Boolean Functions: Cryptography and Applications BFCA'05
Fonctions Booléennes : Cryptographie & Applications

EXPONENTIAL SUMS AND BOOLEAN FUNCTIONS

Julien Bringer[1] and Valérie Gillot, Philippe Langevin[2]

Abstract. We study the nonlinearity of Boolean functions constructed by means of a subgroup of the multiplicative group of a finite field. The functions that we consider are constant over the non trivial cosets of a subgroup of small index. Classical properties of Gauss sums lead us to propose a new conjecture of the Patterson-Wiedemann type. One of the major steps of this approach consists in finding good estimations of exponential sums restricted over subgroup.

1. Nonlinearity

All along the paper, L denotes a finite extension of degree m of $\mathbf{F}_2$ the field of order two. The canonical additive character of L is denoted by μ. It is defined by means of the abolute trace of L over $\mathbf{F}_2$ by $\mu(x) = (-1)^{\mathrm{Tr}_L(x)}$. The *Fourier coefficient* of a complex mapping f is defined, at $a \in L$, by

$$\widehat{f}(a) = \sum_{x \in L} f(x)\mu\big(ax\big). \tag{1}$$

We denote by $R(f) := \sup_{a \in L} |\widehat{f}(a)|$ the *spectral amplitude* of f. One of the most exciting challenge at the intersection of the coding theory and cryptography consists in finding the minimal spectral amplitude that can achieve a binary function i.e. a mapping from L into ± 1. For a such function, the Parseval relation says that $R(f)$ is greater than or equal to $\sqrt{2^m}$. This fact splits the problem

[1] SAGEM Défense Sécurité SA. Avenue du Gros Chêne, 95610 Eragny-sur-Oise, France. email: `julien.bringer@sagem.com`
[2] GRIM, USTV. Bat. U, B.P. 20132. 83957 La Garde, France. email: `{gillot,langevin}@univ-tln.fr`

in two case according to the parity of m. In the case of m is even, there exists *bent functions* of spectral amplitude $\sqrt{2^m}$ and that is the best that we can do. The main questions are : how to construct bent functions, how to classify or merely how to count them. In the case of m is odd, the exact value of $R_m = \inf_f R(f)$ is not known, and the famous conjecture of Patterson-Wiedemann [6] claims the asymptotic behavior:

$$R_m \sim \sqrt{2^m}. \tag{2}$$

Now, let G be the subgroup of $L^\times$ of index v. We ask similar questions. What is the maximal value, say $R^v(f)$, of the character sums

$$\tilde{f}(a) = \sum_{x \in G} f(x)\mu(ax)?$$

The minimal value, say R^v_m of the $R^v(f)$'s when f ranges the set of binary functions is called the *spectral radius of index* v, in this paper we study theses numbers. The main goal of the present contribution is to exhibit examples of groups with small index such R^v_m is rather small. For one thing that could seem artificial but recent works of Bringer, summarized in the next section, show links with the Patterson-Wiedemann conjecture. In section (5), we recall the basic notion over exponential sums that we apply to construct our examples.

2. **Bringer construction**

Let G be a subgroup of index v of $L^\times$ and let Ω be the quotient group $L^\times/G$. Let s be a balanced mapping defined over Ω such that $s(\omega) = \pm 1$ for all $\omega \neq 1$, $s(1) = 0$, and $\sum_{\omega \in \Omega} s(\omega) = 0$. We consider the binary function

$$h(x) = f(x)g(x) + \sum_{1 \neq \omega \in \Omega} s(\omega) g(x/\omega) \tag{3}$$

where f is a binary function, and where g is the indicating function of G i.e. $g(x) = \begin{cases} 1, & x \in G; \\ 0, & x \notin G. \end{cases}$. In this paper, we will say that the binary function h is a configuration of index v by the sequence s and the section f, briefly a (v, s, f)-configuration. The function h

is constant over all cosets of G except over G itself. As in [4], we write the Fourier coefficient of g at a by means of Gauss sums

$$\hat{g}(a) = \frac{1}{v} \sum_{\chi \perp G} \tau_L(\chi)\bar{\chi}(a). \tag{4}$$

