On the Nonlinearity of Power Functions

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

AGCT-8, Marseille 14—18 Mai 2001.

Nonlinearity

- Let L be a finite field of characteristic 2 and order $q = 2^m$.
- $x \mapsto \mathrm{Tr}_L(x)$ the absolute trace of L.

The **nonlinearity** of $f\colon L \to L$ is the maximal distance between the boolean function $x \mapsto \mathrm{Tr}_L\big(f(x)\big)$ and the set of all affine functions

$$x \mapsto \mathrm{Tr}_L(ax) + b, \quad a \in L, b \in \mathbf{F}_2.$$

- $\mu(x) = (-1)^{\mathrm{Tr}_L(x)}$ the canonical character of L

a such distance is

$$2^{m-1} - \frac{(-1)^b}{2} \underbrace{\sum_{x \in L} \mu\big(f(x) + ax\big)}_{\text{Fourier transform}}$$

Fourier Coefficient

The character sum

$$\sum_{x \in L} \mu\big(f(x) + ax\big) \qquad \textbf{Fourier coefficient}$$

$$R(f) := \sup_{a \in \mathbf{F}_2^m} |\widehat{f}(a)| \qquad \textbf{spectral magnitude}$$

▷ The nonlinearity of f is

$$2^{m-1} - \frac{1}{2}\mathrm{R}(f).$$

For cryptographic applications the functions minimizing the spectral magnitude i.e. maximizing the nonlinearity are of great interest.

Bent Functions

$$R(m) := \inf_f R(f), \quad RB(m) := \inf_{f:1-1} R(f)$$

Highly Nonlinear iff $R(f) = R(m)$.

▷

$$\sum_{a \in L} \left(\hat{f}(a)\right)^2 = 2^{2m} \quad \text{(Parseval)} \quad \Longrightarrow \sqrt{2^m} \leq R(f)$$

When m even $R(m) = \sqrt{2^m}$, and f is highly nonlinear iff $R(f) = \sqrt{2^m}$ iff $\hat{f}(a) = \pm 2^{m/2}$ that is a **bent functions**[a].

–*Conjecture*: $R(m) \sim \sqrt{2^m} \sim RB(m)$

$RB(8)$ and $R(9)$ still unknown...

[a] Rothaus, 1976

Cryptographic Parameters

▷ Links between differential cryptanalysis and linear cryptanalysis, Chabaud and Vaudenay, Eurocrypt 94.

Resistance against linear attack

$$\Lambda(f) := \max_{b \in L^\times} R(bf)$$

▷ Let $\delta(a,b)$ be the number of solution of the equation $f(x+a)+f(x)=b$

Resistance against differential attack

$$\Delta(f) := \max_{a \in L, b \in L^\times} \delta(a,b)$$

Almost Perfect Nonlinear APN realize $\Delta(f) = 2$.

Bounds from Fourier Analysis

The "good" functions minimize $\Lambda(f)$ and $\Delta(f)$.

$$\sum_{a,b\in L}\left(\widehat{bf}(a)\right)^4 = 2^{2m}\sum_{a,b}\delta(a,b)^2$$

- again Parseval...

$$\Lambda(f)^2 \geq 2^{m+1}$$

Now, equality is possible when m is odd. In that case f is APN and **almost bent** i.e. the <u>nonzero</u> Fourier coefficients are $\pm 2^{(m+1)/2}$.

A Basic Example

For any $a \in L^\times$, the polynomial $(x+a)^3 + x^3$ has degree two whence $\Delta(x^3) = 2$ and $x \mapsto x^3$ is almost perfect nonlinear.

$$\big(\hat{f}(a)\big)^2 = \Big(\sum_{x \in L} \mu(x^3 + ax)\Big)^2 = \sum_{x \in L} \sum_{y \in L} \mu(x^3 + by^3 + ax + ay)$$

$$= \sum_{x,y \in L} \mu(x^2 y + xy^2 + ax) = 2^m \sum_{x \in K} \mu(ax)$$

where K is the kernel of the symmetric bilinear form $(x, y) \mapsto \mathrm{Tr}_L(x^2 y + xy^2)$. If m is odd then $K = \mathbf{F}_2$ otherwise $K = \mathbf{F}_4$, in all the case

$$\mathrm{R}(x^3) = 2^{t+1} \Longrightarrow \Lambda(x^3) = 2^{t+1}$$

In particular, $\min_f \Lambda(f) \le 2^{t+1}$ with equality when m is odd.

