KERNELS AND DEFAULTS

PHILIPPE LANGEVIN AND PATRICK SOLÉ

Abstract. We consider the metric space of the set of boolean functions from a space over the field with two elements provided of the Hamming distance. The non-linearity of a boolean function is equal to its distance from the space of affine boolean functions. The functions having maximal non-linearity are called the bent functions. In this paper, we generalize the well known notions of kernels and defaults of the theory of quadratic forms, and we apply these notions to the study of the non-linearity of the cubic functions.

1. Boolean functions

Let E be a space of finite dimension m over the finite field $\mathbb{F}_2$. The set of functions from E into $\mathbb{F}_2$ is denoted by ${\mathbb{F}_2}^E$, an element of ${\mathbb{F}_2}^E$ is a *boolean function*. Let f be a boolean function, the set $\{x \in E \mid f(x) = 1\}$ is the *support* of f, it is denoted by $\mathrm{supp}(f)$. Conversely, for any subset X of E, the *indicating* function 1_X is the unic boolean function whose support is X. With the operations inherited of the field $\mathbb{F}_2$, the set of boolean function is a $\mathbb{F}_2$-algebra isomorphic to the algebra of subsets of E with the operations Δ and $\cap$. If $x_1, x_2, \ldots, x_m$ is any basis of the dual of E then the map sending a polynomial p of $\mathbb{F}_2[X_1, X_2, \ldots, X_m]$ to the boolean function $p(x_1, x_2, \ldots, x_m)$ defines an epimorphism of algebras which the kernel is the ideal generated by the polynomials $X_i^2 - X_i$. Hence, the algebra ${\mathbb{F}_2}^E$ is isomorphic to the quotient $\mathbb{F}_2[X_1, X_2, \ldots, X_m]/(X_1^2 - X_1, X_2^2 - X_2, \ldots, X_m^2 - X_m)$. The *degree* of a boolean function f, denoted by $\deg(f)$, is the smallest integer k such that f has an antecedent of degree k by the morphism above. This definition does not depend on the choice of the basis, moreover

Proposition 1. *The space* $\mathrm{RM}(k, m)$ *of boolean functions of degree at most* k *is generated by the indicating functions of the supports of the affine varieties of codimension* k*. In other words, if* f *has degree less than* k *then there exits* N *affine varieties of codimension* k V_1, V_2, $\ldots$, V_N *such that* $f = \sum_{i=1}^{N} 1_{V_i}$.

Proof. This is a result by Delsarte [3]. One can see it as a consequence of the fact that the Reed-Muller codes are the only codes invariant under the action of the general affine group, see also [11]. □

The *weight* of f, denoted by $\mathrm{wt}(f)$, is equal to the cardinality of the support of f. The *Hamming distance* between two function f and g is the weight of $f + g$. The minimal distance between f and any affine function

Key words and phrases. boolean functions, Reed-Muller codes, covering radius.

from E into $\mathbb{F}_2$ is the *non-linearity* of f, that is :

$$\delta(f) = \inf_{\phi} \mathrm{wt}(f + \phi).$$

The maximal value of $\delta(f)$, when f ranges the set of boolean function, is the *covering radius* of the first order Reed-Muller code. It is denoted by $\rho(m)$, a function with non-linearity $\rho(m)$ is a *bent* function. These functions have a great importance for cryptographic applications, see [14, 6].

2. Characters

Let $(a, b) \mapsto a.b$ be a symmetric non-degenerate bilinear symmetric form. Let χ be the non trivial additive character of the field $\mathbb{F}_2$: $\chi(0) = 1$ and $\chi(1) = -1$. The set of boolean functions is embedded in the set of complex function by the mapping $f \mapsto f_\chi$, where $f_\chi(x) = \chi(f(x)) = (-1)^{f(x)}$. The *Fourier transform* of the complex function h is the complex function defined by

$$\hat{h}(a) = \sum_{x \in E} h(x)\chi(a.x).$$

Par abus de langage, we say that $\widehat{f_\chi}$ is the Fourier transform of f. The relation :

$$\mathrm{wt}(f(x) + a.x + b) = 2^{m-1} - \frac{\chi(b)}{2}\widehat{f_\chi}(a), \tag{1}$$

shows that $\delta(f) = 2^{m-1} - \frac{1}{2}\|\widehat{f_\chi}\|_\infty$. This last equality justifies the definition of *spectral radius* of the set of affine functions, that is :

$$R(m) = \min_{f \in \mathbb{F}_2{}^E} \|\widehat{f_\chi}\|_\infty, \tag{2}$$

so that $\rho(m) = 2^{m-1} - \frac{1}{2}R(m)$.