See [5], for generality on Gauss sums. Hence

$$\hat{h}(a) = \frac{1}{v} \sum_{\chi \perp G} \tau_L(\chi)s(\chi)\bar{\chi}(a) + \tilde{f}(a). \tag{5}$$

where $s(\chi) = \sum_{\omega \in \Omega} s(\omega)\bar{\chi}(\omega)$. Note this last sum is nothing but the multiplicative Fourier coefficient of s considered as a mapping from the group G into $\{-1, 0, +1\}$. For $\chi \neq 1$, let us set $\tau_L(\chi) = \upsilon(\chi)\sqrt{q}$, note that $|\upsilon(\chi)| = 1$. Since s is balanced, we have

$$\hat{h}(a) = \frac{\sqrt{q}}{v} \sum_{1 \neq \chi \perp G} \upsilon(\chi)s(\chi)\bar{\chi}(a) + \tilde{f}(a). \tag{6}$$

The last expression allows us to guess sufficients conditions in order to construct a configuration with a small spectral amplitude. For example, if the $\upsilon(\chi)$'s are closed to 1, for all the non trivial χ, then thanks to orthogonality relations, the previous equation becomes $\hat{h}(a) \sim s(\omega)\sqrt{q} + \tilde{f}(a)$, where $a \in \omega \in \Omega$. And so, if the second term is negligeable compared to $\sqrt{q}$, then h would have a spectral amplitude near $\sqrt{q}$. This kind of construction would be helpfull to confirm the Patterson and Wiedemann conjecture. The hypothesis of the example can be achieve in some special case (e.g. for some values of m or for m growing to infinity). A main problem is how small the second term can be.

This is a more general problem than the conjecture of Patterson and Wiedemann, but it is interesting to notice that, if we want to find functions with high non-linearity over L in a such way, we do not have to be very tight over G.

These are the reasons why, as we said in the introduction, we focus our interest in the last point and we try to understand the behaviour of R^v_m. First, note that the Parseval relation, as in the all space case, gives us a lower bound :

$$\sum_{a \in L} \tilde{f}(a)^2 = 2^m \frac{2^m - 1}{v} \Longrightarrow R^v(f) \geq \sqrt{\frac{2^m - 1}{v}}. \tag{7}$$

Again, the question is how far to this lower bound are we ? By analogy with the all-space case, and due to numerical results, we guess that the Patterson-Wiedemann conjecture would become :

Conjecture 2.1. Let v be an odd integer. For a large integer m such that $v \mid (2^m - 1)$:

$$R_m^v \sim \sqrt{\frac{2^m}{v}}$$

3. Quadratic residue construction

In this section, we present a nice configuration involving quadratic residue that gives an higly nonlinear Boolean function of 15 variables constant on the group of index 7 of $\mathbf{F}^{\times}{}_{2^{15}}$.

Let $v > 3$ be a prime congruent to 3 modulo 4 such that 2 generates the group of quadratic residues modulo v. In the terminology of [3], the pair $(v, 2)$ satisfies the *quadratic residue conditions*. Let χ be a multiplicative character of order v. There exist integers t, A and B such that :

$$\tau_L(\chi) = 2^t(A + B\sqrt{-v}), \quad 2 \not| AB;$$

where t is deeply connected to both Stickelberger theorem and the class number of the quadratic field $\mathbf{Q}(\sqrt{-l})$. For all $0 \leq j < v$,

$$\tau_L(\chi^j) = 2^t\big(A + \left(\frac{j}{v}\right)B\sqrt{-v}\big)$$

Let γ be primitive root of L. We assume that $\chi(\gamma)$ is equal to ζ_v the principal root of order v. The elements γ^0, γ^1,..., γ^{v-1} forms a system of representatives of Ω. We define the *quadratic residue spread* by

$$h(x) = \sum_{j=1}^{v-1} \left(\frac{j}{v}\right) g(\gamma^{-j}x).$$

It is a balanced function, $\hat{h}(0) = 0$ and the other Fourier coefficients are given by means of the Legendre symbole

