Checking the main conjectures related to the Walsh-Fourier Spectrum of Power functions

Gregor Leander, Philippe Langevin

BFCA07, Paris, May 2007.

Plan

correlation of binary sequences

A binary sequence takes values ± 1. The *crosscorrelation* at $t = 0, 1, \ldots$ of a pair s' and s of binary sequences of length n is defined by

$$s' \times s(t) = \sum_{i=0}^{n-1} s'_i s_{i+t}$$

The intercorrelation parameter $\theta(s', s)$ is the maximum of

$$\sup_{t \neq 0} |s \times s(t)|, \quad \sup_{t} |s' \times s(t)|, \quad \sup_{t \neq 0} |s' \times s'(t)|$$

A good pair for applications in communication and radar, when $\theta(s', s)$ is small. By a bound of Sidelnikov (1971)

$$\sqrt{\frac{n}{2}} \leq \theta(s', s).$$

Optimal binary pair

Given a length n,

- What is the minimal value of $\theta(s', s)$?

A few years ago, I contacted some specialists for this problem :Turyn, Golomb... It seems there is no work on this subject outside the field of m-sequences !

- Note that for a pair of sequences such that

$$t \neq 0 \Longrightarrow s' \times s(t) = s \times s(t) = -1$$

a bound of Cahn and Stalder (1964) gives

$$\theta(s', s) \geq \sqrt{n} > \sqrt{\frac{n}{2}}$$

m-sequences

Let L be finite field of order $q = 2^m$ and let μ_L be its canonical additive character

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

where $\mathrm{Tr}_L(x) = x + x^2 + \cdots + x^{2^{m-1}}$. An *m-sequence* is a binary sequence of period $n = q - 1$ having the form

$$s_i = \mu_L(\gamma^i), \quad i = 0, 1, \ldots, q - 1.$$

where γ is a primitive root of L. By the orthogonality relations of characters,

$$t \neq 0 \Longrightarrow s \times s(t) = -1$$

But applying Sidelnikov's bound to m-sequences gives :

$$\theta(s', s) \geq 1 + \sqrt{2q} > \sqrt{n} > \sqrt{\frac{n}{2}}$$

Decimation

Let γ' be an other primitive root of L. There exits an integer d such that

$$\gamma' = \gamma^d$$

and the m-sequence s' defined by γ' is a d-decimation of s

$$s'_i = s_{di}$$

The correlation spectra can be nice but are never optimal for the Cahn-Stalder bound. There exists pairs of m-sequences such that

$$\sup_t |s' \times s(t)| = 1 + \sqrt{2q}, \quad (m \text{ odd})$$

optimal for m-sequences by Sidelnikov's bound.

$$\sup_t |s' \times s(t)| = 1 + \sqrt{4q}, \quad (m \text{ even})$$

may be not optimal.

Preferred pair of m-sequences

The cross-correlation spectra corresponding to these nice pairs of *m*-sequences:

- *m* odd,

$$-1-\sqrt{2q}, \quad -1, \quad -1+\sqrt{2q} \tag{1}$$

- $m = 0 \mod 4$

$$-1-\sqrt{q}, \quad -1, \quad -1+\sqrt{q}, \quad -1+2\sqrt{q} \tag{2}$$

- $m = 2 \mod 4$

$$-1-2\sqrt{q}, \quad -1, \quad -1+2\sqrt{q} \tag{3}$$

The pairs of m-sequences with a three valued spectrum (1) or (3) are often called *preferred pairs* of *m*-sequences.