For any complex function h, we have :

$$\sum_{a \in E} \hat{h}(a)\overline{\hat{h}(a)} = 2^m \sum_{a \in E} h(a)\overline{h(a)} \tag{3}$$

this is the famous Plancherel-Parseval identity. Its leads to the estimate

$$R(m) \leq 2^{\frac{m}{2}} \tag{4}$$

3. Quadrics

Let q be a quadratic form, that is a boolean function satisfying

$$q(x + y) = q(x) + q(y) + \phi(x, y), \tag{5}$$

where ϕ is a symetric bilinear form, the bilinear form associated to q. One defines the kernel and the default of q. [5] The kernel of q is the subspace $\ker(q) = \{x \in E \mid \phi(x, y) = 0, \quad \forall y \in E\}$; Clearly, the restriction of q to its kernel is a linear form, and the default of q is the intersection $\ker(q) \cap \mathrm{supp}(q)$. Let us denote by k the dimension of the kernel of q. A straigthforward calculation show that, for any vector a in E, we have :

$$\left(\widehat{q_\chi}(a)\right)^2 = 2^m \sum_{z \in \ker(q)} \chi(a.z) = \begin{cases} 2^{m+k}, & \text{si } a \perp \ker(q); \\ 0, & \text{sinon.} \end{cases} \tag{6}$$

On an other hand, we know that a non degenerate quadratic form has a kernel of dimension 0 if m is even, and dimension 1 if m is odd. Hence, we get the estimation

$$2^{\frac{m}{2}} \le R(m) \le 2^{\lceil \frac{m}{2} \rceil} \tag{7}$$

which is an equality if m is even. When m is odd, the exact value of $R(m)$ is known for $m = 3, 5, 7$, see [12] and [8]. Since the paper of Paterson and Wiedeman [13], we know that there exists a boolean function of $\mathrm{RM}(8, 155)$ which the Fourier transform has norm 216, consequently, for any odd m greater than 15 , we have :

$$R(m) \le 216 \times 2^{\frac{m-15}{2}} = \frac{27}{32} 2^{\lceil \frac{m}{2} \rceil} \tag{8}$$

Conjecture 1. *The spectral radius $R(m)$ is equivalent to $2^{\frac{m}{2}}$.*

Let k be an integer, $0 \le k \le m$. We define the spectral radius of the function of degree less or equal than k by $R_k(m) = \inf_{\deg(f)\le k} \|\hat{f}\|_\infty$. The goal of that paper is to present new notions in order to study $R_3(m)$. We believe that the number of cubic functions is great enough to conjecture :

Conjecture 2. *The spectral radii $R(m)$ and $R_3(m)$ are asymptotically equivalent.*

Note that, $R_3(m) = R_2(m)$ holds for m less or equal to 13, see [8] and [10].

4. Kernel and defaults

In this section, we generalize the notions of kernel and default of the above section. Let v be a vector of ${\mathbb{F}_2}^m$ and let f be a boolean function. The derivation of f in the direction of v is the boolean function $x \mapsto D_v f(x) = f(x + v) + f(x)$. If V is a system of r vectors, say $\{v_1, v_2, \ldots, v_r\}$, then the derivation in the direction of the system V is the composition $D_{v_1} \circ D_{v_2} \circ \cdots \circ D_{v_r}$. The map $V \mapsto D_V f(0)$ is a particular case of the combinatorial polarization of H. Ward [15]. If the vectors of V are linearly dependent then $D_V f$ is equal to zero, else it is equal to the convolutional product of f by the indicating function of the support of the subspace S of ${\mathbb{F}_2}^m$ generated by V : $D_V f(x) = 1_S * f(x)$; that is the derivation of f in the direction of S, introduced by Dillon in [6]. For any vector v , we have :

$$D_v(\sum_S a_S \, 1_S) = \sum_S a_S \, d(v, S) \, 1_{(v+S)\cup S} \tag{9}$$

where the S's are affine spaces, and $d(v, S)$ is equal to 1 if and only if v does not lie in the direction of S. .

