Non-linearity of the Carlet-Feng function, and repartition of Gauss sums

François Rodier*

Abstract

The search for Boolean functions that can withstand the main crypyographic attacks is essential. In 2008, Carlet and Feng studied a class of functions which have optimal cryptographic properties with the exception of nonlinearity for which they give a good but not optimal bound. After several people have worked on this problem of nonlinearity they have asked for a new answer to this issue. We provide a new solution to improve the evaluation of the nonlinearity of the Carlet-Feng function, by means of the estimation of the distribution of Gauss sums. This work is in progress and we give some suggestions to improve this work.

Keywords: Carlet-Feng function, nonlinearity, Gaussian sums, equidistribution, discrepancy

1 Introduction

Boolean functions on the space $\mathbb{F}_2^m$ are important in cryptography, where they occur in stream ciphers or private key systems. In both cases, the properties of systems depend on the nonlinearity of a Boolean function. The nonlinearity of a Boolean function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ is the distance from f to the set of affine functions with m variables. The nonlinearity is therefore an important cryptographic parameter. We refer to [1] for a global survey on the Boolean functions.

It is useful to have at one's disposal Boolean functions with highest nonlinearity. The problem of the research of the maximum of the degree of nonlinearity comes down to minimize the Fourier transform of Boolean functions.

1.1 The Carlet-Feng function

Let n be a positive integer and $q = 2^n$. In 2008, Carlet and Feng [2] studied a class of Boolean functions f on $\mathbb{F}_{2^n}$ which is defined by their support

$$\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\}$$

where α is a primitive element of the field $\mathbb{F}_{2^n}$. In the same article they show that these functions when n varies have optimum algebraic immunity, good nonlinearity and optimum algebraic degree. These computations are very good but still not good enough: in fact these bounds are not enough for ensuring a sufficient nonlinearity. Some works have been done on that by Q. Wang and P. Stanica [10] and other authors (cf. Li et al [7] and Tang et al. [9]). They find the bound

$$2^{n-1} - nl(f) \leq \frac{1}{\pi} q^{1/2} \left(n \ln 2 + \gamma + \ln\left(\frac{8}{\pi}\right) + o(1) \right)$$

*Aix Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, UMR 7373, 13288 Marseille, France

where γ is the Euler's constant. Nevertheless, there is a gap between the bound that they can prove and the actual computed values for a finite numbers of functions which are very good, of order $2^{n-1} - 2^{n/2}$. Carlet and some authors cited above [7, 9, 10] who have also worked on this nonlinearity asked for new answer to this problem. In this paper we bring a new solution to improve the evaluation of the nonlinearity of the Carlet-Feng function, by means of the estimation of the distribution of Gauss sums. We will find a slightly better asymptotic bound (see (2)) but this work is in progress and we give some suggestions to improve this work and hopefully to get a result closer to what expected. It will be the same for other classes of Boolean functions which are based on Carlet-Feng construction.

1.2 The nonlinearity

The nonlinearity of these functions is given by

$$nl(f) = 2^{n-1} - \max_{\lambda \in \mathbb{F}_{2^n}^*} |S_\lambda| \quad \text{where} \quad S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{\mathrm{Tr}(\lambda\alpha^i)}. \tag{1}$$

We define $\zeta = \exp\left(\frac{2i\pi}{2^n-1}\right)$, χ be the multiplicative character of $\mathbb{F}_{2^n}$ such that $\chi(\alpha) = \zeta$. For $a \in \mathbb{F}_q^*$ let us define the Gaussian sum $G(a, \chi)$ by

$$G(a, \chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \exp(\pi i \,\mathrm{Tr}(ax))$$

and $G(\chi) = G(1, \chi)$. Let $\lambda = \alpha^\ell$ with $1 \le \ell \le q-2$. By Fourier transformation of (1) we get

$$S_\lambda = \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} G(\chi^\mu)\zeta^{-\mu\ell} \frac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}} - \frac{q}{2} \right).$$

Carlet and Feng deduced from that the bound

$$|S_\lambda| \le \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} \sqrt{q} \left| \frac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}} \right| + \frac{q}{2} \right).$$

The upperbound of $|S_\lambda|$ is attained if the arguments of $G(\chi^\mu)\zeta^{-\mu\ell}$ are the opposite of the ones of $\frac{\zeta^{-\mu(\frac{q}{2}-1)}-1}{1-\zeta^{-\mu}}$. I will show that this situation is impossible and that will lead us to a better bound.