Fourier coefficient

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

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

Note that $\widehat{f}(a)$ is a Walsh coefficient of the Boolean function

$$x \mapsto \mathrm{Tr}_L(f(x)).$$

Let us consider the pair

$$s'_i = \mu_L(f(\gamma^i)), \quad \text{and} \quad s_i = \mu_L(\gamma^i)$$

The crosscorrelation at t and the Fourier coefficient at γ^t are connected by

$$1 + s' \times s(t) = \widehat{f}(\gamma^t)$$

Notation and terminology

- The *spectrum* of f

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

- The *spectral amplitude*

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

- The *number of zeroes* of f

$$\mathrm{nbz}\,(f) = \sharp\{a \mid \widehat{f}(a) = 0\}$$

- 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 $f(x) = bx^d$. In this talk, we assume that the exponent d is invertible modulo $q-1$.

$$\sum_{x\in L} \mu_L(bx^d + ax) = \sum_{x\in L} \mu_L(bc^d x^d + acx) = \sum_{x\in L} \mu_L(x^d + acx)$$

So we may assume $b = 1$. In that case, 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 :

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

The number of distincts spectrums with d invertible is (roughly) less or equal to the number $\frac{2^{m-1}}{m}$

Gold exponent

$$d = 2^k + 1$$

In that case $x \mapsto \mathrm{Tr}_L(x^d)$ is a quadratic form, its radical has dimension of $r = (2k, m)$. It folllows a three valued spectrum :

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

An exponent d is called a almost bent if its spectrum takes the three values:

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

The distribution of the Fourier coefficients of an AB-exponent are given by the Parseval identity $\sum_{a \in L} \widehat{f}(a)^2 = 2^{2m}$

$$2^{m-1} \quad [0], \qquad 2^{m-2} \pm 2^{\frac{m-3}{2}} \quad [\pm 2^{\frac{m+1}{2}}]$$

Kasami exponent

$$d = 2^{2k} - 2^k + 1$$

It is again a three valued spectrum :

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

The proof is not so simple. In the case $(2k, m) = 1$, one can use the trick of Dobbertin

$$2^{2k} - 2^k + 1 = \frac{2^{3k} + 1}{2^k + 1}$$

It follows

$$\widehat{f}(a) = \sum_{x \in L} \mu_L(f(x) + ax) = \sum_{x \in L} \mu_L(x^{2^{3k}+1} + ax^{2^k+1})$$

The dimension of the radical of the quadratic form $x \mapsto \mathrm{Tr}_L(x^{2^{3k}+1} + ax^{2^k+1})$ is less or equal to 3. Moreover, if it is 3 the quadratic form Q_a is defective, and

$$\widehat{f}(a) = 0.$$

Niho conjecture on 3-valued exponents

In 1972, on the basis of numerical experiments ($m \leq 17$), Niho conjectures the exponents (1) ,(2), (3) are almost bent.

label	exponents	condition	exponent
(1)	$2^{\frac{m-1}{2}} + 3$	m odd	Welch
(2)	$2^{\frac{m-1}{2}} + 2^{\frac{m-1}{4}} - 1$	$m \equiv 1 \pmod 4$	Niho
(3)	$2^{\frac{m-1}{2}} + 2^{\frac{3m-1}{4}} - 1$	$m \equiv 3 \pmod 4$	Niho
(4)	$2^{\frac{m+2}{2}} + 3$	$m \equiv 2 \pmod 4$	?
(5)	$2^{\frac{m}{2}} + 2^{\frac{m+2}{4}} + 1$	$m \equiv 2 \pmod 4$	?

It is not possible to sketch the proof in a few lines! But all of these conjectures have been proven in recent papers by Cusick, Dobbertin, Canteaut, Charpin, Xiang, Hollmann (2000).

Kasami-Welch exponent

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

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

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 $t = 5$ and $\frac{m}{e}$ odd, 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.

Sketch of proof 1/3

The basic idea (McGuire) to disprove conjecture 4-4 consists in finding intances of $d = (2^{tk}+1)/(2^k+1)$ such that the Fourier coefficient at one is greater than $2^{\frac{m+3}{2}}$.