Proposition 2. *Let f be a boolean function; Then*

$$\forall v \in E, \quad \deg(D_v f) \le \deg(f) - 1, \quad et \quad \exists v \in E \quad \deg(D_v f) = \deg(f) - 1$$

Proof. Note that is v is not in the direction of S then the codimension of $(v + S) \cup S$ is equal to the codimension of S minus 1, the first point is a consequence of 1. For the second point, we may assume that, the variable x_1 appears in a monomial of degree $\deg(f)$. Hence, f reads $g(x_2, x_3, \ldots, x_m)+$

$x_1 h(x_2, x_3, \dots, x_m)$ where h is a function of degree $\deg(f) - 1$, which proves the result since $D_{e_1} f = h$. ☐

Let r be an integer. We define the map $\lambda^{(r)}$ which transforms the boolean function f defined on $\mathbb{F}_2{}^m$ in the boolean function defined over $\mathbb{F}_2{}^{mr}$ by :

$$\lambda^{(r)}(f)[x_1, x_2, \dots, x_r] = \sum_{\lambda_1, \lambda^{(2)}, \dots, \lambda^{(r)}} f\Big(\sum_{i=1}^{r} \lambda_i x_i\Big) = D_{\{v_1, v_2, \dots, v_r\}} f(0)$$

Proposition 3. *The restriction of* $\lambda^{(r)}$ *to* $\mathrm{RM}(r, m)$ *is onto* $\Lambda^r(E)$*, its kernel is* $\mathrm{RM}(r-1, m)$*.*

Proof. Indeed, the proposition above shows that the function $x \mapsto D_{\{v_1, v_2, \dots, v_r\}} f(x)$ is constant. ☐

When the degree of f is equal to r, the map $\lambda^{(r)}(f)$ is a r-linear map; That is [1] the multilinear form associate to f. We define the kernel and the default of f as in the degree 2 case :

$$\ker(f) = \{(x_1, x_2, \dots, x_{r-1}) \mid \lambda^{(r)}(f)[x_1, x_2, \dots, x_r] = 0, \quad \forall x_r \in E\}$$

$$\mathrm{def}(f) = \{(x_1, x_2, \dots, x_{r-1}) \mid \lambda^{(r-1)}(f)[x_1, x_2, \dots, x_{r-1}] = 1\}$$

The cardinality of $\ker(f)$ and $\mathrm{def}(f)$ are respectively denoted by $k(f)$ and $d(f)$. These numbers are affine numerical invariants : for any affine transformation T, we have

$$k(f) = k(f \circ T), \qquad \text{et} \qquad d(f) = d(f \circ T),$$

which comes from the equality, $D_v(f \circ T) = (D_{\theta(v)} f) \circ T$, where θ is the linear map associate to the affine map T. For example, let $1 \le i, j, k \le m$ be three distinct integers, and consider the monomial function $x_i x_j x_k$. Its multilinear form is not zero, so that is a lift of the determinant function of the space generated by e_i, e_j and e_k.

$$\lambda^{(3)}(x_i x_j x_k)[x, y, z] = \det_{i,j,k}(x, y, z) = \begin{pmatrix} x_i & y_i & z_i \\ x_j & y_j & z_j \\ x_k & y_k & z_k \end{pmatrix} \tag{10}$$

It follows that for any quadratic function $q \in \mathrm{RM}(2, 3)$, the function $x_1 x_2 x_3 + q(x)$ of $\mathrm{RM}(3, 3)$ has no default.

5. Cubics

In [2] C. Carlet proposes to study the non-linearity of a boolean function by means of the hight order moments of its fourier transform. For example, he gives the inequality :

$$\sum_{a \in E} \big(\widehat{f_\chi}(a)\big)^4 \ge 2^{3m},$$

which is satisfied by any boolean function. The equality occurs if and only if f is bent and m is even. In this section, we study the links between the kernel and the moments of order 4 of the Fourier transform of a cubic. We begin by two simple fact about the trilinear form of a cubic.

