



# On the number of bent functions with 8 variables

P. Langevin, P. Rabizzoni, P. Véron, J.-P. Zanotti

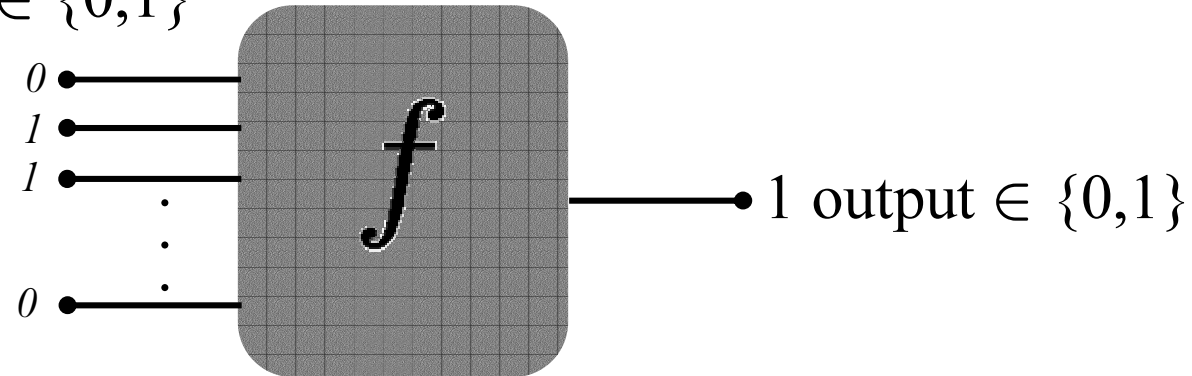
Groupe de Recherche en Informatique  
et Mathématiques

Université du Sud Toulon-Var



## Boolean functions

$m$  inputs  $\in \{0,1\}$



$f: \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$  has a unique representative polynomial in  $\mathbb{F}_2[X_1, \dots, X_m] / (X_1^2 - X_1, \dots, X_m^2 - X_m)$

$$f = \sum_{S \subset \{1, \dots, m\}} a_S X_S, \quad a_S \in \mathbb{F}_2 \quad X_S = \prod_{s \in S} X_s$$

**ANF**

Ex :  $m = 6$ ,  $f = X_1 X_2 X_5 X_6 + X_2 X_3$   $a_{1256} = a_{23} = 1$

**degree 4**



### Bent functions ( $m$ even)

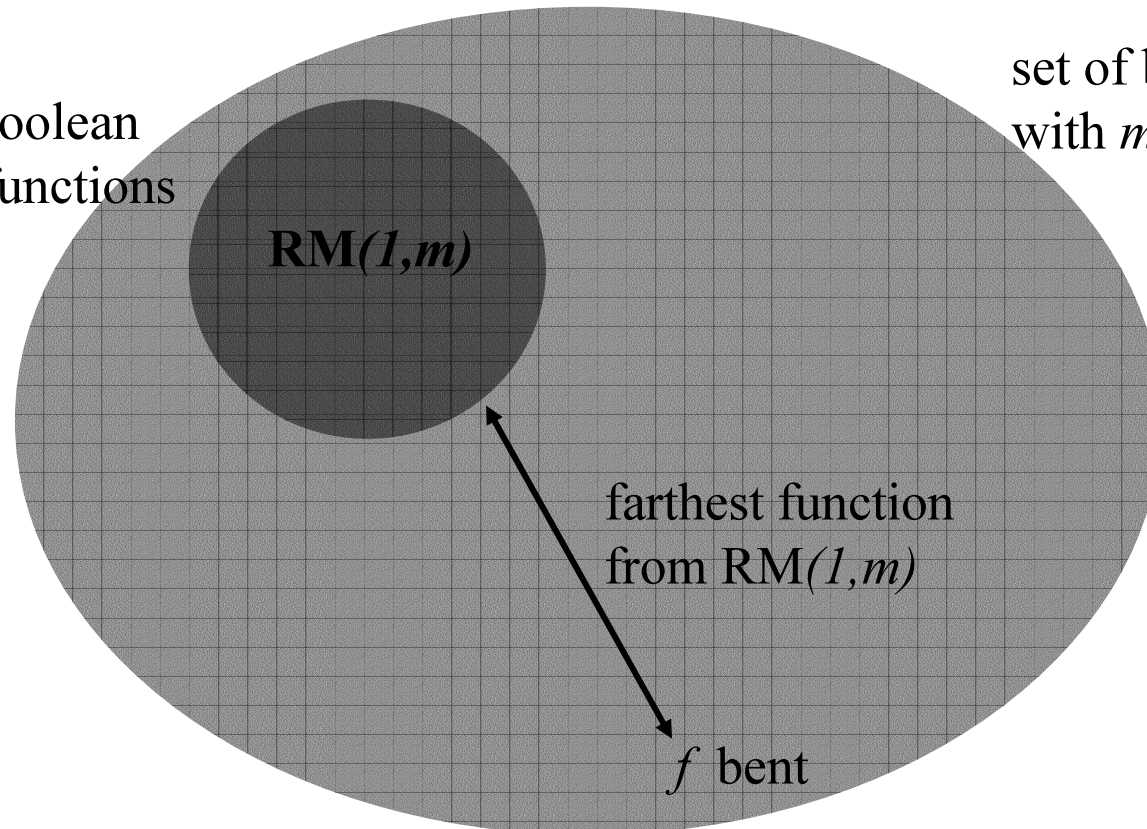
$$d(f, g) = \text{card}\{x \in \mathbb{F}_2^m \mid f(x) \neq g(x)\}$$