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

The radical of the quadratic form $Q(x) = \mathrm{Tr}_L(x^{2^{tk}+1} + x^{2^k+1})$ is the set of solutions of the equation :

$$x^{2^{tk}} + x^{2^{-tk}} + x^{2^k} + x^{2^{-k}} = 0$$

denoting by n the dimension of the radical of Q

$$\widehat{f}(1) = \begin{cases} \pm 2^{\frac{m+n}{2}}, & Q \text{ not defective;} \\ 0, & Q \text{ defective.} \end{cases}$$

Sketch of proof 2/3

By the theory of Linearized Polynomials, the dimension of the radical, is equal to number of $x \in L$ solutions of the system

$$x^{tk} + x^{-tk} + x^k + x^{-k} = 0, \quad x^m + 1 = 0$$

Remark that

$$(x^r + x^{-r})(x^s + x^{-s}) = x^{r+s} + x^{r-s} + x^{s-r} + x^{-r-s}$$

We factorize the radical equation with $tk = r + s$ and $k = r - s$ i.e.

$$r = \frac{(t+1)k}{2}, \quad s = \frac{(t-1)k}{2}.$$

$$(x^r + x^{-r})(x^s + x^{-s}) = 0, \quad x^m + 1 = 0$$

Now, if $(s, m) = 1$ and $r|m$ then the radical is the subfield of degree r, and the quadratic form is not defective, whence

$$\widehat{f}(1) = 2^{\frac{m+r}{2}}.$$

Sketch of proof 3/3

It suffices now to go the market to find k, t and m such that

$$\frac{(t+1)k}{2} = r|m, \quad \text{and} \quad \frac{(t-1)k}{2} = s \quad (s,m) = 1$$

The smallest solutions are obtained with $m = 25$, $k = 3$, and $t = 19$:

$$r = \frac{(t+1)k}{2} = 30 \equiv 5 \mod 25$$
$$s = \frac{(t-1)k}{2} = 25 \equiv 2 \mod 25$$

Numerical Projects

In fact, all the Niho conjectures concerning Kasami-Welch exponents are false, the first counter-examples are in dimension 21 and 23. Since a lot of conjectures concerning power function are based on the numerical experiences done by Niho :

$$m \leq 17 \quad (1972)$$

It is necessary to update the numerical computations. We have four precise projects:

determination of	condition	up to	status
spectrums		$m \leq 25$	done
AB-exponents	odd	$m \leq 33$	done
bent exponents	even	$m \leq 30$	run
APN-exponent	even	$m \leq ??$	no idea!

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.

Langevin-Véron conjecture (2)

Conjecture VI.

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

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

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

Forgotten conjectures ?

All the propositions are welcome !

Fourier algorithm

Considering the true table of a Boolean function f :

$$f(0\dots00)f(0\dots01)f(00\dots10)f(0\dots11)\dots f(1\dots11)$$

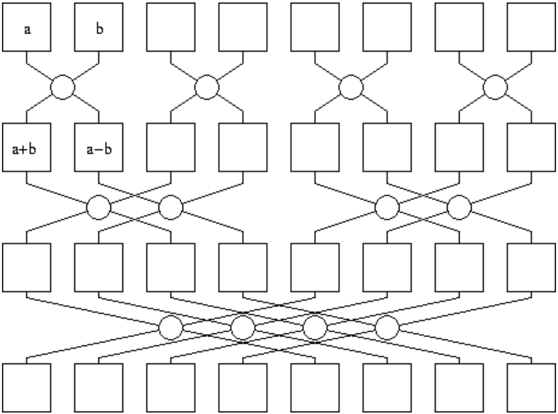
The Walsh-Fourier coefficient of f is computed in $m2^m$ steps by the very short recursive code. It is based on the relation

$$\widehat{f}(b,a) = \widehat{f_0}(a) + (-1)^b \widehat{f_1}(a)$$

where $b \in \mathbb{F}_2$, $a \in \mathbb{F}_2^{m-1}$ and

$$f_0(x) = f(0,x), \quad \text{and} \quad f_1(x) = f(1,x)$$

Fourier algorithm



Running time

m	P4 3Gz	IT-64	Xeon 2Gz	P4 2.4Gz	1980	1972
	6003	2071	3932	690.17	bogomips	
15	0.00s	0.00s	0.00	0.00		
16	0.00s	0.00s				
17	0.01s	0.01s				
18	0.03s	0.03s				
19	0.07s	0.05s				
20	0.15s	0.13s	0.21	0.18		
21	0.32s	0.27s				
22	0.68s	0.57s				
23	1.50s	1.23s				
24	3.24s	2.65s				
25	6.92s	6.52s	10.96	8.9	6 days	$\frac{1}{2}$ year

Fourier algorithm has complexity $m2^m$. The recursive version is faster than the iterative version.