It is easy to check that the trilinear form of the cubic f satisfies

(11) $$\lambda^{(3)}(f)[x,y,z] = \lambda^{(2)}(f)[x,y] + D_{x,y}f(z).$$

Which leads to the main formula of this paper,

Proposition 4. *If f is a boolean function of degree 3 then*

$$\sum_{a\in E}\big(\widehat{f_\chi}(a)\big)^4 = 2^{2m}\big(k(f)-2d(f)\big),$$

Proof. Indeed,

$$\begin{aligned}
\sum_{a\in E}\big(\widehat{f_\chi}(a)\big)^4 &= 2^m f_\chi * f_\chi * f_\chi * f_\chi(0)\\
&= 2^m \sum_{x+y+z+t=0} \chi\big(f(x)+f(y)+f(z)+f(t)\big)\\
&= 2^m \sum_{x,y,z} \chi\big(f(x)+f(y)+f(z)+f(x+y+z)\big)\\
&= 2^m \sum_{x,y,z} \chi\big(f(x+z)+f(y+z)+f(z)+f(x+y+z)\big) \qquad (12)\\
&= 2^m \sum_{x,y,z} \big(\lambda^{(3)}(f)[x,y,z]+\lambda^{(2)}(f)[x,y]\big)\\
&= 2^{2m} \sum_{(x,y)\in\ker(f)} \big(\lambda^{(2)}(f)[x,y]\big)\\
&= 2^{2m}\big(k(f)-2d(f)\big)
\end{aligned}$$

□

We say that a boolean function exceeds the quadratic bound if its nonlinearity is greater than the non-linearity of any quadratic function. Of course, this notion takes sense only is the case of odd m. From [9] and [10], we know that if m is less or equal than 13 then the cubics do not exceed the quadratic bound.

Proposition 5. *Let f be a boolean function of degree 3 such that $k(f) - 2d(f) \geq 2^{m+1}$ then f does not exceed the quadratic bound.*

Proof. That is a consequence of the following trick about meanings. Let $(a_i)_{1\leq i\leq n}$ be a sequence of n positive real numbers. Let μ be the meaning of the a_i's, and let ν be the meaning of the $(a_i)^2$'s. If $\nu > 2\mu^2$ then there exist i such that $a_i \geq 2\mu$. Indeed, $\frac{1}{n}\sum_{i=1}^{n}(a_i-\mu)^2 = \nu - \mu^2$, and there exists i such that $|a_i - \mu| > \mu$, since $a_i \geq 0$, we get $a_i > 2\mu$. □

Note that if f has no default then $k(f) - 2d(f) = k(f) \geq 32^m - 2$, so :

Corollary 1. *If f is cubic without default then f does not exceed the quadratic bound.*

This result was obtained in [11] but only for $m \leq 19$. The proposition 4 shows that in order to construct cubics far from the first order Reed-Muller code, we have to construct cubics f doing $k(f) - 2d(f)$ small.

6. Bounds

Let f be a boolean function of degree 3. The ordered pair $(x, y) \in {\mathbb{F}_2}^m \times {\mathbb{F}_2}^m$ is in the kernel of f if and only if y is in the kernel of the quadratic function $D_x f$. Let us denote by $r(x)$ the dimension of the kernel of the quadratic form $D_x f$. We have,

$$|\ker(f)| = \sum_{x\in E} 2^{r(x)}. \tag{13}$$

Proposition 6. *Assume that m is even. If f is a boolean function of degree 3 then the kernel of f contains at least $5 \times 2^m - 4$ elements.*

Proof. One remarks that the kernel of $D_x f$ contains x. Hence, $r(x) \geq 2$ since $r(x)$ and m have the same parity. □

Proposition 7. *Assume m odd. If f is a boolean function of degree 3 then the kernel of f contains at least $3 \times 2^m - 2$ elements.*

Proof. idem. □

In the next section, we will see that these bound are reached when $m = 3$ and $m = 6$. The above estimate must be compared with some results of Goethals about the space of quadratic forms, [4, 7]. For any odd integer m, there exists a space of dimension m of quadratic forms of rank 0 or $m - 1$. For example, the space of quadratic forms $x \mapsto \mathrm{Tr}_{{\mathbb{F}_2}^m/\mathbb{F}_2}\big(ax^{2^t} + (ax)^{2^{t+1}}\big)$, where $a \in {\mathbb{F}_2}^m$.