$f$  bent

$$d(f, \text{RM}(1, m)) = \inf_{g \in \text{RM}(1, m)} d(f, g) = 2^{m-1} - 2^{\frac{m}{2}-1}$$

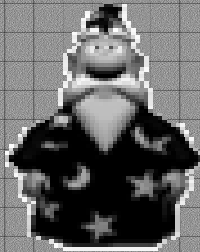
set of boolean  
affine functions

set of boolean functions  
with  $m$  variables



farthest function  
from  $\text{RM}(1, m)$

$f$  bent



What is the number of bent functions with  $m$  variables ?

$f$  bent  $\Rightarrow \deg f \leq m/2$  [Rothaus 76]

# of bent functions with  $m$  variables  $\leq 2^{2^{m-1} + \frac{\binom{m}{m/2}}{2}}$   
 $\downarrow$   
 # RM( $m/2, m$ )

A general upper bound [Carlet, Klapper 2002]

$$2^{2^{m-1} + \frac{\binom{m}{m/2}}{2}} - 2^{m/2 + \frac{m}{2} + 1} (1 + \varepsilon) + 2^{2^{m-1} - \frac{\binom{m}{m/2}}{2}}$$

where  $\varepsilon = 1/2^{\Omega((2^m/m)^{1/2})}$



# Constraints on bent functions (1)

$$f \text{ bent} \Rightarrow \deg f \leq m/2 \text{ [Rothaus 76]}$$

- $m = 2$

~~$$f \in \text{RM}(1, m)$$~~



Let  $m$  fixed  
What is the number of bent functions ?

- $m = 4$

# of boolean functions =  $2^{16}$   
*computer search can be used.*

$$\deg f = 2$$

the number of quadratic bent functions is well known for any  $m$ .

- $m = 6$

$$\deg f = 2 \text{ or } 3$$

'all' cubic bent functions in 6 variables are known [Rothaus 1976]

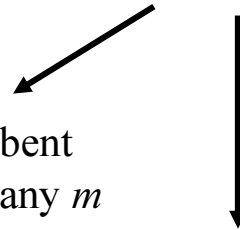


$f$  bent  $\Rightarrow \deg f \leq m/2$  [Rothaus 76]

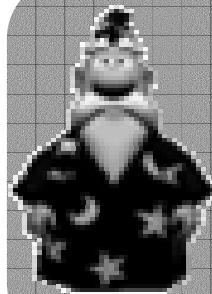
•  $m = 8$

$\deg f = 2, 3$  or  $4$ ?