Running time

The work factor to compute, up to equivalence, the spectrums of the x^s, s invertible in dimension 25 looks like :

$$\frac{1}{50} \times \varphi(2^{25} - 1) \times 6.92 = 4484160 \,\mathrm{sec} = 52 \,\mathrm{days}$$

The running time for all invertible power functions in dimension 25 is estimated to 52 days, but there is an extra time of 150 days for the datas managements ! We used network tools (bigloop) to deals computations over 54 processors.

All the results are avaible :

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

Baby file

d=1	127 [0], 1 [128]
d=3	64 [0], 28 [-16], 36 [16]
d=5	64 [0], 28 [-16], 36 [16]
d=7	36 [0], 1 [-40], 14 [-16], 28 [-8], 28 [8], 14 [16], 7 [24]
d=9	64 [0], 28 [-16], 36 [16]
d=11	64 [0], 28 [-16], 36 [16]
d=19	36 [0], 1 [-40], 28 [-8], 14 [-16], 14 [16], 28 [8], 7 [24]
d=21	36 [0], 1 [-40], 14 [-16], 28 [-8], 28 [8], 7 [24], 14 [16]
d=23	64 [0], 28 [-16], 36 [16]
d=63	15 [0], 8 [-12], 7 [-20], 7 [-16], 21 [-8], 7 [-4], 14 [16], 21 [4], 14

Table: All the spectrum, up to equivalence, for $m = 7$ reported in the data file `spec-7.txt`

Example in dimension 8

d=1	255 [0], 1 [256]
d=3	28 [-32], 192 [0], 36 [32]
d=5	6 [-64], 240 [0], 10 [64]
d=7	16 [-32], 52 [-16], 105 [0], 68 [16], 14 [32], 1 [64]
d=9	28 [-32], 192 [0], 36 [32]
d=11	1 [-64], 8 [-32], 64 [-16], 101 [0], 68 [16], 10 [32], 4 [48]
d=13	18 [-32], 48 [-16], 101 [0], 84 [16], 4 [48], 1 [64]
15	120 [-16], 136 [16]
d=17	255 [0], 1 [256]
d=19	88 [-16], 88 [0], 64 [16], 8 [32], 8 [48]
d=21	4 [-32], 96 [-16], 48 [0], 96 [16], 12 [32]
d=23	88 [-16], 90 [0], 56 [16], 20 [32], 2 [64]
d=25	1 [-64], 80 [-16], 90 [0], 80 [16], 5 [64]
d=27	1 [-32], 72 [-16], 108 [0], 72 [16], 3 [96]
d=31	80 [-16], 120 [0], 16 [16], 40 [32]
d=39	28 [-32], 192 [0], 36 [32]
d=43	8 [-32], 60 [-16], 109 [0], 76 [16], 1 [64], 2 [96]

Checking conjectures...

We computed the spectrum of all power functions, up to $m = 25$, the conjectures still hold:

- Sarwate conjecture
- Helleseth conjecture
- Dobbertin conjecture
- Leander conjecture
- Michko conjecture

Conjecture V is false

Recall this conjectures claims that the minimal value in the spectrum appears with two signs. We found exactely 6 counter examples, 3 are in dimension 21 and 3 others in dimension 24.