$$\hat{h}(\gamma^k) = 2^t \times \big(\left(\frac{k}{v}\right)A - B + vB\delta_0(k)\big) \tag{8}$$

where $\delta_0(k) = 1$ or 0 according to whether $k = 0$ or not. Indeed, from Gauss we know $\sum_{j=0}^{v-1} \left(\frac{j}{v}\right) \zeta_v^{ks} = \left(\frac{s}{v}\right)\sqrt{-v}$. In particular, $s(\chi^j) = \sum_{i=0}^{v-1} \left(\frac{i}{v}\right) \bar{\chi}(\gamma^{ij}) = -\left(\frac{j}{v}\right)$. The remainder is a straightforward calculation:

$$\begin{aligned}
v\hat{h}(\gamma^k) &= \sum_{j=1}^{v-1} \tau_L(\chi^j) s(\bar{\chi}^j) \chi^j(\gamma^k) = -\sum_{j=1}^{v-1} \tau_L(\chi^j) [\left(\frac{j}{v}\right)\sqrt{-v}] \zeta^{kj} \\
&= -2^t \sum_{j=1}^{v-1} [A\left(\frac{j}{v}\right)\sqrt{-v} - Bv] \zeta^{kj} \\
&= -2^t A\sqrt{-v} \sum_{j=1}^{v-1} \left(\frac{j}{v}\right) \zeta^{kj} + 2^t Bv \sum_{j=1}^{v-1} \zeta^{kj} \\
&= 2^t Av\left(\frac{k}{v}\right) + 2^t Bv \sum_{j=1}^{v-1} \zeta^{kj}.
\end{aligned}$$

Let χ be a multiplicative character of order 7 in $\mathbf{F}_{2^{15}}$. We can realize χ as the lift of a non trivial multiplicative character χ' of $\mathbf{F}_8$, so that

$$\tau_{\mathbf{F}_{2^{15}}}(\chi) = (\tau_{\mathbf{F}_8}(\chi'))^5 = (-1 + \sqrt{-7})^5 = -16(11 + \sqrt{-7})$$

i.e. $A = 11$ and $B = 1$, whence the Fourier transform of the quadratic spread takes the values -160, -96 and 192.

By an exhaustive computer search among the monomial x^s, we have found that the binary function

$$h(x^s) = \mu(x^{755}) g(x) + \sum_{j=1}^{v-1} \left(\frac{j}{v}\right) g(\gamma^{-j} x).$$

has spectral amplitude 232 when $s = 755$. The spectrum of the function is detailed in TABLE 1. We believe it is possible to obtain such good nonlinearity for all the instances $m = 3r$ for which the Gauss sums lies within a narrow angular sector. It is the case for $m = 15$. According to the table TABLE 2 below, the best situation for that point of view seems $r = 13$ i.e. for dimension 39.

TABLE 1. Spectrum of the quadratic resisue spread $h(x) = \mu(x^{755})g(x) + \sum_{j=1}^{v-1} \left(\frac{j}{v}\right) g(x/\gamma^j)$.

value	-216	-152	-88	-24	40	104	168	232
multiplicity	7550	6494	1208	3020	755	151	6795	6795

TABLE 2. arguments of the Gauss sums for the group of index 7 in an extension of degree r of $\mathbf{F}_8$ lies in a sector of Δ degree.

r	13	26	39	52	65	78	91	96	83	70	57	31	44	18	5
Δ	1	3	5	7	9	11	11	15	17	19	21	23	13	25	27

4. Asymptotic Bound

Asymptotically, it is known [7] that almost all boolean functions have high non linearities, and so that they have low spectral amplitudes. For binary functions over a subgroup G of $L^\times$, we show here that this phenomenon is always true.

First, let us recall known bounds on sums of binomial coefficients.

Lemma 4.1. *Let N be any positive integer and $0 < \lambda < 1/2$. Then*

$$\frac{2^{NH_2(\lambda)}}{\sqrt{8N\lambda(1-\lambda)}} \leq \sum_{0\leq i\leq \lambda N} \binom{N}{i} \leq 2^{NH_2(\lambda)} < 2^N e^{-2N(1/2-\lambda)^2}$$

where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the entropy function.

