Conjectures related to the Fourier Spectrum of Power functions

Gregor Leander, Philippe Langevin

December 2006

Plan

crosscorrelation

The *crosscorrelation* at $t = 0, 1, \ldots$ of two binary sequences s' and s, of length n:

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

For applications in communication, radar, etc. . . Good pairs of sequences have to satisfy

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

By a bound of Sidelnikov (1971)

$$\sqrt{\frac{n}{2}} \leq \sup_{t \neq 0} |s' \times s(t)|$$

If in addition s and s' have autocorrelation equal to -1, a bound of Cahn and Stalder (1964) says

$$\sqrt{n} \leq \sup_{t \neq 0} |s' \times s(t)|$$

m-sequences

The d-decimation of s

$$s_i^{(d)} = s_{di}$$

Let L be finite field of order $q = 2^m$. A *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.
A lot works (Gold, Welch, Niho, Golomb ...) concern the crosscorrelation of m-sequences by decimations. The spectra can be nice but never optimal. There exists d such that

$$\sup_{t \neq 0} |s^{(d)} \times s(t)| = 1 + \sqrt{2q}, \quad (m \text{ odd})$$

$$\sup_{t \neq 0} |s^{(d)} \times s(t)| = 1 + \sqrt{4q}, \quad (m \text{ even})$$

Preferred pair of m-sequences

If m is odd the value

$$\sup_{t \neq 0} |s^{(d)} \times s(t)| = 1 + \sqrt{2q}$$

is optimal, and $s^{(d)} \times s(t)$ takes three values

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

If m is even

$$|s^{(d)} \times s(t)| = 1 + \sqrt{4q}$$

is the best known correlation. The corresponding pairs are called preferred pairs of m-sequences when the spectrum takes the three values

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

this is possible only if $m \neq 0 \mod 4$. Note that when $m = 0 \mod 4$, the four-valued spectrum :

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

is possible.

Fourier coefficient

Let $\mu_L(x) = (-1)^{\mathrm{Tr}_L(x)}$ be the canonical character of L. The *Fourier coefficient* of $f \in L[X]$, at $a \in L$ is

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

The *spectrum* of f

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

and the *spectral amplitude* of f

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

Note that if $s'_i = \mu_L(f(\gamma^i))$ and $s_i = \mu_L(\gamma^i)$ then

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

Power Function $f(x) = bx^d$

The spectrum of f is invariant under the transformation $x \mapsto x^2$ and $x \mapsto cx$ where c generates the cyclic group of index $\Delta = (q-1, d)$.

- The number of distincts spectrums in the non invertible case is less or equal to

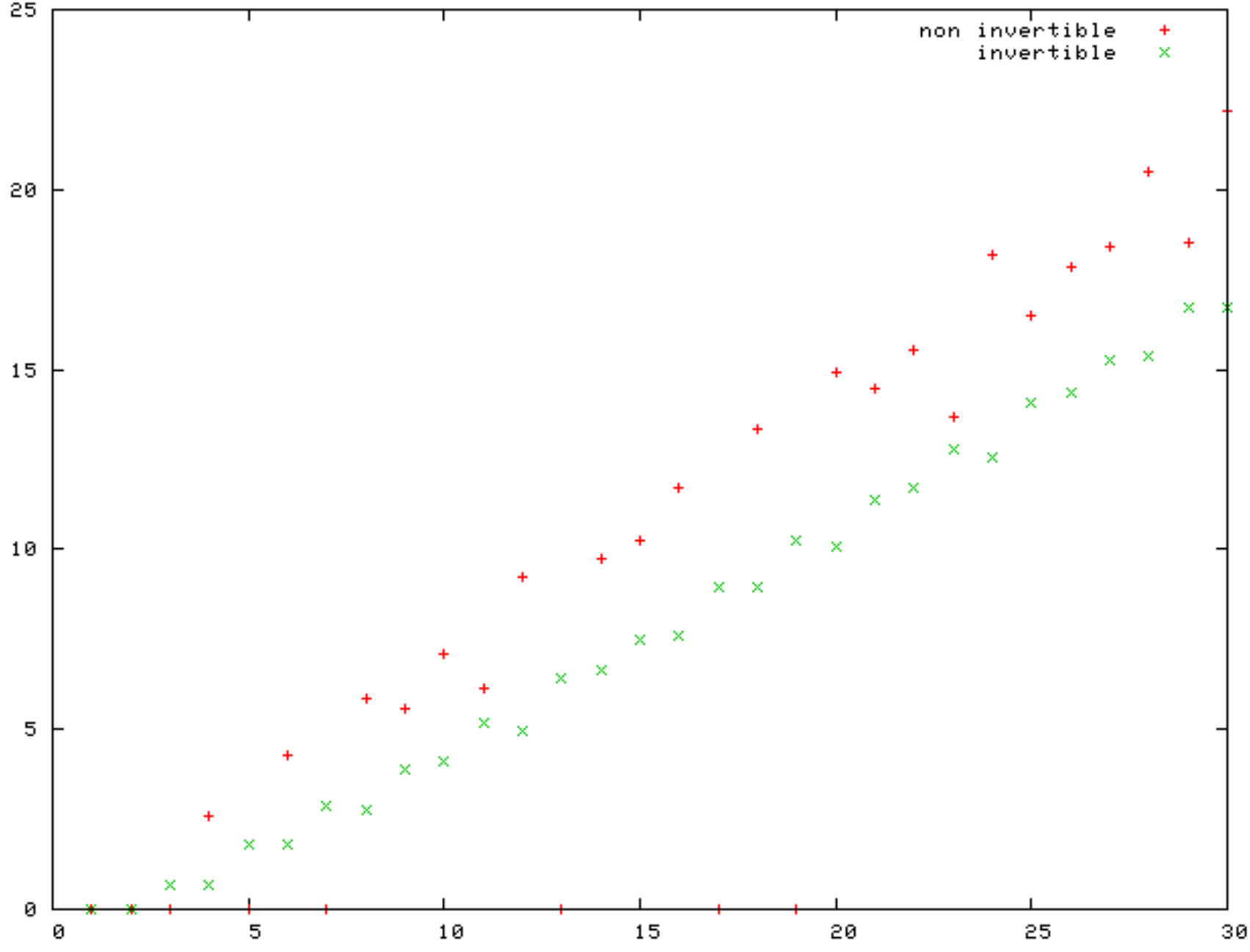
$$\sum_{1<\Delta<q-1} \varphi(\frac{q-1}{\Delta})\mathrm{cl}\,(\Delta)$$