Problem 1. *Let τ be a trilinear alternate form. We have a natural map from E into $\Lambda^2(E)$ which sends $a \in E$ on a bilinear form. Let $r(a)$ be the rank of the image of a. What can we say about $\sum_{a\in E} 2^{r(a)}$ when τ varies ?*

Problem 2. *Let f be a boolean function. From proposition 1, we know that f decomposes as $\sum_{S\in X} 1_S$ where X is a set of affine subspaces. Let x and y be two vectors of E. The derivation of f in the direction of $\{x, y\}$ is $D_{x,y}(f) = \sum_{S\in X} d(x, y, S)1_{S(x,y)}$ where $S(x, y)$ is the affine space $S \cup (x + S) \cup (y + S) \cup (x + y + S)$, and where $d(x, y, S) \in \mathbb{F}_2$ is equal to 0 if and only if the direction of S contains al least one vector of x, y or $x + y$. Use this description to construct a set X of variety of codimension 3 in order to obtain a cubic with small kernel.*

7. Numerical Results

The next tables give all the values of kernel, and default for all the cubic functions, $4 \leq m \leq 7$. Kernels and defaults are affine invariant, so we use the action of the general linear group $GL(m, \mathbb{F}_2)$ on the space of boolean cubics modulo the space of quadratic functions to reduce the problem of enumeration. In the paper [8], one can find systems of representatives for small m. For each representative h, there is a three columns table. Let us denote by k be the cardinality of the kernel of h. When q ranges the space of the homogeneous quadratic functions $\ker(h + q)$ is invariant, the value of k appears in the header of the table. A row (d, δ, c) means that there are c homogeneous quadratic functions q with d defaults, and δ is to $k - 2d$: the quantity that appears in the RHS of (12). Note that if f is a boolean function of degree more than 2 then its kernel and default do not depend of the affine terms.

$m=4,\ k=88,\ h_1$			$m=4,\ k=88,\ h_2$		
24	40	56	24	40	56
0	88	8	24	40	56

$m=5,\ k=352,\ h_1$			$m=5,\ k=184,\ h_3$		
132	88	512	60	64	192
144	64	336	48	88	480
96	160	168	36	112	320
0	352	8	0	184	32

$m=6,\ k=1408,\ h_1$			$m=6,\ k=736,\ h_3$		
528	352	3584	336	64	192
624	160	25088	288	160	23520
672	64	1344	96	544	32
576	256	2352	240	256	8192
384	640	392	192	352	480
0	1408	8	144	448	320
			0	736	32

$m=6,\ k=316,\ h_6$			$m=6,\ k=484,\ h_4$			$m=6,\ k=400,\ h_5$		
84	148	7680	168	148	10752	168	64	64
60	196	21504	144	196	18816	120	160	15680
36	244	3584	96	292	3136	96	208	14336
			0	484	64	72	256	2240
						24	352	448

$m=7,\ k=5632,\ h_1$			$m=7,\ k=760,\ h_{12}$		
2640	352	917504	240	280	32256
2112	1408	17920	216	328	516096
2496	640	376320	192	376	959616
2688	256	772800	168	424	368640
2304	1024	11760	0	760	128
1536	2560	840	96	568	16128
0	5632	8	144	472	204288

$m=7,\ k=2944,\ h_3$			$m=7,\ k=928,\ h_{10}$		
1104	736	32768	168	592	6144
1248	448	512000	216	496	92160
1296	352	983040	312	304	284672
1344	256	450624	264	400	632832
1152	640	93600	336	256	3072
384	2176	96	288	352	801792
960	1024	24192	240	448	236288
768	1408	480	192	544	27648
576	1792	320	144	640	11776
0	2944	32	48	832	768