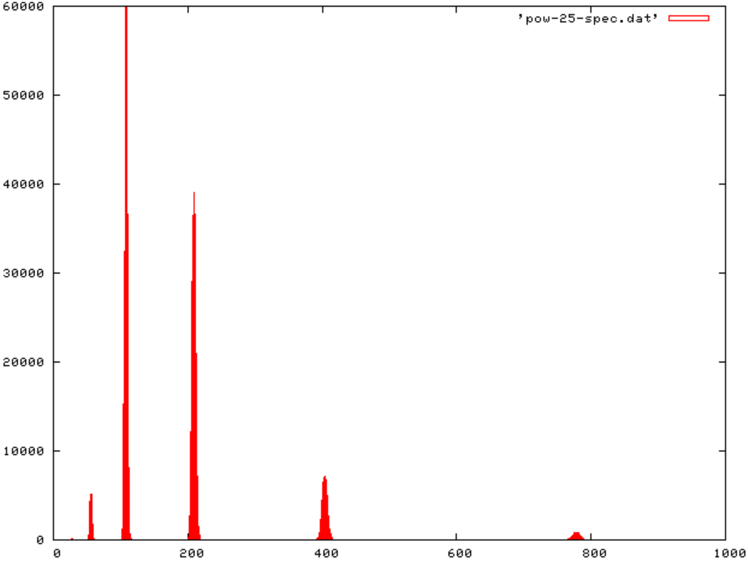
- $d = 149797$: 5712 [-3968], 38745 [-3072], 12754 [-2688], 116298 [-2176], 78666 [-1792], 13314 [-1408], 195678 [-1280], 195888 [-896], 63756 [-512], 194649 [-384], **7119 [-128]**, 258854 [0], **128982 [384]**, 117579 [512], 29631 [768], 195530 [896], 2569 [1152], 130977 [1280], 38346 [1408], 43722 [1664], 76881 [1792], 6804 [2048], 65352 [2176], 5880 [2304], 462 [2432], 28434 [2560], 13104 [2688], 7056 [2944], 13125 [3072], 966 [3328], 7140 [3456], 63 [3712], 2534 [3840], 504 [4224], 63 [4608], 7 [4992], 1 [298880], 3 [299264], 3 [300160],

Conjecture VI is false

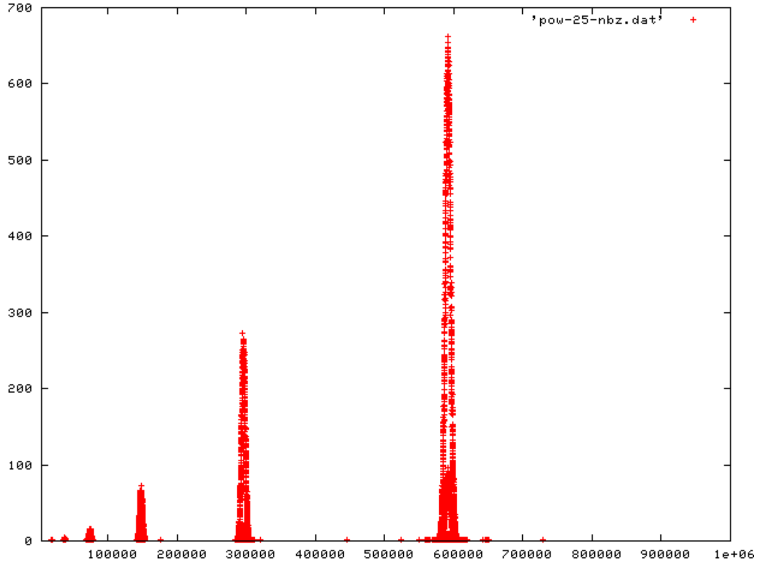
Recall this conjectures claims that the minimal value is a power of 2. We found exactely 3 in dimension 21 :

- $s = 1198373$: 44100 [-6656], 312420 [-5888], 932802 [-5120], 1561332 [-4352], 1559748 [-3584], 933828 [-2816], 104700 [-2304], 312888 [-2048], 625578 [-1536], 44124 [-1280], 1559172 [-**768**], 2077957 [0], 1562208 [**768**], 623634 [1536], 103644 [2048], 103760 [2304], 519528 [2816], 1039038 [3584], 1039452 [4352], 518514 [5120], 104916 [5888], 57432 [6400], 231504 [7168], 345036 [7936], 232080 [8704], 56844 [9472], 18886 [10752], 58524 [11520], 57492 [12288], 19452 [13056], 3720 [15104], 8328 [15872], 3744 [16640], 360 [19456], 456 [20224], 8 [23808], 1 [2391040], 3 [2394112], 3 [2401280],

