ON THE COUNTER-EXAMPLE OF PATTERSON–WIEDEMANN

PHILIPPE LANGEVIN, JEAN-PIERRE ZANOTTI

Abstract. Following Patterson and Wiedemann [10], we find new counter-examples to the conjecture of Mykkelveit [9] related to the covering radius of the first order Reed-Muller code. One of them has a remarkable algebraic structure.

1. Spectral magnitude

Let L be an extension of degree m of $\mathbf{F}_2$, the field of order 2. Let μ_L be the canonical additive character of L that applies $z \in L$ onto $(-1)^{\mathrm{tr}_L(z)}$, where $\mathrm{tr}_L(z)$ is the trace of z over $\mathbf{F}_2$. The bilinear symmetric form $(x, y) \mapsto \mathrm{tr}_L(xy)$ is non-degenerate, and one defines the Fourier coefficient of the boolean function $f : L \to \mathbf{F}_2$ at $a \in L$ by :

$$\widehat{f}(a) = \sum_{x \in \mathbf{F}_2^m} (-1)^{f(x)} \mu_L(ax) \tag{1}$$

The Hamming distance between f and the affine function $x \mapsto a.x + b$ ($b \in \mathbf{F}_2$) equals to $2^{m-1} - \frac{(-1)^b}{2}\widehat{f}(a)$. The *spectral magnitude* of f defined by $\mathrm{Sp}(f) = \sup_{a\in L} |\widehat{f}(a)|$ measures the distance between f and the space of affine functions. The *spectral radius* $R(m) = \inf_f \mathrm{Sp}(f)$ is particularly relevant for cryptographic point of view. The Fourier analysis gives the Parseval's lower bound :

$$\sqrt{2^m} \le R(m) \tag{2}$$

The functions reaching that bound are the *bent functions* of Rothaus [11], they exist in even dimension only. All along that paper, we will denote $m = 2t$ or $m = 2t + 1$ according whether m is even or odd. It is easy to see that the spectral magnitude of a quadratic form of rank k is $2^{\frac{m+k}{2}}$. In even dimension, non-degenerate quadratic functions are bent, but there are bent functions of degree d for all d between 2 and t. In odd dimension, the minimal spectral magnitude of quadratic functions is 2^{t+1} whence we get the quadratic bound :

$$R(m) \le 2^{t+1}. \tag{3}$$

We say that f exceeds the quadratic bound if its spectral magnitude is less than 2^{t+1}. Berlekamp and Welch [2], Mykkelveit [9] and more recently Hou [6] have proved that if $m \in \{3, 5, 7\}$ then $R(m) = 2^{t+1}$: such a function does not exist, for these values of m. For $m = 9$, 11 and 13 nothing more than the bounds (2) and (3) is known. In their famous note [10], Patterson and Wiedemann construct boolean functions of spectral magnitude 216 in

Date: May 1999 – May 2000.

dimension 15 providing counter-examples to a conjecture of Mykkelveit that claimed $R(m)^2 = 2^{m+1}$ for odd m. They did not succeeded in finding algebraic structures of their functions but they conjecture that $R(m) \sim \sqrt{2^m}$. Here, we give a new counter-example that makes a link with the (relative) difference sets theory.

2. Action of cyclic groups

Let G be a subgroup of order d of $L^\times$. We say that a boolean function f is invariant under G if and only if $F(gz) = F(z)$ for all $g \in G$ and $z \in L$. It is equivalent to say that f is an union of cosets of $L^\times$ modulo G. We want to study the spectral magnitude of the G-invariant boolean functions in order to obtain functions exceeding the quadratic bound.