This lemma implies the following result :

Theorem 4.2. *Let $m > 0$ be an integer, G a subgroup of $L^\times$ and N, v the order and the index of G. Let c be any strictly positive real number such that $N > 2c^2m$. Then, the density of the set $\{f : G \to \{\pm 1\}, R^v(f) \leq c\sqrt{2Nm}\}$ is greater than $1 - 2^{m(1-c^2\log_2(e))}$.*

If $c^2\log_2(e) > 1$, then this density tends to 1 when m tends to infinity. For every $m \geq 3$ and G such that $N > 2m$, a majority of functions f defined over G are such that $R^v(f) \leq \sqrt{2Nm}$.

Proof. Let $l : L \to \mathbf{F}_2$ be a linear function and l_G its restriction over G, then the number of functions $f : G \to \{\pm 1\}$, such that the distance between f and $\mu(l_G)$ over G is lower than $N/2 - c\sqrt{m}\sqrt{N/2}$, is :

$$A = \sum_{0 \le i \le N/2 - c\sqrt{m}\sqrt{N/2}} \binom{N}{i}.$$

Thanks to lemma 4.1, we deduce that : $A \le 2^N e^{-2N(1/2-\lambda)^2}$, where $0 < \lambda = 1/2 - c\sqrt{m}/\sqrt{2N} < 1/2$. So, $A \le 2^{N - mc^2 \log_2(e)}$.

Hence, the number of functions f at a distance over G lower than $N/2 - c\sqrt{m}\sqrt{N/2}$ from a linear function is at most $2^m A = 2^{m+N-mc^2\log_2(e)}$. As $\tilde{f}(a) = N - 2d(f, x \mapsto \mu(ax))$, we obtain that the density of the set defined previously in the theorem, among all the binary functions defined over G, is greater than $1 - 2^{m(1-c^2\log_2(e))}$.

Moreover, if $c^2 \log_2(e) > 1$ and if we have a sequence $(G_m)_m$, where for all m, G_m is a subgroup of order $N_m > 2c^2 m$ of $\mathbf{F}_{2^m}^\times$, then the density, of the functions defined over G_m such that $R^{v_m}(f) \le c\sqrt{2N_m m}$, tends toward 1 when m grows to the infinity.

For the last result, notice that we have $2^{m(1-c^2\log_2(e))} < \frac{1}{2}$ if $m \ge 3$ and $c = 1$. $\square$

Hence, if $m \ge 3$ and $N > 2m$, then

$$\sqrt{\frac{2^m - 1}{v}} \le R_m^v \le \sqrt{2m}\sqrt{\frac{2^m - 1}{v}},$$

and a majority of functions are between these two bounds. Notice that in particular, if $N = o(2^m/m)$, then the majority of binary functions f defined over G are such that $R^v(f) = o(\sqrt{2^m})$. Which is sufficient, added to the others points seen in section (2), to construct boolean functions with high non linearities.

5. Exponential Sums

We consider a polynomial $f(X) \in L[X]$ and we write $\tilde{f}(a)$ the Fourier coefficient of the binary function $x \mapsto \mu\big(f(x)\big)$:

$$\tilde{f}(a) = \sum_{x \in G} \mu\big(f(x) + ax\big) = \frac{1}{v} \sum_{x \in L^\times} \mu\big(f(x^v) + ax^v\big). \qquad (9)$$

In particular, if the degree of $f(X)$ is an odd integer $s > 1$ the famous Hasse-Weil bound gives the estimation

$$R^v(f) \leq \frac{1}{v}(sv-1)\sqrt{2^m} + \frac{1}{v} \lesssim s\sqrt{2^m}. \tag{10}$$

This in comparison of (7) seems bad. However, when the index of G is fixed and m increases then (10) is the best that one can say. Whence, for a given polynomial, there is infinitely many extensions such that the Parseval bound (7) is far from the reallity.