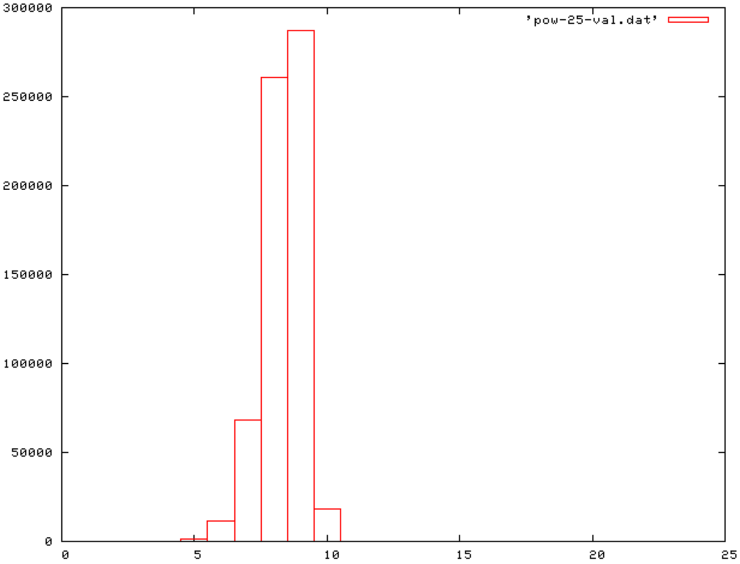
Size spectrum distribution



Number of zeroes distribution



Valuation distribution



Exponent of 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

J-set

Using Stickelberger's conruences on Gauss one can prove that the valuation of d is :

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

with equality when $(d, 2^m - 1) = 1$. One can, of course, use McEliece theorem to get this result but... McEliece theorem depend on Stickelberger's congruences also !

- The J-set of d :

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

$$\hat{f}(a) \equiv 2^\nu \sum_{j\in J} a^{dj} \pmod{2^{\nu+1}}$$

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

Sieving good candidates

We remark that all the exponents of the form

$$d = \frac{-r}{s}$$

where $\mathrm{wt}(r) + \mathrm{wt}(s) \leq \frac{n-1}{2}$ are not AB-exponents.

Proof.

For such a d, we have

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

Therefore it exists a such that

$$\widehat{F}(a) \neq \pm 2^{(m+1)/2}$$

□

Sieving good candidates

Generate all the pair (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 the exponents which are not marked have valuation less or equal to $\frac{m-1}{2}$.
- Aan exponent which is not marked as bad is good candidates to be AB-exponents.
- The work factor for sieving is about $2^{1.2m}$.
- The set of candidates has a very small size.

Checking Dobbertin farther

We detemine all the *good candidates* up to the dimension 33.

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

All these exponents are Kasami-Welch exponents except a few exceptions : Niho and Welch exponent, but also, for each odd m, 3 new exponents of valution $\frac{m+1}{2}$ with a 5-valued spectrum.

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

m	d	bits	spec size
19	481	0000000000111100001	5
	767	0000000001011111111	5
	20165	0000100111011000101	5
21	1535	000000000010111111111	5
	1985	000000000011111000001	5
	161323	000100111011000101011	5
23	1985	00000000000011111000001	5
	3071	00000000000101111111111	5
	645307	00010011101100010111011	5
25	6143	0000000000001011111111111	5
	8065	0000000000001111110000001	5
	2581111	0001001110110001001110111	5

Exceptions in another form

m	d	equiv.	numerator
19	481	545 / 3	9 5 0
	767	769	9 8 0
	20165	13 / 3	3 2 0
21	1535	1537	10 9 0
	1985	2113 / 3	11 6 0
	161323	13 / 3	3 2 0
23	1985	2113 / 3	11 6 0
	3071	3073	11 10 0
	645307	13 / 3	3 2 0

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

m	d	bits	spec size
27	8065	0000000000000001111110000001	5
	12287	0000000000000010111111111111	5
	10324441	0001001110110001001110110001	5
29	24575	000000000000000101111111111111	5
	32513	000000000000000111111100000001	5
	41298235	000100111011000101001001110111	5
31	32513	00000000000000000111111100000001	5
	49151	00000000000000001011111111111111	5
	82595525	00000100111011000100111011000101	5
33	98303	0000000000000000010111111111111111	?
	130561	0000000000000000011111111000000001	?
	660764203	0001001110110001001110110001010111	?
	925070009	0001101110010001101110010101111001	?
	1265184173	0010010110110100100101101101011101	?

