On Dobbertin's conjecture

Gregor Leander, Philippe Langevin

SAGA07, Papeete, May 2007.

Fourier coefficient

- m positive integer
- L the finite field order $q := 2^m$
- Tr_L the absolute trace of L
- μ_L the canonical character of L

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

The *Fourier coefficient* of $f \in L[X]$, at $a \in L$ is

$$\widehat{f}(a) = \sum_{x \in L} \mu_L(f(x) + ax)$$

Definitions

- The *spectrum* of f

$$\mathrm{spec}\,(f) = \{\widehat{f}(a) \mid a \in L\}$$

- The *valuation*

$$\mathrm{val}\,(f) = \nu, \qquad \forall a \in L, \quad 2^{\nu} \mid \widehat{f}(a)$$

  but there exists a such $\widehat{f}(a)$ is not divisible by $2^{1+\nu}$

Power Function

It corresponds to the monomial case where

$$f(x) = x^d$$

In this talk, we assume that d is invertible modulo $q - 1$.
It is easy to prove that

$$\mathrm{spec}\,(d) = \mathrm{spec}\,(2d) \quad \text{and} \quad \mathrm{spec}\,(d) = \mathrm{spec}\,(d^{-1})$$

The exponents d and d' are equivalent :

$$\exists k, \quad d' = 2^k d, \quad \text{or} \quad d' = 2^k d^{-1}$$

AB-exponent

Let $f(x) = x^d$, applying the Sidelnikov's bound

$$\sup_{a \in L} |\widehat{f}(a)| \geq \sqrt{2q}$$

By definition, an almost bent exponent satisfies

$$\sup_{a \in L} |\widehat{f}(a)| = \sqrt{2q}$$

In that case, m is odd, and the spectrum is three-valued:

$$-2^{\frac{m+1}{2}}, \quad 0, \quad +2^{\frac{m+1}{2}}$$

In particular, the valuation of AB-exponents is $\frac{m+1}{2}$

From now and on, we assume that m is odd.

In connection to the Voloch's talk :

$$d \text{ is AB} \iff d \text{ is APN and } \mathrm{val}\,(d) = \frac{m+1}{2}$$

Gold and Kasami exponents

Let $k > 0$ be an integer,

$$d = 2^k + 1 \quad \text{(Gold)} \qquad d = 2^{2k} - 2^k + 1 \quad \text{(Kasami)}$$

$$\operatorname{spec}(d) = \{-2^{\frac{m+r}{2}}, \quad 0, \quad +2^{\frac{m+r}{2}}\}$$

where $r = (k, m)$.

- There are $\varphi(m)/2$ classes of AB-exponents of Gold type.
- There are $\varphi(m)/2$ classes of AB-exponents of Kasami type.
- Remark that
$$2^4 - 2^2 + 1 = 2^2 + 1$$
for $m > 9$, this is the only class which is both Gold and Kasami.

Welch and Niho exponents

On a basis of numerical experiments ($m \leq 17$), Niho conjectured (1972) that the following exponents are almost bent :

$$d = 2^{\frac{m-1}{2}} + 3 \quad \text{(Welch)}$$

and

$$d = 2^{2r} + 2^r - 1. \quad \text{(Niho)}$$

where $4r \equiv -1 \pmod{m}$.

- This conjecture of Niho has been proved recently by Dobbertin, Canteaut, Charpin, Xiang, and Hollmann (2000).

Dobbertin conjecture

type	s	condition	nb. classes
Gold	$2^r + 1$	$(r, m) = 1)$	$\frac{1}{2}\varphi(m)$
Kasami	$2^{2r} - 2^r + 1$	$(r, m) = 1)$	$\frac{1}{2}\varphi(m)$
Welch	$2^{(m-1)/2} + 3$		1
Niho	$2^{2r} + 2^r - 1$	$4r \equiv -1 \mod m$	1

Table: Known AB-exponents m odd.

Up to equivalence, if $m > 9$ then the number of AB-exponents is equal to $\varphi(m) + 1$.

Kasami-Welch exponent

Using quadratic form theory, one can easely prove that the Fourier coefficients of the exponent

$$d = \frac{2^{tk}+1}{2^k+1} \quad \text{(Kasami-Welch)}$$

takes values in

$$0, \quad \pm 2^{\frac{m+e}{2}}, \quad \pm 2^{\frac{m+3e}{2}}, \quad \pm 2^{\frac{m+5e}{2}}, \quad \ldots$$

where $e = (m, k)$.

