Around the counter-example of Patterson & Wiedemann

Philippe Langevin
with Jean-Pierre Zanotti
Groupe de **R**echerche
en **I**nformatique et **M**athématiques
université de Toulon, France.
http://www.univ-tln.fr/~grim

F_{q^6}, Oaxaca, May 21–25 2001.

Fourier Coefficients

- Let L be an extension of degree m of $\mathbf{F}_2$
- μ_L be the canonical additive character of L

$$\mu_L(z) = (-1)^{\mathrm{Tr}_L(z)}$$

- 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 :

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

Spectral Magnitude

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

$$\mathrm{R}(f) = \sup_{a \in L} |\widehat{f}(a)|$$

measures the distance between f and the space of affine functions. The **spectral radius** $R(m) = \inf_f \mathrm{R}(f)$ is particularly relevant for cryptographic point of view.

Lower and Upper Bounds

The Fourier analysis gives the Parseval's lower bound :

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

Equality holds for the **bent functions** of Rothaus.

–*prop.*: The spectral magnitude of a quadratic form of rank k is

$$2^{\frac{m+k}{2}}.$$

In odd dimension, the minimal spectral magnitude of quadratic functions is 2^{t+1} whence we get the quadratic bound :

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

“Exceeding” the quadratic bound

▷ m odd, $m = 2t + 1$.

We say that f **exceeds the quadratic bound** if its spectral magnitude is less than 2^{t+1}.

–*Berlekamp & Welch*, 1972 : for $m = 5$, no function exceeds the quadratic bound

–*Mykkelveit*, 1981 : for $m = 7$, it is idem.

See Hou for a short proof.

–*Mykkelveit's conjecture* : If m is odd then

$$R(m) = \sqrt{2^{m+1}}$$

A counter-example

In a famous note, Patterson and Wiedemann (1983) construct boolean functions of spectral magnitude 216 with $m = 15$

$$216 < 256 = 2^{(15+1)/2}$$

that is a counter-example !

–Patterson & Wiedemann's conjecture:

$$R(m) \sim \sqrt{2^m}$$

For $m = 9$, 11 and 13 nothing more is known.

Structures ?

They have found the counter-examples by an exhaustive search in the space of the functions invariant under the actions

$$x \mapsto x^2; \qquad x \mapsto \alpha x, \quad \alpha \in \mathbf{F_8}^\times \cup \mathbf{F_{32}}^\times.$$

... We have not succeeded in understanding <u>algebraically</u> the choice of orbits and thus have not succeeded in generalizing our construction to other dimensions although we suspect there is a construction when m is not a prime power ...

Patterson-Wiedemann

Today, we will see that $m = 15$ is a very special case.

Action of cyclic groups

- Let G be a subgroup of order d of $L^\times$.

  A boolean function f is **invariant under** G iff

$$F(gz) = F(z), \qquad \forall g \in G, \quad z \in L.$$

f is invariant under G iff $\mathrm{supp}(f)$ is an union of cosets in $\Omega := L^\times / G$.

Let us denote by G (abuse of notations) the indicating boolean function of the group G

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

- s is a numerical boolean sequence
- $D = \{\omega \mid s(\omega) = 1\}$, a set of cardinality say k.

Notations

We want a connexion with **Design theory**

- v the order of $\Omega = L^\times/G$;
- D the support of s;
- k the cardinality of D

Of course $dv = 2^m - 1$ and 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.

Links with Gauss sums

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

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

▷ where $\tau_L(\chi) = \sum_{z\in L^\times} \chi(z)\mu_L(z)$ is a Gauss sum.

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

We identify $G^\perp$ with the dual of Ω, whence $D(\chi)$ is nothing but the (multiplicative) Fourier transform of D at χ.

Functions from Subfields

- m even, say $m = 2t$.
- K a subfield of degree t in L.

–*Stickelberger*: The Gauss sums of order dividing $2^t + 1$ are rational equal to 2^t.

The Fourier transform of F follows :

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

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

Key Idea of Patterson & Wiedemann

They proceed by analogy looking for boolean function that are invariant under the multiplicative group of subfields of the field $\mathbf{F}_{2^m}$.

$$2^{15} - 1 = 7 \times 31 \times 151$$

▷ Let $G \sim \mathbf{F}_8{}^\times \times \mathbf{F}_{32}{}^\times$.

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.

Numerical results, order 217.

▷ 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.

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

Correlation Properties

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 :

$$s \times s(t) = \begin{cases} 76, & 1 \text{ times;} \\ 36, & 60 \text{ times;} \\ 38, & 30 \text{ times;} \\ 40, & 60 \text{ times;} \end{cases}$$

Its structure is near of that of “difference sets” but is not a difference set neither a relative difference set.

Function from Subgroup

- again, assume m even.
- G 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 [a]. Argumenting with elliptic curves theory, Lachaud and Wolfmann 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] Dillon

–*Davenport-Hasse*: 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 $-\tau_K(\bar{\chi})\chi(c)/2$.

–*claim* : Let $c \in K^\times$. The set D_c defines a bent functions.

–*sketch* : 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 :

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

Other Counter-Examples, order 151.

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 exceed the quadratic bound with spectral magnitude :

$$248, \quad 234, \quad 232, \quad 246.$$

Correlation Properties, order 151.

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 $\mathbf{Z}/151\mathbf{Z}$

A remarkable structure

Let D the support of sequence defining the "best" function.

$$D = [1] \cup [7] \cup [9] \cup [11] \cup [25] \cup [37] \cup [49]$$

$(7.31, 108, 100, 46)$ relative difference set.

As a subset of $\mathbf{Z}/217\mathbf{Z} = \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/31\mathbf{Z}$,

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

- D_1 is the Singer set $\{1, 2, 4\}$
- D_2 the Singer set $\{3, 5, 7, \ldots\}$

The End.