Exceptions in another form

m	d	equiv.	numerator
27	8065	8321 / 3	13 7 0
	12287	12289	13 12 0
	10324441	13 / 3	3 2 0
29	24575	24577	14 13 0
	32513	33025 / 3	15 8 0
	41298235	13 / 3	3 2 0
31	32513	33025 / 3	15 8 0
	49151	49153	15 14 0
	82595525	13 / 3	3 2 0
33	98303	98305	16 15 0
	130561	131585 / 3	17 9 0
	660764203	13 / 3	3 2 0

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 introduce the modular add-carry algorithm to analyze the weight of dj. There exist *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

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

J-set and cycles in graph

Assume that

$$d = 2^L + \ldots + 2^0$$

We consider the graph of order $2^{L+1}\mathrm{wt}\,(d)$ vertices and edges:

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

where

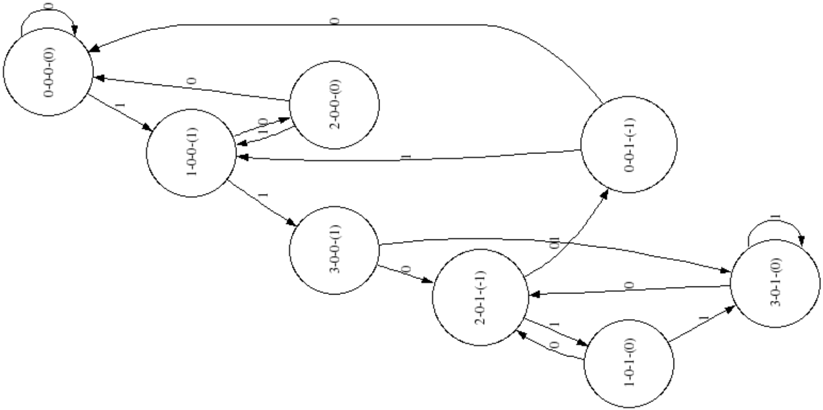
$$c' = (c + \sum_{k \in \mathrm{supp}\,(d)} j_{L-k})/2$$

We define the cost of the vertex (j, c)

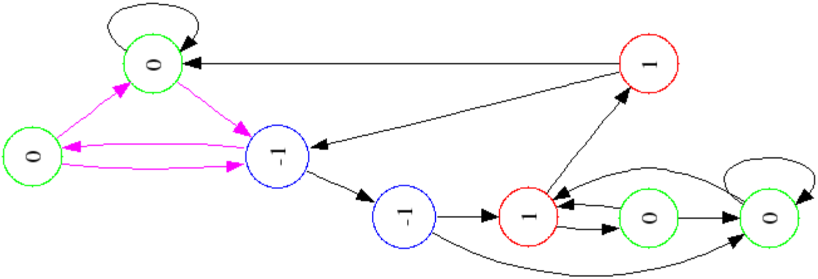
$$K(j, c) = (\mathrm{wt}\,(d) - 1)j_L - c$$

The cycles of length m minimizing the cost function correspond to the elements of the Jset.