Power Functions

When m is odd the minimal value of $\Lambda(f)$ is known and reached by the power function x^3. The main question is what are the power functions x^s such that

$$\lambda(x^s) = \lambda(x^3) = 2^{t+1}.$$

▷ We know that s is coprime to $q - 1$. Moreover the x^s must be almost perfect nonlinear.

The minimal value of $\Lambda(f)$ when m is even is still open even in the case of power functions.

–*Welch'conjecture*:

$$\Lambda(x^s) \geq \Lambda(x^3) = 2^{t+1}$$

m **even: open questions.**

▷ $m = 2t$. Questions on the admissible spectrums appears in the in the works by : Gold, Golomb, Welch, Niho, Solomon (196x). The power functions with spectrum composed of the three values

$$-2^{t+1}, 0, +2^{t+1}$$

correspond to the **preferred pairs** of m-sequences.

–*Calderbank-McGuire, 1994* : If m is a multiple of 4 then the spectrum of f is not of the above type.

ex-conjecture of Sarwate-Pursley (1980)

–*Helleseth'conjecture, 1976* : If m is a power of 2 the Fourier spectrum of a power function contains more than three values

–*Calderbank, McGuire, Poonen, Rubinstein, 1996* : True if the spectrum is symmetric about -1.

odd m only

▷ We assume m odd, say $m = 2t + 1$.

An integer s is a **good exponent** if and only if $R(x^s) = 2^{t+1}$ this implies $(s, q-1) = 1$.

The set of good exponents in invariant under the **shift** $s \mapsto 2s$ and the **inversion** $s \mapsto s^{-1}$.

If s is a good exponent then the mapping $x \mapsto x^s$ is APN but the converse is false !

A function f such that all the Fourier coefficients of $\hat{f}(a)$ have a dyadic valuation greater or equal to v is called **v-divisible**.

–*lemma*: The exponent s is good if and only if x^s is APN and $(t+1)$-divisible.

Known good exponents

type	s	condition	proof	date
Gold	$2^k + 1$	$(k, m) = 1$	easy	1968
Kasami	$2^{2k} - 2^k + 1$	$(k, m) = 1$	Kasami.	1971
Welch	$2^t + 3$		DCC(†)	1999
Niho	$2^t + 2^{(m-1)/4} - 1$	$m \equiv 1\,(4)$	DHX(‡)	2000
Niho	$2^t + 2^{(3m-1)/4} - 1$	$m \equiv 3\,(4)$		

Table 1: Good exponents, $m = 2t + 1$.

† Canteaut, Charpin, Dobbertin.

‡ Dobbertin, Hollmann, Xiang.

Main Question

type	s	condition	proof	date
Gold	$2^k + 1$	$(k, m) = 1$	easy	1968
Kasami	$2^{2k} - 2^k + 1$	$(k, m) = 1$	Kasami.	1971
Welch	$2^t + 3$		DCC(†)	1999
Niho	$2^t + 2^{(m-1)/4} - 1$	$m \equiv 1\,(4)$	DHX(‡)	2000
Niho	$2^t + 2^{(3m-1)/4} - 1$	$m \equiv 3\,(4)$		

–*Dobbertin's conjecture*: If s is a good exponent then s is equivalent to an integer of Gold, Kasami, Welch or Niho type.

Gauss sums

- The Gauss sum at χ is $G_L(\chi) = \sum_{x \in L^\times} \chi(x)\mu(x)$.

$$\mu(z) = \frac{1}{q-1} \sum_{\chi} G(\chi)\bar{\chi}(z) \qquad \text{(Fourier inversion)}$$

The Fourier coefficient of x^s by **mean of Gauss sums**†:

$$\begin{aligned}\widehat{f_\chi}(a) &= \sum_{x \in L} \mu_L(x^s + ax) \\ &= \frac{q}{q-1} + \frac{1}{q-1} \sum_{1 \neq \chi \in \widehat{L^\times}} G_L(\chi^{1/s}) G_L(\bar{\chi}) \chi(a)\end{aligned}$$

- where $1/s$ is an inversion modulo $q-1$.

†: is that really useful ?

Congruence of Stickelberger

- ξ is the principal $(q-1)$-root in $\mathbf{C}$
- $\wp$ a prime above 2 in $\mathbf{Z}[\xi]$
- $L = \mathbf{Z}[\xi]/\wp$

$$\omega \colon class(\xi) \mapsto \bar{\xi} \qquad \textbf{Teichmüller character}$$

–*Stickelberger*: Let j be a positive integer, $0 \leq j \leq q-2$. Then

$$-G_L(\omega^j, \mu_L) = (-2)^{S(j)} \pmod{\wp^{S(j)+1}},$$

where $S(j)$ is the sum of the **bits** of j.

