **Fourier coefficient** of F at $a \in \mathbf{F}_2^m$ is

$$\hat{F}(a) = \sum_{x \in \mathbf{F}_2^m} F(x)(-1)^{a.x}$$

- ▷ if F and G are in the same orbit under the action of $\mathrm{GL}(m, 2)$ then distribution of the Fourier coefficient are equal.

- ▷ An invariant χ of degree $r-1$ lifts to an invariant of degree r

$$\chi^* := \text{spectrum of } u \mapsto \chi(\mathrm{der}_u f)$$

$\mathrm{inv}_{1,1}^*$ splits completely $\mathrm{RM}^*(3,8)$ in 32 class of cubics.

9 variables

$\mathrm{inv}_{1,2}$	9 values	7 classes
$\mathrm{inv}^c_{3,3}$	84 values	24 classes
both		28 classes
$\mathrm{inv}'_{1,1}$		174 classes
$\mathrm{inv}^*_{1,1}$		335 classes
$\mathrm{inv}^c_{3,3}$ & $\mathrm{inv}^*_{1,1}$		344 classes

The results have been obtained after 1 month of computation by a C-program on a alpha machine.

Check of invariants

A Class that appears with the frequency ν has an apparent fixator F_a given by

$$F_a = \frac{\sharp \mathrm{GL}(m,2)}{2^{\binom{m}{3}} \times \nu}$$

In the case of F_a **small** we may compute the true fixator of one representative to detect "collisions" i.e. functions $f \not\sim g$ such that

$$\chi(f) = \chi(g).$$

After 5×10^6 iterations in the algorithm, we were able to detect 4 collisions whence we have (virtually) found 348 cubics !

Collisions

cpt	F_a	F_c	cubic
181281	1	1	125+135+245+345+126+246+346+056+...
181277	1	2	124+235+245+345+236+146+246+056+...
180742	1	2	123+124+234+235+245+345+136+236+...
180591	1	2	124+134+234+135+136+246+056+127+...
180482	1	2	012+123+124+034+134+234+125+135+...
91269	2	2	124+234+235+245+345+126+136+236+...
90993	2	2	124+134+234+245+345+136+246+346+...
90728	2	2	123+125+235+245+246+056+256+356+...
90719	2	2	123+124+235+245+345+236+146+246+...
90708	2	2	134+234+135+235+245+345+126+246+...

At this times we have 4 collisions, that 348 cubics detected.

The restriction

Let $\pi\colon \mathbf{F}_2^{m-1} \longrightarrow H$ be a parameterization of an hyperplane

◇ The **restriction** of $f \in \mathrm{RM}(r,m)$ with **respect** to $\pi$is

$$\mathrm{res}_\pi(f) := f \circ \pi$$

▷ The function $\mathrm{res}_\pi(f)$ lies in $\mathrm{RM}(r,m-1)$, if π' is an other parameterization of H then

$$\mathrm{res}_\pi(f) \sim \mathrm{res}_{\pi'}(f)$$

An $(r,m-1)$-invariant χ lifts to an (r,m)-invariant

$$\chi^r := \text{distribution of } [\chi(\mathrm{res}_{u^\perp}(f))]_{u \in \mathbf{F}_2^m}$$

$$\boxed{(\mathrm{inv}_{1,1}^*)^r \text{ complexity } \mathrm{O}(2^{2m} m^4) \text{ splits completely } \mathrm{RM}(3,9)}$$

Complete Enumeration

◇ A **complete enumeration** of $\mathrm{RM}^*(r,m)$ is a list of inequivalent forms f given with its orbit size $\nu(f)$.

▷ Using a complete enumeration X of $\mathrm{RM}^*(r-1,m-1)$ and an (r,m)-invariant, we can construct a complete enumeration of $\mathrm{RM}^*(r,m)$ by means of counting formula :

$$\begin{aligned}\nu(f) &= \sum_{g\in X} \nu(g) \times \sharp\{g+qx_m \sim f \mid q \in \mathrm{RM}^*(r-1,m-1)\} \\ &= \sum_{g\in X} \nu(g) \times \sharp\{g+qx_m \sim f \mid q \in W(g)\} \times 2^{\mathrm{var}(g)}\end{aligned}$$

where $W(g)$ is a supplementary of $V(g) := \{\mathrm{der}_u(g) \mid u \in \mathbf{F}_2^{m-1}\}$ in $\mathrm{RM}(r-1,m-1)$. The dimension $V(g)$ equals to the minimal number of variables $\mathrm{var}(g)$ to express g up to GL equivalence.

Conclusion

We have find a complete enumeration of RM$(3,9)$. This result can be used to determine :

- The weight distribution of the RM$(3,10)$.
- The covering radius of RM$(3,9)$ in RM$(2,9)$.