2 Equidistribution of the arguments of Gauss sums

2.1 A result of Nicolas Katz

Nicolas Katz (chapter 9 in [5]) has proved that

Proposition 2.1 *For a fixed in $\mathbb{F}_{2^n}^*$ the arguments of $G(a, \chi^\mu)$ for $1 \le \mu \le q-2$ are equidistributed on the segment $[-\pi,\ \pi]$.*

For l fixed in $\mathbb{F}_{2^n}^*$ the arguments of $G(\chi^\mu)\zeta^{-\mu l}$ for $1 \le \mu \le q-2$ are also equidistributed on the segment $[-\pi,\ \pi]$ since by [8] theorem 5.12, they satisfy: $G(\chi^\mu)\zeta^{-\mu l} = G(\alpha^l, \chi^\mu)$.

2.2 Discrepancy

To get a result a little more precise than Katz's we need the notion of discrepancy. We define the discrepancy (see [4] or [6]) of a sequence of N real numbers $x_1, \ldots, x_N \in [0,\ 1[$ by

$$D_N(x_N) = \max_{0 \le x \le 1} |\frac{A(x,N)}{N} - x|$$

where $A(x,N) =$ number of $m \le N$ such that $x_m \le x$.

Proposition 2.2 *A sequence $(x_N)_{N\ge 1}$ is uniformly distributed mod 1 if and only if*

$$\lim_{N\to\infty} D_N(x_N) = 0.$$

We have an estimate of the discrepancy thanks to Erdös-Turan-Koksma's inequality.

Lemma 2.3 (Erdös-Turan-Koksma's inequality) *There is an absolute constant C (independent of x_N) such that for every $H \ge 1$,*

$$D_N(x_N) < C\left(\frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h}\left|\frac{1}{N}\sum_{m=1}^{N} \exp(2\pi i h x_m)\right|\right)$$

We will use also a result of Deligne obtained by using Algebraic Geometry "à la Grothendieck".

Proposition 2.4 (Deligne [3]) *For ψ an additive character of $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, we have*

$$|\sum_{x_1 x_2 \ldots x_r = 1} \psi(x_1 + x_2 + \cdots + x_r)| \le r q^{(r-1)/2}.$$

With this proposition, we can show that, for $a \ne 0$ one has $|\sum_{1\le\mu\le q-2} G(a,\chi^\mu)^r| \le 1 + rq^{(r+1)/2}$. So we can show more than Katz's result with the help of proposition (2.2).

Proposition 2.5 *For l fixed in $\mathbb{F}_{2^n}^*$ the arguments $\arg(z_\mu)$ of $z_\mu = G(\chi^\mu)\zeta^{-\mu l}$ for $1 \le \mu \le q-2$ fulfill*

$$D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) < O(q^{-1/4})$$

Proof: We use Erdös-Turan-Koksma's inequality to evaluate this dicrepancy, and use Deligne's result to bound $|\sum_{1\le\mu\le q-2} G(a,\chi^\mu)^r|$ which gives the result. Whence, if $H \le q^{1/2}$

$$\begin{aligned} D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) &< O\left(\frac{1}{H} + \frac{1}{q-2}\sum_{h=1}^{H}\frac{1}{hq^{h/2}}\left|\sum_{\mu=1}^{q-2} G((-1)^{\mathrm{Tr}(\alpha^l)},\chi^\mu)^h\right|\right) \\ &< O\left(\frac{1}{H} + \frac{1}{q-2}\sum_{h=1}^{H}\frac{1}{hq^{h/2}}hq^{(h+1)/2}\right) \\ &= O\left(\frac{1}{H} + \frac{Hq^{1/2}}{q-2}\right) \end{aligned}$$

If $H = q^{1/4}$, then $D_{q-2}\left(\frac{\arg(z_\mu)}{2\pi}\right) < O\left(\frac{q^{3/4}+q^{3/4}}{q-2}\right) = O\left(q^{-1/4}\right)$. □

Lemma 2.6 *If the a_m is an increasing sequence and if the discrepancy of a_m is D, then $|a_i - \frac{i}{m}| \le D$.*

Proof: The lemma is a consequence of [6, Section 2, Discrepancy, theorem 1.4]. □

3 Distribution of the arguments of a_μ

Let $a_\mu = \dfrac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}}$.