number of quadratic bent  
functions known for any  $m$



'all' cubic bent functions in 8  
variables are known [Hou 1998])



We will focus our study  
on the number of bent  
functions of degree 4 in  
8 variables



## Constraints on bent functions (2)

Let  $f = \sum_{S \subseteq \{1, \dots, 8\}} a_S X_S$  be a boolean function of degree 4 in 8 variables

**Necessary condition for  $f$  to be bent** [Hou, Langevin 1998]

$f$  bent  $\Rightarrow$  for any  $V \subseteq \{1, \dots, 8\}$  such that  $|V| \in \{6, 7, 8\}$ ,


$$\sum_{\{S, T\} | S \cup T = V} a_S a_T = 0$$

$$f = \sum_{\substack{S \subseteq \{1, \dots, 8\} \\ |S|=4}} \alpha_S X_S + \sum_{\substack{S \subseteq \{1, \dots, 8\} \\ |S|=3}} \beta_S X_S + \sum_{\substack{S \subseteq \{1, \dots, 8\} \\ |S|=2}} \gamma_S X_S + h$$

↓ quartic part
↓ cubic part
↓ quadratic part
↘ affine part



# Constraints on bent functions (2)



$$f = \sum a_S X_S$$

$$= \sum_S \alpha_S X_S^4 + \sum_S \beta_S X_S^3 + \sum_S \gamma_S X_S^2 + h$$

$$f \text{ bent} \Rightarrow \begin{cases} V \subseteq \{1, \dots, 8\} \\ |V| \in \{6, 7, 8\} \end{cases}, \quad \sum_{\{S,T\} | S \cup T = V} a_S a_T = 0$$

gives a system of equations which must be fulfilled by the quadratic part of  $f$



**system III**

gives a system of equations which must be fulfilled by the cubic part of  $f$



**system II**

gives a necessary condition on the quartic part of  $f$

$$\sum_{\substack{S \subseteq \{1, \dots, 8\} \\ |S|=4}} \alpha_S \alpha_{\bar{S}} = 0$$



**system I**





### Strategy to compute an upper bound

$$f = \sum_{\substack{S \subset \{1, \dots, 8\} \\ |S|=4}} \alpha_S X_S + \sum_{\substack{S \subset \{1, \dots, 8\} \\ |S|=3}} \beta_S X_S + \sum_{\substack{S \subset \{1, \dots, 8\} \\ |S|=2}} \gamma_S X_S + h$$

$\times 2^9$

Enumerate all quartic part  
and check:

**(I)**  $\sum_{\substack{S \subset \{1, \dots, 8\} \\ |S|=4}} \alpha_S \alpha_{\bar{S}} = 0$

eliminates quartic forms which cannot be part of a bent function.

**(II)**  $A_{\alpha} y_{\beta} = b_{\alpha}$   
8 equations , 56 unknowns

gives an upper bound on the number of possible cubic part for a fixed quartic part

$2^{56-\text{rank}(A)}$  or 0

**(III)**  $A_{\alpha} y_{\gamma} = b_{\alpha, \beta}$   
28 equations , 28 unknowns

gives an upper bound on the number of possible quadratic part for a fixed quartic part

$2^{28-\text{rank}(A)}$



Let  $f \in \text{RM}(4,8)$  and  $A \in \text{GL}(8,2)$

$$(f \circ A)(X_1, \dots, X_8) := f((X_1, \dots, X_8)A)$$

$g \longrightarrow f \sim g$

$f$  bent  $\Leftrightarrow g$  is bent

Let  $q$  be an homogeneous quartic form

$q$  is the quartic part of a bent function

$\Leftrightarrow$

$\forall A \in \text{GL}(8,2), q \circ A$  is the quartic part of a bent function

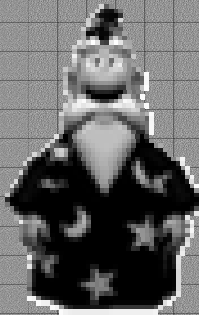
Systems I, II and III give exactly the same number of solutions for two quartic forms in the same orbit. (it's an invariant)

if you consider the action of  $\text{GL}(8,2)$  on the space of quartic forms  $\text{RM}(4,8)^* := \text{RM}(4,8)/\text{RM}(3,8)$  then all  $q' \in \text{Orb}_{\text{GL}(8,2)}(q)$  are the quartic part of a bent function.