Example $d = 3$

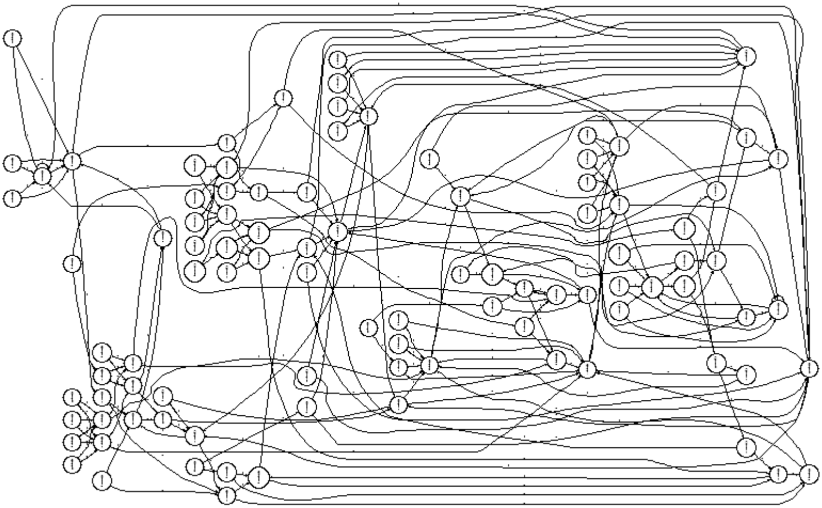


Cost $d = 3$

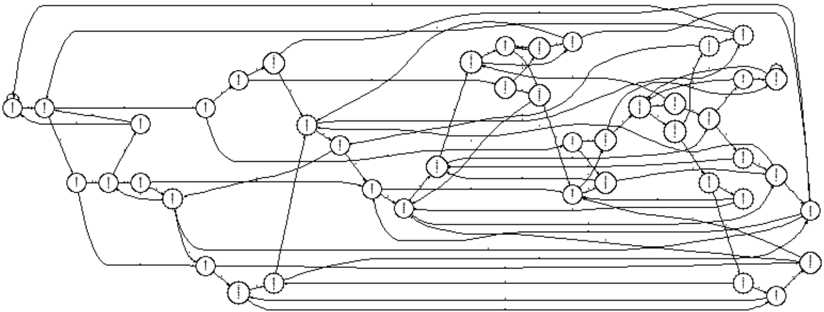


The cost of an elementary cycle is of length $2L$ or $2L + 1$ is greater than $-L$: the valuation is greater or equal to $\lfloor \frac{m+1}{2} \rfloor$. The two cycles of type $(2, -1)$ and $(3, -1)$ shows this is the exact value.

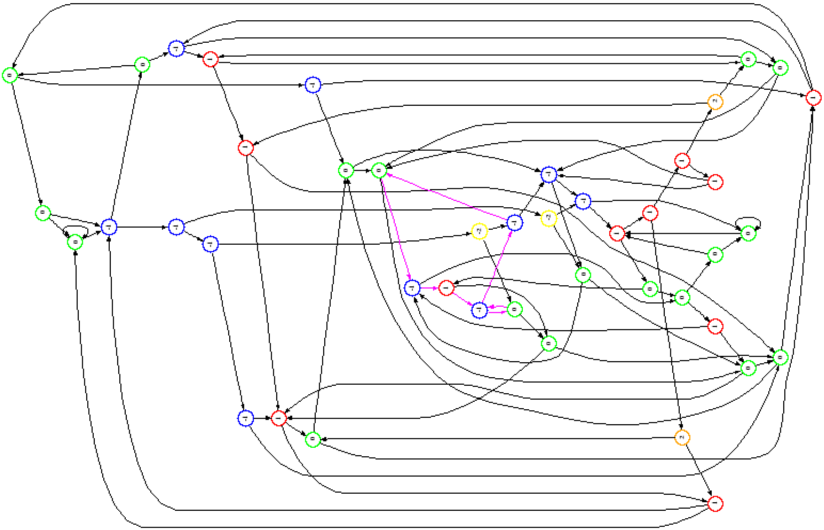
Graph for 13/3



The graph after simplifictaion



Costs for 13/3



Cycles analysis

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

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

- 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 $\frac{m-1}{2}$

Conclusion

- All the main conjecture are checked up to 25
- Dobbertin conjecture up to 33
- New nice exponents :

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

  And according to the congruence of m modulo 4 :

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

  or

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

- By mean of not usual tools, we determined the valuation of the nice exponent 13/3.