Proposition 3.1 *The a_μ are on the singular plane cubic which is the image of the unit circle by the map*

$$z \longrightarrow \frac{1}{z + z^2}$$

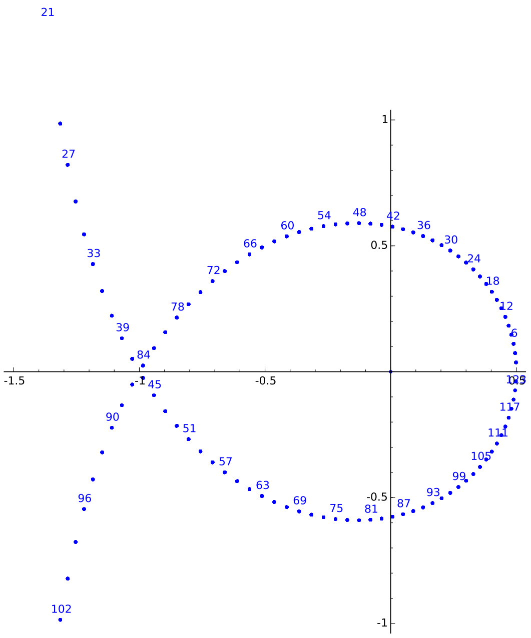
with $|z| = 1$. The absolute value is $|a_\mu| = (2\cos(\frac{\pi\mu}{2(q-1)}))^{-1}$. The argument is $\arg a_\mu = \frac{3\pi\mu}{2(q-1)}$ for μ even or $\pi/2 + \frac{3\pi\mu}{2(q-1)}$ for μ odd. The complex conjugate of a_μ is $a_{q-1-\mu}$.

Proof: If μ is even, let us take $z = \exp(-\frac{\pi\mu i}{q-1})$. One has $z^2 = \zeta^{-\mu}$. And one has also

$$z^{q-1} = \exp(-\pi\mu i) = \exp(-2\pi i\mu/2) = 1.$$

Thus $z^{q-2} = z^{-1}$, hence $a_\mu = \frac{z^{2(\frac{q}{2}-1)}-1}{1-z^2} = \frac{z^{(q-2)}-1}{1-z^2} = \frac{z^{-1}-1}{1-z^2} = \frac{1-z}{z-z^3} = \frac{1}{z+z^2}$. If μ is odd, we just use $z = -\exp(-\frac{\pi\mu i}{q-1})$. To compute the absolute value and the argument of a_μ, you just have to consider the rhombus of vertices $0, z, z+z^2, z^2$. □

3.1 Exemple: with $m = 7$



4 Applications

So we conclude from the preceding sections that for a fixed ℓ the arguments of $G(\chi^\mu)\zeta^{-\mu\ell}$ are equidistributed on $[-\pi,\ \pi]$, and the arguments of a_μ are equidistributed on $[-3\pi/2,\ 3\pi/2]$

so, as we said before, it is impossible to have $\arg(G(\chi^{\mu})\zeta^{-\mu\ell})+\arg(a_{\mu}) = 0 \pmod{2\pi}$ and the upperbound of $|S_{\lambda}|$ is not attained.
So, in place of computing the sum $\sum_{\mu=1}^{q-2} G(\chi^{\mu})\zeta^{-\mu\ell}a_{\mu}$ we can replace it by the sum $\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_{\mu})$ where $H = \{h_{\mu}\}$ is the set of Gauss sums and σ is some permutation of this set. Let us renumber the h_{μ} for μ even (with multiplicities) in the anticlockwise orientation: from h_2 which will be of weakest positive or zero argument up to h_{q-2} which will be of higher positive argument. Let $k_x = q^{1/2}\exp\left(i\left(\frac{2\pi x}{q-1}\right)\right)$. Let σ runs over the set of all permutation of the set H. The preceding proposition implies $\sum_{\mu=1}^{q-2} G(\chi^{\mu})\zeta^{-\mu\ell}a_{\mu} \leq 2\max_{\sigma}\left(\Re e \sum_{\substack{\mu=2\\ \mu \text{ even}}}^{q-2}(\overline{h_{\sigma(\mu)}}a_{\mu})\right)$.

Lemma 4.1 *For $2 \leq \mu \leq q-2$ and μ even, we have*

$$\left|\Re e(\overline{h_{\sigma(\mu)}}a_{\mu} - \overline{k_{\sigma(\mu)}}a_{\mu})\right| = O\left(\frac{q^{1/4}}{\cos\frac{\pi\mu}{2(q-1)}}\right)$$

Proof: We use Proposition 2.5 and Lemma 2.6. □

From Proposition 2.5, we get the following lemma.