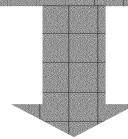


Since  $|\text{RM}(4,8)^*| = 2^{70}$ , it is impossible to compute straightforward the action of  $\text{GL}(8,2)$  over  $\text{RM}(4,8)^*$ .

Our goal :



Find a sufficiently small ( $< 2^{20}$ ) set of quartic forms which represents the space  $\text{RM}(4,8)^*$  up to linear equivalence.



**We found a set of 68647 such functions after 3 reductions**



# First Reduction

Let  $f \in \text{RM}(4,8)^*$

$$f = (q) + X_8(c) \rightarrow \text{RM}(3,7)^*$$

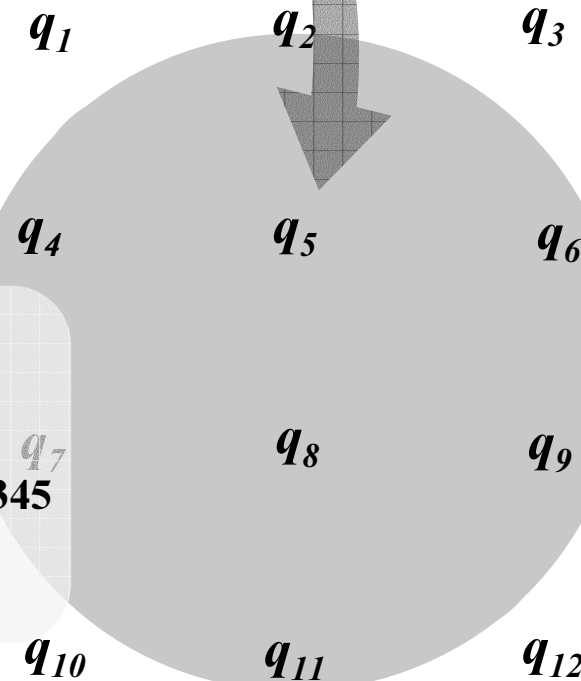
$\downarrow$   
 $\text{RM}(4,7)^*$

For any  $A = \left( \begin{array}{c|c} B & \mathbf{t0} \\ \hline 0\dots 0 & 1 \end{array} \right)$  where  $B \in \text{GL}(7,2)$ , then

$$f \circ A = (q \circ B) + X_8(c \circ B)$$

$$\in \text{Orb}_{\text{GL}(7,2)}(q) = \{ q \circ B \mid B \in \text{GL}(7,2) \}$$

$\text{GL}(7,2)$  acting on  $\text{RM}(4,7)^*$



<b>0</b>	<b>3456+2457+2367</b>
<b>4567</b>	<b>3456+2457+2367+1567</b>
<b>3467+2567</b>	<b>4567+1247+1356</b>
<b>3457+2467+1567</b>	<b>3467+2567+2467+1356+1246+2345</b>
<b>3457+1267</b>	<b>3456+2357+1457+1267</b>
<b>2467+2357+1467+1457+1367</b>	<b>2356+2347+1456+1357+1267</b>