Using a slight abuse of notations, we denote by G the indicating boolean function of the group G so that

$$F(z) = \sum_{\omega \in \Omega} s(\omega) G(\omega z) = \sum_{\omega \in D} G(\omega z),$$

where s is a numerical boolean sequence corresponding to a choice of cosets of G in $L^\times$ whose support denoted by D is a set of cardinality say k. We denote by v the order of the quotient group $\Omega = L^\times/G$ of course $dv = 2^m - 1$. Later we will make connection with difference sets theory that explains our notations : D, v, k. The Fourier coefficient of F at 0 is

$$\widehat{F}(0) = 2^m - 2dk = 2^m - 1 + 1 - 2dk = dv + 1 - 2dk.$$

This equality shows that d must be chosen less or equal to $2^t + 1$ to obtain bent functions, and less than 2^{t+1} to have some chance to exceed the quadratic bound. In particular, if we want F to have a spectral magnitude less or equal than R we must assume

$$|v - 2k| \leq \frac{R+1}{d}.$$

Let a be a non-zero element of L. The Fourier coefficient of G at a depends on the class of a modulo G and is given by

$$\widehat{G}(a) = -\sum_{g \in G} \mu_L(ag) + \sum_{g \notin G} \mu_L(ag) = -2\sum_{g \in G} \mu_L(ag) = -\frac{2}{v} \sum_{\chi \perp G} \tau_L(\chi)\bar{\chi}(a),$$

where $\tau_L(\chi) = \sum_{z \in L^\times} \chi(z)\mu_L(z)$ is the Gauss sum associated to the multiplicative character χ and the additive character μ_L. Those of F, is equal to the intercorrelation of s by $\widehat{G}$ and is given by :

$$\widehat{F}(a) = \sum_{\omega \in \Omega} s(\omega)\widehat{G}(a\omega) = \sum_{\omega \in D} \widehat{G}(a\omega) = -\frac{2}{v} \sum_{\chi \perp G} \tau_L(\chi) D(\chi) \bar{\chi}(a).$$

In that last equality, we identify $G^\perp$ with the dual of Ω, whence $D(\chi)$ is the (multiplicative) Fourier transform of D at χ. The main question is : what kind of D could make small the absolute value of the $\widehat{F}(a)$'s ?

3. Basic facts

We continue denoting by $g(a)$ the function $\hat{G}(a)$ which is well defined over Ω.

The function g is perfect since its multiplicative Fourier transform $g(\psi)$ is

$$g(\psi) = -\frac{2}{v}\sum_{x\in\Omega}\sum_{\chi\perp G}\tau_L(\chi)\bar{\chi}(a)\psi(a) = -\tau_L(\psi)$$

Of course, we can also make straiforward calculation and prove

$$g\times g(a) = \begin{cases} 2^m-1, & \text{if } a=1; \\ -1, & \text{else.} \end{cases}$$

Need a proof ?

$$\begin{aligned} g\times g(a) &= 4\sum_{\omega\in\Omega} g(\omega)g(\omega a) \\ &= 4\sum_{\omega\in\Omega}\sum_{x\in G}\sum_{y\in G}\mu_L(\omega x+\omega a y) \\ &= \sum_{\omega\in\Omega}\sum_{x\in G}\sum_{y\in G}\mu_L(\omega x+\omega a x y) \\ &= \sum_{y\in G}\sum_{z\in L^\times}\mu_L(z(1+ay)) \end{aligned}$$

We remark that

$$\begin{aligned} \sum_{\omega}(g\times s(\omega))^2 &= \sum_{\omega}(g\times g(\omega))(s\times s(\omega)) \\ &= 2^m - \sum_{\omega} s\times s(\omega) \\ &= 2^m - k^2 \end{aligned}$$

4. functions from subfields

Assume that m is even. Let K be the subfield of degree t in L. By a Stickelberger's theorem [8], we know that the Gauss sums of order dividing 2^t+1 are all rational and so equal to 2^t. It follows that the Fourier transform of F at a is given by :

$$-\frac{1}{2}\widehat{F}(a) = \frac{1}{v}\sum_{\chi\perp G}\tau_L(\chi)s(\chi)\bar{\chi}(a) = \frac{2^t}{v}\sum_{1\neq\chi\perp G}s(\chi)\bar{\chi}(a) - \frac{k}{v} = 2^t s(a) - k$$

We have recover a result of Dillon [4].