- The case $t = 3$ corresponds to the Kasami exponent. In this case the spectrum is actually 3-valued.
- In the case $t = 5$, Niho proved the spectrum is at most 5-valued. In fact the spectrum is 5-valued (Kasami). A simpler proof was given by Bracken (2004), generalizing a proof of the $t = 3$ case by Dobbertin (1999).

Niho conjecture

On the basis of numerical experiences, Niho (page 72) proposes the following conjectures on Kasami-Welch exponents :

conjecture	cond.	m		spectrum
conj. 4-2	$e > 1$		3-valued	$0, \pm 2^{\frac{m+e}{2}}$
conj. 4-3	$e = 1$	not prime	5-valued	
conj. 4-4	$e = 1$	prime	5-valued	$0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}$

A counter-example

Take $m = 25,\ k = 3,\ t = 19$!!!

Fourier Coeff.	multiplicity
$+2^{15}$	1025
$+2^{14}$	337225
$+2^{13}$	7031500
0	18815956
-2^{13}	7031500
-2^{14}	337225
-2^{15}	1

This is a consequence of a joint work with McGuire and Leander.

Checking conjectures

- In december 2006, we computed the spectrum of all power functions, up to the dimension 25 and we did not find any counter-example to the main conjectures about power functions.

  http://langevin.univ-tln.fr/project/spectrum

- Hans Dobbertin knew its conjecture true up to dimension 27, and he was curious to know the status of his claim for higher dimension.

The purpose of this talk is to check Dobbertin's conjecture up to the dimension 33.

Link with Gauss sum

For all $x \in L^\times$,

$$\mu_L(x) = \frac{1}{q-1} \sum_{\chi \in \widehat{L^\times}} G_L(\chi)\bar{\chi}(x)$$

where

$$G_L(\chi) = \sum_{x \in L^\times} \chi(x)\mu(x)$$

is a Gauss sum.
The Fourier coefficients of the power function $f(x) = x^d$.

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

Congruences of Stickelberger

By mean of a Teichmüller character ω:

$$\widehat{f}(a) \equiv -\sum_{j=1}^{q-2} G_L(\omega^j) G_L(\bar{\omega}^{dj}) \omega^{dj}(a) \mod q$$

By Stickelberger, for any positive integer j

$$G_L(\bar{\omega}^j, \mu_L) \equiv 2^{\mathrm{wt}\,(j)} \mod 2^{\mathrm{wt}\,(j)+1}$$

where $\mathrm{wt}\,(j)$ is the sum of the bits of the residue j. We get

$$\mathrm{val}\,(d) \geq \nu_d = \min_{1 \leq j \leq q-2} \mathrm{wt}\,(-j) + \mathrm{wt}\,(jd)$$

We introduce the J-set of d

$$J = \{j \mid \mathrm{wt}\,(-j) + \mathrm{wt}\,(jd) = \nu_d\},$$

Valuation of an exponent

Collecting the terms of valuation ν_d, we obtain the congruence

$$\widehat{f}(a) \equiv 2^{\nu_d} \sum_{j \in J} \omega^{jd}(a) \pmod{2^{\nu_d+1}}$$

since d is invertible, all the ω^{jd}'s are distincts, thus:

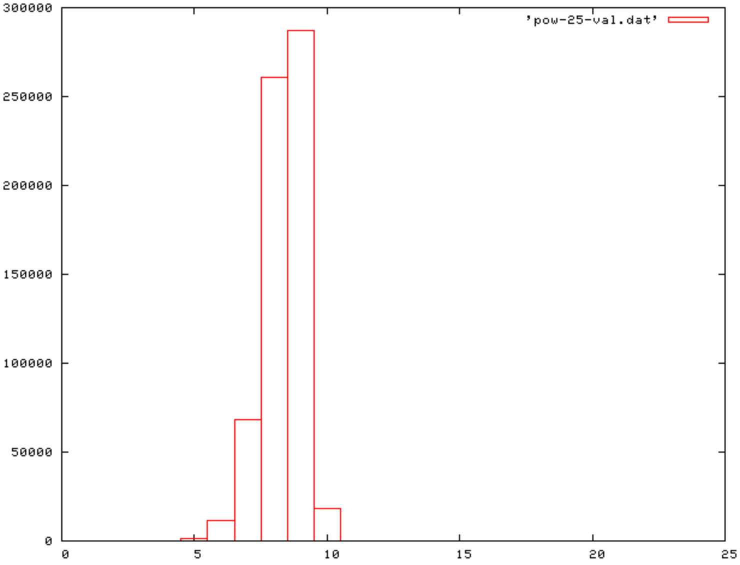
$$\mathrm{val}\,(d) = \nu_d = \min_{1 \leq j \leq q-1} \mathrm{wt}\,(j) + \mathrm{wt}\,(-jd)$$