Lemma 4.2 *The sums $\Re e \sum_{\substack{\mu=2\\ \mu\ even}}^{q-2}(\overline{h_{\sigma(\mu)}}a_{\mu})$ satisfy*

$$\max_{\sigma}\left(\Re e\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_{\mu})\right) \leq 2\Re e\sum_{\substack{\mu=2\\ \mu\ even}}^{q/2}(\overline{b_{\mu}}a_{\mu}) + O(q^{5/4}\log q)$$

where we denote by b_{μ} the following numbers for μ even and $2 \leq \mu \leq q-2$: if $2 \leq \mu \leq q/2$, then $b_{\mu} = k_{\mu/2}$, if $q/2 < \mu \leq 2q/3$, then $b_{\mu} = k_{3\mu/2-q/2}$, if $2q/3 < \mu \leq q-2$, then $b_{\mu} = k_{3\mu/4}$.

Proof: We use the lemma 4.1 to replace $\max_{\sigma}\left(\Re e\sum_{\mu=1}^{q-2}(\overline{h_{\sigma(\mu)}}a_{\mu})\right)$ by $\max_{\sigma}\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}}a_{\mu})\right) + O(q^{5/4}\log q)$.
Then denote by D the discrepancy of the sequence H. Let β be the largest integer (if there is some) such that $|\arg k_{\sigma(\beta)} - \arg(b_{\beta})| > 2\pi D$. Then for all $\mu > \beta$ we have $|\arg k_{\sigma(\mu)} - \arg(b_{\mu})| \leq 2\pi D$. From the lemma 2.6 there exists γ such that $|\arg k_{\sigma(\gamma)} - \arg(b_{\beta})| \leq 2\pi D$. Let τ be the transposition between β and $\sigma(\gamma)$. Then one can check that

$$\Re e(\overline{b_{\beta}}a_{\beta} + \overline{k_{\sigma(\gamma)}}a_{\sigma(\gamma)}) > \Re e(\overline{k_{\sigma(\gamma)}}a_{\beta} + \overline{b_{\beta}}a_{\sigma(\gamma)})$$

therefore $2\Re e\sum_{\substack{\mu=1\\ \mu \text{ even}}}^{q-2}(\overline{k_{\sigma(\mu)}}a_{\mu}) < 2\Re e\sum_{\substack{\mu=1\\ \mu \text{ even}}}^{q-2}(\overline{k_{\sigma\circ\tau(\mu)}}a_{\mu})$ and the sum is not maximal. So, if the sum is maximal, then there does not exist such a β, that is for all μ we have $|\arg k_{\sigma(\mu)} - \arg(b_{\mu})| \leq 2\pi D$. Whence $\left|\Re e\sum_{\mu=1}^{q-2}(\overline{b_{\mu}}a_{\mu}) - \max_{\sigma}\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}}a_{\mu})\right)\right| \leq O(q^{5/4}\log q)$.
Let B be the set of all b_{μ}'s for μ even. Now we have to take also in consideration the μ odd. When you make the same reasoning, you end up with a set $\overline{B}$ which is just the complex conjugate of B. When you take the union $B \cup \overline{B}$, you get q elements uniformly distributed in the interval $[0,\ 2\pi]$. □

Proposition 4.3 *The upper bound of* $\sum_{\mu=1}^{q-2} G(\chi^{\mu})\zeta^{-\mu\ell}a_{\mu}$ *is at most equal to*

$$\frac{q^{3/2}}{\pi}(\ln q - 0.3786 + o(1)).$$

Proof: Up to $O(q^{5/4}\log q)$ it is enough to compute:

$$\begin{aligned}\max_{\sigma}\left(\Re e\sum_{\mu=1}^{q-2}(\overline{k_{\sigma(\mu)}a_{\mu}})\right) &\leq 2q^{1/2}\sum_{\substack{\mu=1\\ \mu\text{even}}}^{q/2}\frac{1}{2} - 2q^{1/2}\sum_{\substack{\mu=q/2\\ \mu\text{even}}}^{2q/3}\frac{\cos\frac{3\pi\mu}{2(q-1)}}{2\cos\frac{\pi\mu}{2(q-1)}} + 2q^{1/2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}}\\ &\leq \frac{q^{3/2}}{2} - 4q^{1/2}\sum_{\substack{\mu=q/2\\ \mu\text{even}}}^{2q/3}\cos^2\frac{\pi\mu}{2(q-1)} + 2q^{1/2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}}.\end{aligned}$$