Proposition 4.1. *If D is a set of 2^{t-1} cosets of the group G in $L^\times$ then the corresponding function is bent.*

Proof. Clear. □

orbits	degree	-216	-152	-88	-24	40	168	232
0 1 7 11 15 17	8	5		1		1	5	
0 1 3 7 17 35	9	5		1		1	5	
0 3 5 23 35 37	10	2	4	1	1		1	3
0 5 11 15 23 37	10	2	4	1	1		1	3

TABLE 1. Spectral distributions of Patterson-Wiedemann functions

In [10], Patterson and Wiedemann proceed by analogy looking for boolean function that are invariant under the multiplicative group of subfields of the field $\mathbf{F}_{2^m}$. The multiplicative group of the field of order 2^{15} factors in $7 \times 31 \times 151$ and contains a cyclic group G of order 217 which is the direct product of $\mathbf{F}_8{}^\times$ and $\mathbf{F}_{32}{}^\times$, there are 2^{151} G-invariant functions but only 2^{12} of them are also invariant under the Frobenius automorphism and correspond to the 12 cyclotomic classes modulo 151 represented by the coset leader 0, 1, 3, 5, 7, 11, 15, 17, 23, 35, and 37. Using a computer, one can see that 8 of these functions exceed the quadratic bound, see TAB.1.

We have computed the autocorrelation function of the sequences s corresponding to them, and for example, the autocorrelation of the first row takes only four values : 60 times the value 36, 30 times the value 38, 60 times the value 40 and 1 time 76. Its structure is near of that of "difference sets" but is not a difference set neither a relative difference set.

5. FUNCTION FROM SUBGROUP

Once again, assume that m is even. We suppose that G is the group of order $d := 2^t + 1$. The function $z \mapsto \mathrm{tr}_L(az^{2^t+1})$ is G-invariant, bent iff the Kloosterman sum $\mathrm{K}l(a)$ is equal to -1 [5]. Argumenting with elliptic curves theory, Lachaud and Wolfmann [7] prove that for any L there are $2^t - 1$ such a. Now, we re-find a similar result by means of Gauss sums. A classical proposition of Davenport-Hasse [8] asserts that for any character χ of order v, the negative of the Gauss sum $\tau_L(\chi)$ is equal to $\tau_K(\chi)^2$. It follows that

$$-\frac{1}{2}\widehat{F}(a) = \frac{1}{v}\sum_{\chi \perp G} \tau_L(\chi)s(\chi)\bar{\chi}(a) = \frac{1}{v}\sum_{\chi \perp G} \tau_K(\chi)^2 s(\chi)\bar{\chi}(a).$$

Let c be a non-zero element of K and let $E_c = \{z \in K^\times \mid \mathrm{tr}_K(z/c) = 1\}$. It has order 2^{t-1} and the multiplicative Fourier transform of E_c at $\chi \neq 1$ is

$$E_c(\chi) = -\frac{1}{2}\sum_{z \in K^\times} [1 - \mu_K(z/c)]\chi(z) = -\frac{1}{2}\tau_K(\chi)\chi(c).$$

Similarly those of the set $D_c = \{z \mid \mathrm{tr}_K(c/z) = 1\}$ is equal to $-\tau_K(\bar{\chi})\chi(c)/2$.