For example,

Proposition

An exponent d is AB iff $\nu = \frac{m+1}{2}$ and $a \mapsto \sum_{j \in J} a^{dj}$ is balanced.

Valuation distribution



Exponent with high valuation

	ν	nb. of s
	2	1
	3	12
	4	155
	5	1549
	6	11396
	7	68348
	8	260754
	9	287221
	10	18228
	11	249
	12	8
valuation of AB-exponent	**13**	79
	15	3
	25	1

Good exponents

Our strategy to check Dobbertin's conjecture consists in enumerating the *good exponents* i.e.

$$\mathrm{val}\,(d) \geq \frac{m+1}{2}$$

- It is a small set containing the AB-exponents
- We compute the Fourier spectrums of good exponents to check which are AB.
- The running time to compute a Fourier transform in dimension 25 is approximatively 6 secondes.

Key idea for sieving

An exponent of the form

$$d = \frac{-r}{s}, \qquad \mathrm{wt}\,(r) + \mathrm{wt}\,(s) \leq \frac{m-1}{2},$$

is **not** almost bent.

Proof.

For a such d, we have

$$\mathrm{wt}\,(s) + \mathrm{wt}\,(-sd) = \mathrm{wt}\,(s) + \mathrm{wt}\,(r) < \frac{m+1}{2}.$$

Thus,

$$\mathrm{val}\,(d) = \nu_d < \frac{m+1}{2}$$

$\square$

Sieving Algorithm

Generate all the pairs (r, s) with

$$\mathrm{wt}\,(s) \leq \mathrm{wt}\,(r), \quad \mathrm{wt}\,(s) + \mathrm{wt}\,(r) \leq \frac{m-1}{2}.$$

and mark $d = \frac{-r}{s}$ as a bad exponent.

- All exponents which are not marked have valuation greater then $\frac{m-1}{2}$.
- All exponents which are not marked are good candidates for AB-exponents. It is a small size.
- The work factor of sieving is about $2^{1.2m}$.

Number of candidates

There where only a very few exponents with valuation greater or equal $(m+1)/2$ that are not Gold, Kasami, Niho, Welch :

- 69 for dimension 27.
- 80 for dimension 29.
- 93 for dimension 31.
- 141 for dimension 33.

Now, the compute of the spectra of these exponents is feasible. Note that, for $m = 33$, we use the transitivity of the AB-property.

Numerical results

This is what we get after approximately one week of computation:

- Dobbertin's conjecture is correct up to $n \leq 33$.
- Nearly all the invertible d of valuation greater or equal to $\frac{m+1}{2}$ are Kasami-Welch exponents.
- Up to dimension 33 all the exponents of valuation

$$(m+1)/2$$

are Niho, Welch, Gold or Kasami-Welch except three exceptions.

Exceptions of valuation $\frac{m+1}{2}$

m	d	bits	equiv
27	8065	000000000000001111110000001	8321 / 3
	12287	000000000000010111111111111	12289
	10324441	000100111011000100111011001	13/3
29	24575	00000000000000101111111111111	24577
	32513	00000000000000111111100000001	33025 / 3
	41298235	00010011101100010100100111011	13 / 3
31	32513	0000000000000000111111100000001	33025 / 3
	49151	0000000000000001011111111111111	49153
	82595525	0000100111011000100111011000101	13 / 3
33	98303	000000000000000010111111111111111	98305
	130561	000000000000000011111111000000001	131585 / 3
	660764203	000100111011000100111011000101011	13 / 3