The objective of this section is to estimate the spectral amplitude of index v of monomials $f(x) = \gamma x^s$ for certain $\gamma \in L$ and integer s. If m is not prime ($m = lt$), the strategy consists to evaluate the exponential sum over $K = \mathbf{F}_q$ instead of L, with $[L : K] = l$ and $q = 2^t$, like in [2]. So, we search instances of (m, l, t, v, s) where v is the index of a group G and s an exponent such that $R^v(\gamma x^s)$ is small for a good choice of $\gamma \in L$. In practice, it is difficult to obtain smooth hypersurfaces from any γx^s. So, we determine the forms of s and vs to apply the results of [2]. Let $w_q(e)$ be the sum of the digits of the q-ary expansion of an integer e. Assume that $w_q(s) \neq w_q(sv)$, denote $w = \max\{w_q(s), w_q(sv)\}$ and let $d \in \{v, sv\}$ the integer such that $w = w_q(d)$.

If $d < q$ is odd or if the q-ary expansion of d is $d = 1 + kq^j$ for any even integer k and $j < (m/l)$, then Theorem 2.1 in [2] gives the following estimation

$$R^v(f) \leq \frac{1}{v}(w-1)^l\sqrt{2^m} + \frac{1}{v} \tag{11}$$

With a computer, we can find a lot of numerical intances (m, l, t, v, s) satisfying $(w-1)^l < (sv-1)$. Unfortunately, we did not find any which satisfy the inequality (**??**). We obtain the following proposition for group with index 3.

Proposition 5.1. *Set $m = 2t$, with odd t. Consider $f(x) = \gamma x^s$, with $\mathrm{Tr}_{L/K}(\gamma) \neq 0$. The instance $\big(2t, 2, t, 3, (q+1)/3\big)$ satisfies*

$$R^3_m(f) \leq \frac{4}{3}\sqrt{2^m} + \frac{1}{3} \tag{12}$$

Proof. Set $m = 2t$, $v = 3$, $vs = q + 1$. If $f(x) = \gamma x^s$, we have to estimate

$$\tilde{f}(a) = \frac{1}{v} \sum_{x \in L^\times} \mu\big(\gamma x^{sv} + a x^v\big) = \frac{1}{v} \sum_{x \in L^\times} \mu\big(\gamma x^{q+1} + a x^3\big)$$

If $a \neq 0$, $\max\{w_q(3), w_q(q+1)\} = 3$, the estimation (11) gives (12). If $a = 0$, we have to calculate

$$\tilde{f}(0) = \frac{1}{v} \sum_{x \in L^\times} \mu\big(\gamma x^{q+1}\big)$$

Let μ_K be the additive character of K and let be $x \in L^\times$,

$$\mu(\gamma x^{q+1}) = \mu_K(\mathrm{Tr}_{L/K}(\gamma x^{q+1})) = \mu_K(x^{q+1}\mathrm{Tr}_{L/K}(\gamma)).$$

The map from $L^\times$ to $K^\times$ defined by $x \mapsto x^{q+1}$ is onto, so we have

$$\tilde{f}(0) = \frac{q+1}{v} \sum_{y \in K^\times} \mu_K(y\mathrm{Tr}_{L/K}(\gamma)) = -\frac{q+1}{v}$$

Thus, the inequality (12) rises from $|\tilde{f}(0)| = \frac{q+1}{3} \leq \frac{4}{3}q + \frac{1}{3}$. □

References

[1] Bringer J., Nonlinearity of some Patterson-Wiedemann type functions. *Yacc-04 Conference*, Porquerolles, France (2004).

[2] Gillot V., Bounds for Exponential Sums over Finite Fields *Finite Fields and Their Applications*,vol.1, pp 421–436 (1995).

[3] Langevin P., A New Class of Two Weight Codes. *Finite Fields Conference Fq3*, Glasgow, Scotland pp 181–187 (1996).

[4] Langevin P., Zanotti J.-P., A Note on the Counter-Example of Patterson-Wiedemann. *Finite Fields Conference Fq6*, Oaxaca, Mexico pp 214–219 (2001)

[5] Lidl R., Niederreiter H., Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20 (1983).

[6] 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*, vol. 29, pp 354–356 (1983).

[7] Rodier F., Sur la non-linéarité des fonctions booléennes, *Acta Arithmetica*, vol. 115, pp 1–22 (2004).

.