Proposition 5.1. *Let $c \in K^\times$. The set D_c defines a bent functions.*

spectra	orbits	degree	correlation
248	3 5 13 19 21	12	186 [46], 1 [108]
	27 31 33 35 77		10 [99], 10 [100], 10 [101]
234	0 3 5 13 19 21	15	186 [47], 30 [101], 1 [109]
	27 31 33 35 77		186 [47], 30 [101], 1 [109]
232	1 7 9 11 15 25	10	186 [46], 30 [100], 1 [108]
	37 49 93 105		186 [46], 30 [100], 1 [108]
246	0 1 7 9 11 15 25	15	186 [47] , 1 [109]
	37 49 93 105		10 [100], 10 [101], 10 [102]

TABLE 2. Action of $\mathbf{Z}/151\mathbf{Z}$

Proof. Let s the indicating function of E_c. Let F be the boolean function defined by D_c whose the Fourier coefficient at a is :

$$\begin{aligned}
-\frac{1}{2}\widehat{F}(a) &= \frac{1}{v}\sum_{\chi\perp G} -\tau_K(\chi)^2 D_c(\chi)\bar{\chi}(a) \\
&= \frac{2^t}{v}\sum_{1\neq\chi\perp G} -\tau_K(\chi)\chi(c)/2\bar{\chi}(a) + \frac{2^{t-1}}{v} \\
&= -2^t s_c(a) + 2^{t-1}.
\end{aligned}$$

□

6. A REMARKABLE EXAMPLE

As Patterson and Wiedemann did for the group of order 217, we have look for invariant boolean functions under the action of the group of order 151. There are 2^{217} such functions but only 2^{23} are also invariant by the Frobenius automorphism. Four of them (TAB.2) exceed the quadratic bound with spectral magnitude : 248, 234, 232, and 246. It is worst than in the case of the group of order 217 but one of these functions has a remarkable structure. Indeed, the autocorrelation of the function of the second row takes only three values. Its support D is composed of the cyclotomic classes of 1, 7, 9, 11, 25, 37, 49, it defines a $(7.31, 108, 100, 46)$ relative difference set. Moreover, regarding $\mathbf{Z}/151\mathbf{Z}$ as the direct product $\mathbf{Z}/7\mathbf{Z}\times\mathbf{Z}/31\mathbf{Z}$, D is equal to

$$D_1 \times \mathbf{Z}/31\mathbf{Z} \quad \cup \quad \{0\}\times D_2$$

where D_1 is the Singer set $\{1,2,4\}$ and D_2 the Singer set $\{3,5,7,\ldots\}$ so that D appears as one of the relative difference sets described by theorem 2.1 of [1].

ACKNOWLEDGEMENTS

The authors wish to thank professors K. T. Arasu and J. Wolfmann for pointing us and communicating us the references [1, 7].

References

[1] Arasu K. T., Haemers W. H., Jungnickel D., Pott A. Matrix constructions of divisible designs. *Linear of Algebra and its Applications*, 153, 1991.

[2] Berlekamp E. R., Welch L. R. Distributions of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, 13(1):203–207, 1972.

[3] Constantin J., Courteau B., Wolfmann J. Numerical experiments related to the covering radius of some Reed-Muller codes. In Lecture Notes in Computer Science, editor, *Algebraic Algorithms and Error-Correcting Codes*, volume 229, pages 69–75. 3rd International Conference AAECC, 1986.

[4] Dillon J. F. *Elementary Hadamard Difference Sets.* PhD thesis, University of Maryland, 1974.

[5] Dillon J. F. Elementary Hadamard difference sets. In *sixth SECCGTC*, 1975.

[6] Hou X.-D. Covering radius of the Reed-Muller code $R(1, 7)$ — a simpler proof. *Journal of Combinatorial Theory*, 74, 1996.

[7] Lachaud G., Wolfmann J. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *Comptes rendus de l'académie des sciences*, 305:881–883, 1987.

[8] Lidl R., Niederreiter H. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, 1983.

[9] Mykkelveit J. J. The covering radius of the $(128, 8)$ Reed-Muller codes is 56. *IEEE Transactions on Information Theory*, 26(3):359–362, 1980.

[10] Patterson N. J., Wiedemann D. H. The covering radius of the $(1, 15)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, 29:354–356, 1983.

[11] Rothaus O. S. On bent functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.

GRIM, Université de Toulon, 83957 La Garde, France.