Conjecture

Outside Gold, Niho, Welch, Kasami-Welch, there are exactely three exponents of valuation $\frac{m+1}{2}$ with valuation $(m+1)/2$:

$$2^{\frac{m-1}{2}} + 2^{\frac{m-3}{2}} + 1, \qquad \frac{13}{3}$$

and according to the congruence of m modulo 4 :

$$\frac{2^{\frac{m-1}{2}} + 2^{\frac{m+1}{4}} + 1}{3}$$

or

$$\frac{2^{\frac{m+1}{2}} + 2^{\frac{m-1}{4}} + 1}{3}$$

Moreover, all have a 5-valued spectrum :

$$\{0, \pm 2^{(m+1)/2}, \pm 2^{(m+3)/2}\}$$

Conjecture

The Kasami-Welch exponent

$$d = \frac{2^{tk}+1}{2^k+1}$$

is almost bent iff

$$t = 3 \quad \text{and} \quad (k, m) = 1$$

$$\widehat{f}(a) = \sum_{x \in L} \mu_L(x^d + ax) = \sum_{x \in L} \mu_L(x^{2^{tk}+1} + ax^{2^k+1})$$

Modular add-carry algorithm

Let j be a residue modulo $q-1$.

$$j = (j_{m-1} \dots j_1 j_0) \quad dj = (s_{m-1} \dots s_1 s_0)$$

Evans, Hollmann, Krattenthaler and Xiang introduced the *modular add-carry algorithm* to analyze the weight of dj. There are *carries* $0 \leq c_i < \mathrm{wt}\,(d)$ such that:

$$\forall i, \quad 2c_i + s_i = \sum_{k \in \mathrm{supp}\,(d)} j_{i-k} + c_{i-1}$$

Adding these m equalities:

$$\sum_i c_i + \mathrm{wt}\,(dj) = \mathrm{wt}\,(d)\mathrm{wt}\,(j)$$

whence

$$\mathrm{wt}\,(jd) + wt(-j) = (\mathrm{wt}\,(d) - 1)\mathrm{wt}\,(j) - \sum_i c_i + m$$

Graph of the multiplication d

Assume that $d = 2^L + \ldots + 2^0$.

$$2c_{i-1} + s_{i-1} = j_{i-1} + \ldots + j_{i-1-L} + c_{i-2}$$
$$2c_i + s_i = j_i + \ldots + j_{i-L} + c_{i-1}$$
$$2c_{i+1} + s_{i+1} = j_{i-1} + \ldots + j_{i+1-L} + c_i$$

$$(j_{i-1}, \ldots, j_{i-1-L}, c_{i-2}) \to (j_i, \ldots, j_{i-L}, c_{i-1}) \to (j_{i+1}, \ldots, j_{i+1-L}, c_i)$$

The sequences of carries of dj correspond to cycle of lentgh m in the graph of order $2^{L+1}\mathrm{wt}\,(d)$

$$(j_L, \ldots, j_0, c) \longrightarrow (*, j_L \ldots, j_1, c')$$

where

$$c' = (c + \sum_{k \in \mathrm{supp}\,(d)} j_{L-k})/2$$

J-set and cycles

We define the cost of the vertex

$$x = (j_L, \ldots, j_0, c)$$

$$K(x) = (\mathrm{wt}\,(d) - 1)j_L - c$$

and the cost of cycle of length n

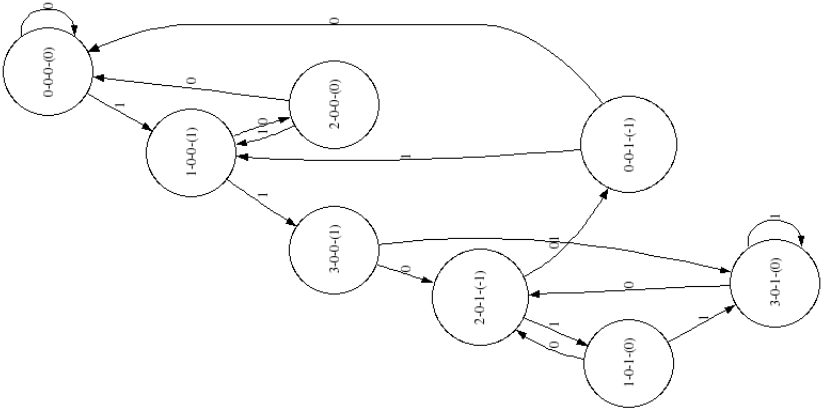
$$x_1 \longrightarrow x_2 \longrightarrow \ldots \longrightarrow x_n \longrightarrow x_1$$