$m=7,\ k=1936,\ h_4$			$m=7,\ k=1600,\ h_5$			$m=7,\ k=1264,\ h_8$		
768	400	903168	672	256	161344	456	352	589824
672	592	111104	624	352	1376256	480	304	483840
816	304	903168	576	448	397824	384	496	225408
720	496	150528	480	640	26432	336	592	46080
576	784	18816	528	544	114688	288	688	18944
528	880	7168	384	832	17920	144	976	1024
384	1168	3136	288	1024	2240	192	880	768
0	1936	64	96	1408	448	0	1264	128
						432	400	731136

$m=7,\ k=2272,\ h_7$			$m=7,\ k=1264,\ h_6$			$m=7,\ k=928,\ h_9$		
1008	256	368640	480	304	645120	336	256	24576
960	352	999936	336	592	7680	288	352	1476608
912	448	645120	432	400	1290240	240	448	544768
768	736	40320	384	496	129024	144	640	28672
720	832	43008	240	784	21504	192	544	21504
0	2272	128	144	976	3584	0	928	1024

$m=7,\ k=592,\ h_{11}$		
120	352	983040
96	400	1024000
48	496	81920
0	592	8192

List of homogeneous cubics :
$h_1 = X_1X_2X_3$, $h_2 = X_1X_2X_3 + X_2X_3X_4$, $h_3 = X_1X_2X_3 + X_2X_4X_5$,
$h_4 = X_1X_2X_3 + X_4X_5X_6$, $h_5 = X_1X_2X_3 + X_2X_4X_5 + X_3X_4X_6$,
$h_6 = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6$,
$h_7 = X_1X_2X_7 + X_3X_4X_7 + X_5X_6X_7$,
$h_8 = X_1X_2X_3 + X_4X_5X_6 + X_1X_4X_7$,
$h_9 = X_1X_2X_3 + X_2X_4X_5 + X_3X_4X_6 + X_1X_4X_7$,
$h_{10} = X_1X_2X_3 + X_4X_5X_6 + X_1X_4X_7 + X_2X_5X_7$,
$h_{11} = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6 + X_1X_6X_7$,
$h_{12} = X_1X_2X_3 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 + X_4X_5X_6 + X_2X_4X_7 + X_1X_6X_7$
.

References

[1] C. Carlet. A new generalization of bent functions to the odd case. *private communication.*

[2] C. Carlet. *Codes de Reed-Muller, codes de Kerdock et de Preparata.* 1990.

[3] P. Delsarte. A geometrical approach to a class of cyclic codes. *Journal of Combinatorial Theory*, 6, 1969.

[4] P. Delsarte and J.M. Goethals. Alternating bilinear forms over $gf(q)$. *Journal of combinatorial theory*, (A) 19, 1975.

[5] J. Dieudonné. *La géométrie des groupes classiques.* 1971.

[6] J. F. Dillon. *Elementary Hadamard Difference Sets.* 1974.

[7] J.M. Goethals. Nonlinear codes and quadratic forms. *Information and Control*, 31(1), 1976.

[8] X.D. Hou. $gl(m,2)$ acting on $r(r,m)/r(r-1,m)$.
[9] X.D. Hou. On the covering radius of $(1,\mathrm{m})$ into $(3,\mathrm{m})$.
[10] Ph. Langevin. *The covering radius of* $\mathrm{RM}(1,9)$ *in* $\mathrm{RM}(3,9)$, volume 514. 1990.
[11] Ph. Langevin. *rayon de recouvrement des codes de Reed-Muller affines*. 1992.
[12] J. J. Mykkelveit. The covering radius of the (128,8) reed-muller codes is 56. *IEEE transactions on information theory*, 26, 1980.
[13] N.J. Patterson and D.H. Wiedemann D.H. The covering radius of the $(2^{15},16)$ reed-muller code is at least 16276.
[14] O.S. Rothaus. on bent functions. *Journal of Combinatorial Theory*, 20, 1976.
[15] Harold N. Ward. Combinatorial polarization. *Discrete Math.*, 26, 1979.

CNRS, I3S, bâtiment 4, 250 rue A. Einstein, 06560 Valbonne, France
Email address: langevin@alto.unice.fr, sole@alto.unice.fr