- $j = j_0 + j_1 2^1 + \ldots j_r 2^r \Longrightarrow S(j) = j_0 + j_1 + \ldots + j_r$, here $(0 \leq j_i \leq 1)$.

W-Divisibility

$$\widehat{f_\chi}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{1 \neq \chi \in \widehat{L^\times}} G_L(\chi^{1/s}) G_L(\bar{\chi}) \chi(a)$$

$$= \frac{q}{q-1} + \frac{1}{q-1} \sum_{j=1}^{q-2} G_L(\omega^{j/s}) G_L(\bar{\omega}^j) \omega^j(a)$$

J where the valuation is minimal, say W.

$$\equiv \sum_{j \in J} G_L(\omega^{j/s}) G_L(\bar{\omega}^j) \omega^j(a) \mod \wp^{W+1}$$

$$\equiv 2^W \sum_{j \in J} \omega^j(a) \mod \wp^{W+1}$$

Fundamental map

Stickelberger suggests the introduction of a mapping V with domain $[0, q-2]$ defined by

$$V : j \mapsto S(j/s) + S(-j)$$

$$W = \min_{1 \leq j \leq q-2} V(j), \quad J = \{j \mid V(j) = W\}, \quad P(X) = \sum_{j \in J} X^j.$$

–*Claim* : The power function x^s is exactly W-divisible. Moreover,

$$\widehat{f}(a) \equiv 0 \mod 2^{W+1} \Leftrightarrow P(\bar{a}) = 0.$$

▷ where $a \mapsto \bar{a} = \chi(a^s) \mod \wp$.

Numerical Example $m = 7$

d	type	inv	2	3	4	5	6	7	J
1		1						126	all
3	Gold. 1 Kasa.1	43			7	14	28	28	1
5	Gold 2	27			7	21	28	14	1
7		55		7		14	35	14	1
9	Gold 3	15			7	28	21	14	1
11	Dobb	13			7	28	7	42	9
13	Kasa. 2 Niho	11			7	28	7	42	5
15		9			7	28	21	14	7
19		47		7		21	28	14	1
21		31		7	7	14	21	28	1
23	Kasami 3	29			21		28	28	1 3 13

The Results

Since $S(2j) = S(j)$ the polynomial $P(X)$ is an idempotent whence the Fourier coefficient $\widehat{f}(a)$ has a dyadic valuation equal to W if and only if $\sum_{j \in J} \bar{\omega}^{jd}(a) \equiv 1 \pmod{\wp}$ that is $P(\bar{a}) = 1$.

–*THM*: The integer s is a good exponent if and only if $W = t + 1$ and $P(X)$ has 2^{m-1} roots in L.

▷ Let $x(a)$ be the integer such that $\widehat{f}_d(a) = x(a)2^{\frac{m+1}{2}}$.

$$\sum_{a \in L} x(a)^2 = 2^{m-1}$$

since half of the $x(a)$'s are odd, we deduce they are equal to ± 1 and the other are 0.

–*COR*: Let s be an integer of weight t. If the polynomial $\sum_{j \in J} X^j$ is a permutation polynomial of L then s is a good exponent.

Single Cyclotomic Case

The corollary gives a strategy to eventually find new good exponent s looking for among the s whose the set J is a single cyclotomic class.

–*Lemma*: If $J = \{1, 2, \dots\}$ then $\mathrm{Tr}_L\big((x+1)^s + x^s\big) = 1$.

▷ Use Poisson's formula...

–*Lemma*: The J-set of an exponent of Gold type is equal to the cyclotomic class of 1.

–*Lemma*: If $\mathrm{Tr}_L\big((x+1)^s + x^s\big)$ then the weight of s is even.

–*Conjec.*: If $\mathrm{Tr}_L\big((x+1)^s + x^s\big) = 1$ then s has binary weight 2.

Numerical Experience

For a given m, we propose to find all the integer s satisfying the conditions

(a) s is not of Gold type;

(b) $W = \frac{m+1}{2}$;

(c) J= single cyclotomic class.

We have run a program for $9 \leq m \leq 29$, m odd.

and after 21 days...

Numerical Results

m	(s, j)
9	–
11	(43,293,K)
13	(171,1189,K)
15	—
17	(683,21141,K)
19	(2731, 84629, K)
21	—
23	(10923, 1387093, K)
25	(43691, 5548629, K)
27	—
29	(174763, 89303381,K)

The End.