as

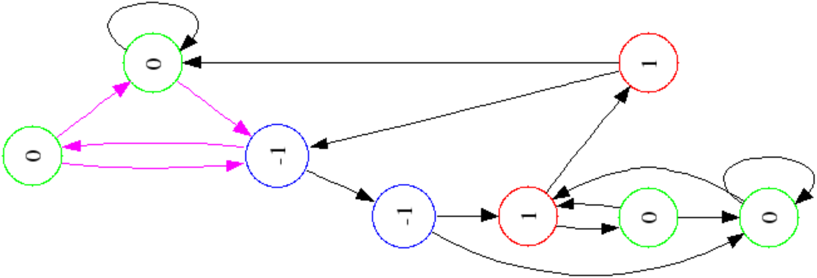
$$\sum_{i=1}^{n} K(x_i)$$

The cycles of length m minimizing the cost function correspond to the elements of the J-set.

Example $d = 3$

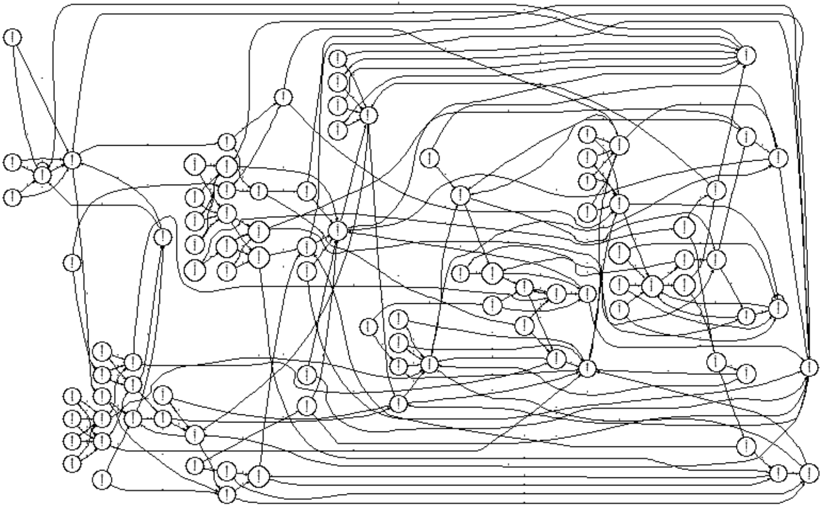


Cost function, $d = 3$

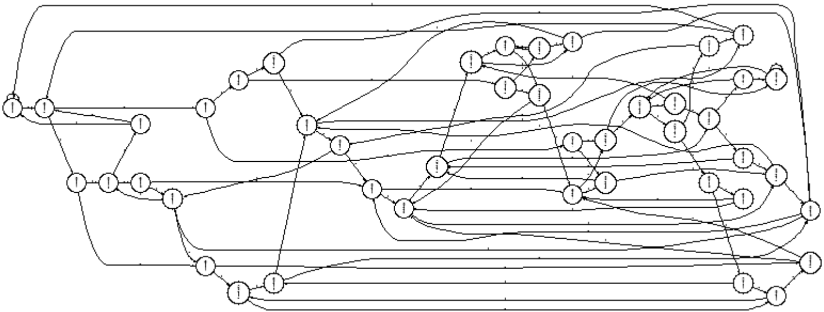


The cost of an elementary cycle is of length $2L$ or $2L + 1$ is greater than $-L$: the valuation is greater or equal to $\lfloor \frac{m+1}{2} \rfloor$. The two cycles of type $(2, -1)$ and $(3, -1)$ shows this is the exact value.