Since the function $\frac{1}{2\cos(x\pi/2)} - \frac{1}{\pi(1-x)}$ is continuous on $[2/3,\ 1]$, and since the $\frac{\mu}{q-1}$ are uniformly distributed on $[2/3,\ 1]$ we get by [6, theorem 1.1]:

$$\begin{aligned}&\frac{2}{q-2}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{2\cos\frac{\pi\mu}{2(q-1)}} - \frac{2}{\pi}\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}\frac{1}{q-\mu} = (1+o(1))\int_{2/3}^{1}\left(\frac{1}{2\cos\frac{x\pi}{2}} - \frac{1}{\pi}\frac{1}{1-x}\right)dx\\ = &\frac{\ln 2\ -\ln\pi + \ln 3}{\pi} - \frac{\ln(7+4\sqrt{3})}{2\pi} + o(1).\end{aligned}$$

Then, using Euler's formula on harmonic series:

$$\frac{2}{q^{1/2}(q-2)}\Re e\sum_{\substack{\mu=2q/3\\ \mu\text{even}}}^{q-2}(\overline{\sigma(h_{\mu})a_{\mu}}) \leq \frac{\log q - \ln\pi + \gamma}{\pi} - \frac{\ln(7+4\sqrt{3})}{2\pi} + o(1).$$

Finally, it is easy to compute the other terms, and we get the result. □

4.1 Final result

Having noticed that

$$\left|\sum_{\mu=1}^{q-2}G(\chi^{\mu})\zeta^{-\mu\ell}a_{\mu}\right| \leq 2\max_{\sigma}\left(\Re e\sum_{\substack{\mu=2\\ \mu\text{even}}}^{q-2}(\overline{h_{\sigma(\mu)}a_{\mu}})\right) + O(q^{5/4}\log q)$$

we get finally

Theorem 4.4 *The nonlinearity of the Carlet-Feng function fulfills*

$$2^{n-1} - nl(f) \leq \frac{q^{1/2}}{\pi}\left(\log q - 0.3786 + o(1)\right). \tag{2}$$

5 Conclusion

The improvement is not very important, but this argument may be optimised by

- taking in account the invariance of Gauss sums under the Frobenius automorphism;
- making it possible to make our argument work for all n instead of having an asymptotic result;
- taking in account the irregularity of the distribution of Gauss sums (one way to do this might be to look at the equidistribution of several Gauss sums simultaneously);
- improving the bound of nonlinearity for other classes of Boolean functions which are based on Carlet-Feng construction.

References

[1] Claude Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monography, Boolean Models and Methods in Mathematics, Computer Science and Engineering published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257-397, 2010.

[2] Claude Carlet, Keqin Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. Advances in cryptology- ASIACRYPT 2008, 425-440, Lecture Notes in Comput. Sci., 5350, Springer, Berlin, 2008.

[3] Deligne, P., Applications de Ia formule des traces aux sommes trigonometriques, in: Cohomologie Etale (SGA 4 1/2), Lecture Notes in Mathematics, vol. 569, Springer-Verlag.

[4] M. Drmota and R. Tichy, Sequences, discrepancies and applications, Springer-Verlag, Berlin, 1997.

[5] Katz, N.: Gauss Sums, Kloosterman Sums and Monodromy Groups, Annals of math. Studies 116, Princeton Univ. Press, 1988

[6] L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Wiley-Interscience, New York-London-Sydney, 1974.

[7] Jiao Li , Claude Carlet , Xiangyong Zeng , Chunlei Li, Lei Hu , Jinyong Shan, *Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks* Des. Codes Cryptogr. 76 (2015), no. 2, 279-305.

[8] R. Lidl, and H. Niederreiter, *Introduction to finite fields and their applications.* Cambridge university press, 1994.

[9] Tang D., Carlet C., Tang X. *Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks.* IEEE Trans. Inform. Theory 59 (2013), no. 1, 653-664.

[10] Qichun Wang, Pantelimon Stanica, Trigonometric Sum Sharp Estimate and New Bounds on the Nonlinearity of Some Cryptographic Boolean Functions, Des. Codes Cryptogr. 87 (2019), no. 8, 1749-1763.