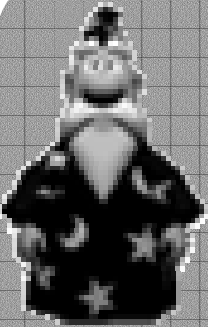
X.D. Hou

$\text{RM}(4,7)^*$

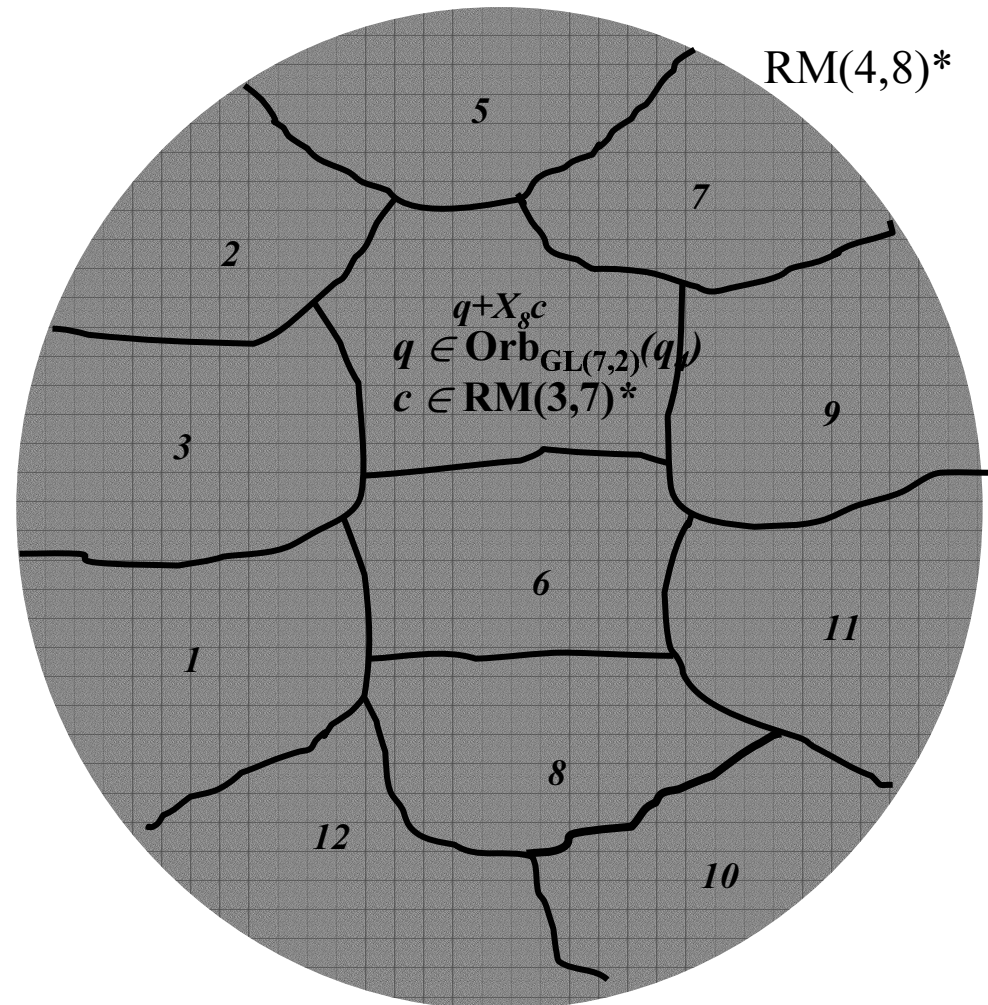


The classification of  $RM(4,7)^*$  under the action of  $GL(7,2)$  allows us to consider only the quartics forms  $q_i + X_8 c$  for  $i \in \{1, 2, \dots, 12\}$  and  $c \in RM(3,7)^*$

$\text{card}(RM(3,7)^*)$



We could check systems I, II and III on  $12 \times 2^{35}$  functions instead of  $2^{70}$ .





## Second Reduction

Let  $f \in \text{RM}(r, m)^*$ . The **derivative** of  $f$  in the **direction** of  $u \in \mathbf{F}_2^m$  is

$$\delta_u f(X) = \underbrace{f(X + u) + f(X)}_{\in \text{RM}(r - 1, m)^*} \pmod{\text{RM}(r - 2, m)}$$

The set  $\Delta(f) = \{\delta_u f, u \in \mathbf{F}_2^m\}$  is a subspace of  $\text{RM}(r - 1, m)^*$



$$q_i + X_8 c$$
$$c \in \text{RM}(3,7)^*$$

[Brier, Langevin 2003] Let  $q \in \text{RM}(4,7)^*$  and  $c \in \text{RM}(3,7)^*$ . For any  $d \in \Delta(q)$ , there exists  $A \in \text{GL}(8,2)$  such that