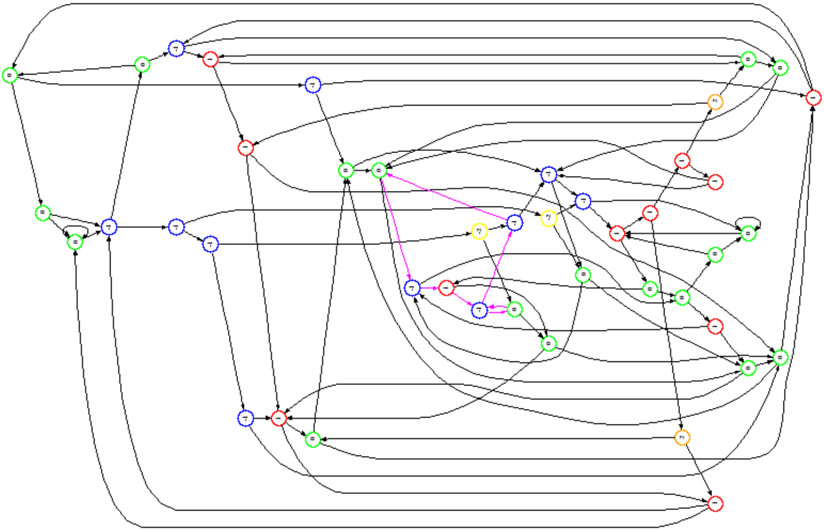
Graph, $d = 13/3$



The graph after simplification



Cost function, $d = 13/3$



Cycles analysis

- The cost of *elementary cycles* of length $2L$ or $2L+1$ are greater or equal to $-L$ (computer checking).

$$\mathrm{val}\,(\frac{13}{3}) \geq \frac{m+1}{2}$$

- There exists a cycle of type $(2,-1)$ connected to cycle of type $(5,-2)$:

$$\mathrm{val}\,(\frac{13}{3}) = \frac{m+1}{2}$$

Indeed, if $m = 5 + 2L$ then one can loop L times in the cycle of type $(2,-1)$ and one time over the cycle of type $(5,-2)$ for a total cost of $\frac{m-1}{2}$

end of the talk.

Sarwate-Pursley

Conjecture I. Let m be even. If s is coprime to $q-1$ then

$$R(s) \geq \sqrt{4q}$$

Helleseth conjecture

If s is coprime to $q-1$, the Fourier coefficient of x^s at 0 is equal to zero. The Helleseth conjecture claims the existence of an outphase Fourier coefficient equal to zero.

Conjecture II. If s is coprime to $q-1$ then

$$\exists a \in L - \{0\}, \quad \widehat{f_s}(a) = 0.$$

Dobbertin conjecture

type	s	condition	number
Gold	$2^r + 1$	$(r, m) = 1)$	$\varphi(m)/2$
Kasami	$2^{2r} - 2^r + 1$	$(r, m) = 1)$	$\varphi(m)/2$
Welch	$2^{(m-1)/2} + 3$		1
Niho	$2^{2r} + 2^r - 1$	$4r \equiv -1 \mod m$	1

Table: Known almost bent exponents, m odd.

The Dobbertin conjecture claims the above list is complete.

Conjecture III. In odd dimension, up to equivalence, the number of good exponents is equal to

$$\varphi(m) + 1.$$

(smaller if $m \leq 9$).

Leander conjecture

Let $\mathrm{nbz}\,(s)$ the number of $a \in L$ such that $\widehat{f}(a) = 0$.

Conjecture IV.
If $1 < d < q - 1$ is coprime to $q - 1$ then

$$\mathrm{nbz}\,(-1) \leq \mathrm{nbz}\,(d)$$

Of course, this conjecture implies Helleseth (1) since

$$\mathrm{nbz}\,(-1) = 1 + H(-1 + 4q) > 0$$

where $H(d)$ is the class number of $\mathrm{Q}(\sqrt{d})$, see e.g. Lachaud-Wolfmann, 1990.

Langevin-Véron conjecture (1)

Let us denote by $L(s)$ the smallest non zero Fourier coefficient of the power function x^s in absolute value.

Conjecture V.

If $1 < s < q-1$ is coprime to $q-1$ then the spectrum of x^s contains the two value walues

$$-L(s), \quad \text{and}, \quad -L(s)$$

- Non-linearity of power functions
  DCC, 2005.

false!

Langevin-Véron conjecture (2)

Conjecture VI.

If s is coprime to $2^m - 1$ then $L(s)$ is a power of two.

false!

Helleseth (1976)

Conjecture VII.

If m is a power of 2 and s coprime to $2^m - 1$ then

$$\sharp\mathrm{spec}\,(s) \neq 3$$

- Proved in the symmetric case by Calderbank, McGuire, Poonen and Rubinstein (1996)
- Langevin-Véron conjecture implies this conjecture.

Michko conjecture

Conjecture VIII.

If m is odd and coprime to $2^m - 1$ then

$$\sharp\mathrm{spec}\,(s) \neq 4$$

If $m \geq 5$ is odd

$$\sharp\mathrm{spec}\,(s) \neq 6$$

Remark that if $m = 5$ then

$$\mathrm{spec}\,(15) = 5[-8], 5[-4], 6[0], 10[4], 5[8], 1[12],$$