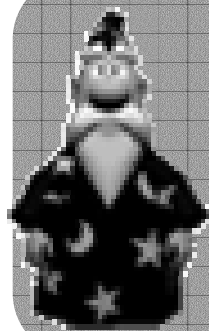
$$(q + X_8 c) \circ A = q + X_8 (c + d)$$

$$q_i + X_8 c,$$
$$c \in \text{RM}(3,7)^* / \Delta(q)$$



Foreach  $i \in \{1, \dots, 12\}$ , instead of checking all forms  $q_i + X_8 c$  where  $c \in \text{RM}(3,7)^*$ , we can restrict ourselves to those  $c \in \text{RM}(3,7)^* / \Delta(q_i)$ .

$i$	$\dim \text{RM}(3,7)^* / \Delta(q_i)$
1	35 $\longrightarrow q_1=0$
2	31
3	29
4	28
5	28
6	28
7	29
8	28
9	28
10	28
11	28
12	28



We could check systems I, II and III on

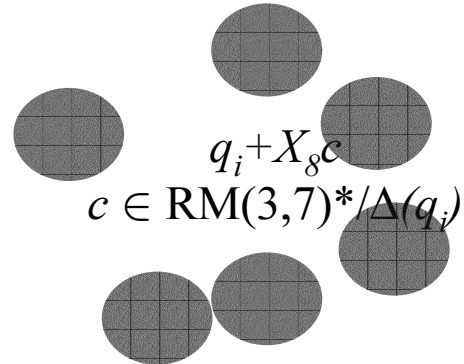
$$\sum_{i=1}^{12} 2^{\dim \text{RM}(3,7)^* / \Delta(q_i)} \text{ functions instead of } 12 \times 2^{35}$$

$2^{35} + 5 \cdot 2^{30}$





## Last Reduction



$\theta_i$ : # orbits

$$\text{Stab}(q_i) = \{ B \in \text{GL}(7,2) \mid q_i \circ B = q_i \}$$

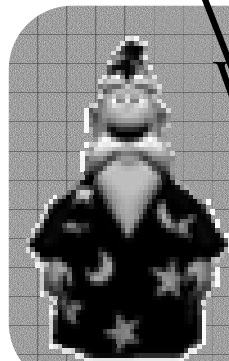
**Proposition 2.**  $\text{Stab}(q_i)$  acts on  $\text{RM}(3,7)^* / \Delta(q_i)$



Foreach  $i \in \{1, \dots, 12\}$ , instead of checking all forms  $q_i + X_8 c$  where  $c \in \text{RM}(3,7)^*/\Delta(q_i)$ , we can restrict ourselves to cubics  $c$  which are representatives of  $\text{RM}(3,7)^*/\Delta(q_i)$  under the action of  $\text{Stab}(q_i)$ .

Let  $\theta_i$  be the number of orbits of  $\text{RM}(3,7)^*/\Delta(q_i)$  under the action of  $\text{Stab}(q_i)$

Special Case :  $\text{Stab}(q_1) = \text{Stab}(0) = \text{GL}(7,2)$  and  $\text{RM}(3,7)^*/\Delta(0) = \text{RM}(3,7)^*$

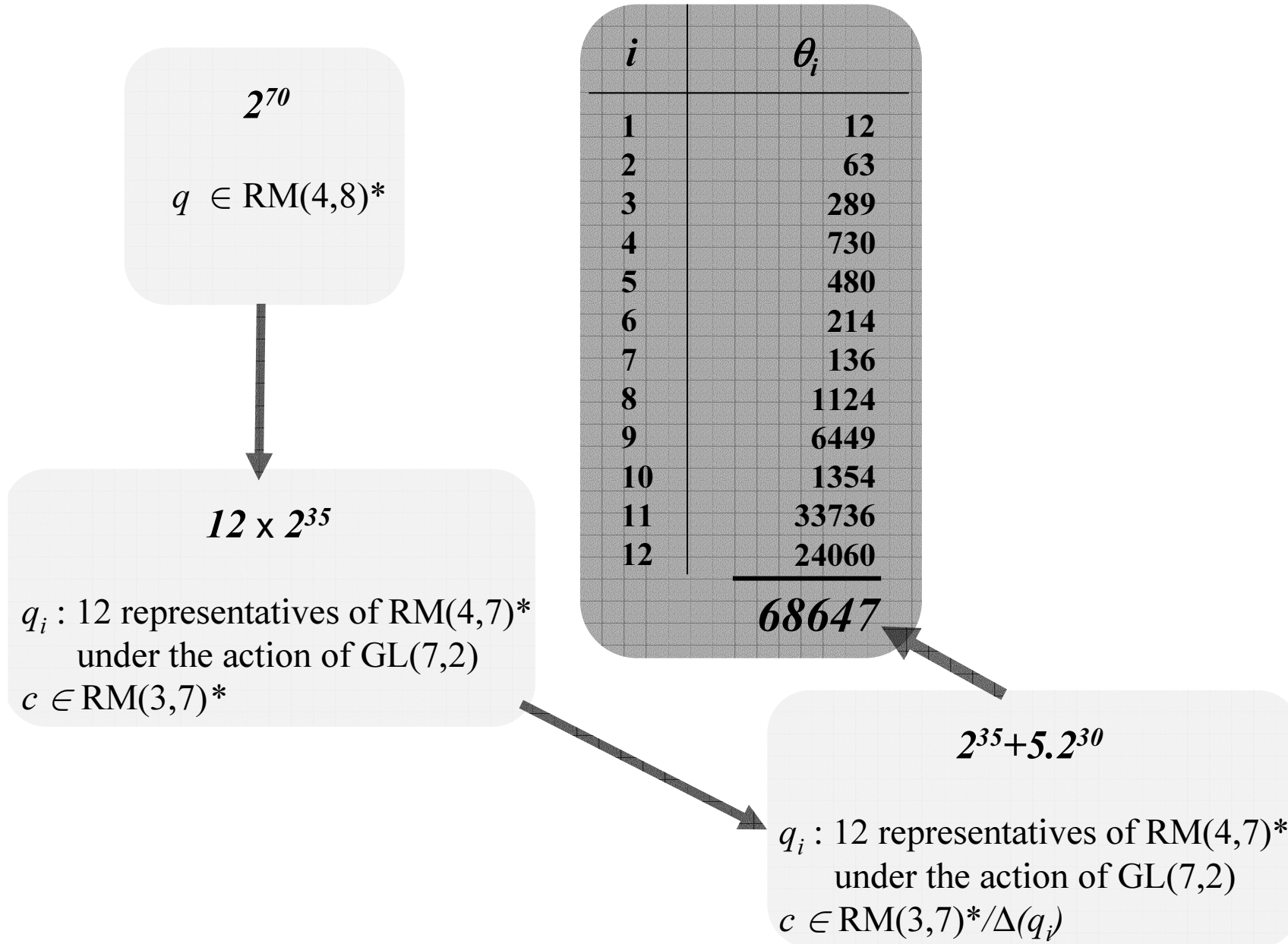


We only have to check systems I, II and III on

$$12 + \sum_{i=2}^{12} \theta_i \text{ functions instead of } \sum_{i=1}^{12} 2^{\dim \text{RM}(3,7)^*/\Delta(q_i)} = 2^{35} + 5 \cdot 2^{30}$$



$\theta_i$  : Number of orbits of  $RM(3,7)^*/\Delta(q_i)$  under the action of  $Stab(q_i)$





Our main result :  
the number of bent functions in 8 variables is  
less or equal to  $2^{129.2}$

Carlet - Klapper bound :  $2^{152}$



Work in progress: reduce the set of the **68647** functions to a set of **999** representatives of  $RM(4,8)^*$  under the action of  $GL(8,2)$ .