- In the case where d invertible, we may assume $b = 1$ and

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

The number of distincts spectrums with d non invertible is less or equal to

$$\frac{1}{2}\mathrm{cl}\,(q-1)$$


non invertible
invertible
0
5
10
15
20
25
0
5
10
15
20
25
30

Gold exponent - good exponent

$$d = 2^k + 1$$

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

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

In general, an exponent d is called a *good exponent* if its spectrum takes the three values:

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

The multiplicities are given by the Parseval identity

$$\sum_{a \in L} (\hat{f}(a))^2 = q^2$$

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

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

It follows

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

The kernel of the quadratic form
$Q_a(x) = x \mapsto \mathrm{Tr}_(x^{2^{3k}+1} + ax^{2^k+1})$ is the set of x such that

$$x^{2^{3k}} + x^{2^{-3k}} + ax^{2^k} + a^{2^{-k}} x^{2^{-k}}$$

which has dimension less than 3. Moreover, if it is 3 the quadratic form Q_a is not defective whence

Welch exponent - Niho exponent

On a basis of numerical experiments ($m \leq 17$), Niho conjectured (1972) the goodness of the exponent

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

and

$$2^{2r} + 2^r - 1.$$

where $4r \equiv -1 \pmod{m}$.
These conjecture are proved in recent papers (2000) by Dobbertin, Canteaut, Charpin, Xiang, Hollmann.
It is not possible to sketch the proof in a few lines!

Another conjecture of Niho

In his Thesis, Niho conjectured that the spectrum of the power function with exponent

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

takes at most five values when m is odd, and $2^k + 1$ is relatively prime to $q - 1$.

- The case $t = 3$ has been proved by Kasami and Welch. The functions are known as the Kasami (or Kasami-Welch) functions. In this case the spectrum is actually 3-valued.
- In the case $t = 5$ the conjecture has also been proved. It follows from a theorem of Kasami on cyclic codes. A simpler proof was given by Bracken (2004), generalizing a proof of the $t = 3$ case by Dobbertin (1999).

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

Sketch of proof

Let $d = (2^{tk}+1)/(2^k+1)$, where k and t are odd, and suppose that 2^k+1 is relatively prime to $q-1$. The Fourier transform at 1 of $f(x) = Tr(x^d)$ is

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

$x \mapsto x^{2^k+1}$ is a bijection of K

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

The dimension of the kernel

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

is equal to the number of $x \in L$ solutions of the system

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

$$x^m + 1 = 0$$

Sketch of proof

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 kernel equation with $tk = r + s$ and $k = r - s$ i.e.

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

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

Whence if $(s, m) = 1$ and $r|m$ then the kernel is the subfield of degree r, and the quadratic form is not defective.

Numerical Projects

This shows that an update of numerical experiments has to be done !!! Indeed, a lot of conjectures are based on Niho experiments :

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

- All spectrums $m \leq 25$.
- APN exponents m odd, $m \leq 33$
- Bent exponents m even, $m \leq 30$

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

$$\exists a \in L - \{0\}, \quad \hat{f}_s(a) = 0.$$

Dobbertin conjecture

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

Table: Known good 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

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

Leander conjecture

Let $\mathrm{nbz}(s)$ the number of $a \in L$ such that $\hat{f}(a) = 0$.
Conjecture IV. If $1 < s < q - 1$ is coprime to $q - 1$ then

$$\mathrm{nbz}(s) \leq \mathrm{nbz}(-1)$$

Langevin-Véron conjecture

Let us denote by Δ_s the smallest positive Fourier coefficient of the power function x^s.

Conjecture V. If $1 < s < q-1$ is coprime to $q-1$ then there exists a such that

$$\hat{f}(a) = -\Delta_s.$$

Conjecture VI. Δ_s is a power of two.

Fourier algorithm

m	P4 3Gz	IT-64	Xeon 2Gz	P4 2.4Gz	P2 340Mz	1980
	6003	2071	3932	4818	690.17	
15	0.00s	0.00s	0.00	0.00	0.02	
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	6.85	
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	28.38	6 days

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 looks like

$$2^{2m-1}$$

The running time for all invertible power functions in dimension 25 is estimated to 54 days, and 150 days for the data managements. For this reason we used network tools to deals computations over 54 processors.
The result are avaible :
http://langevin.univ-tln.fr/powspec

baby example m=8

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

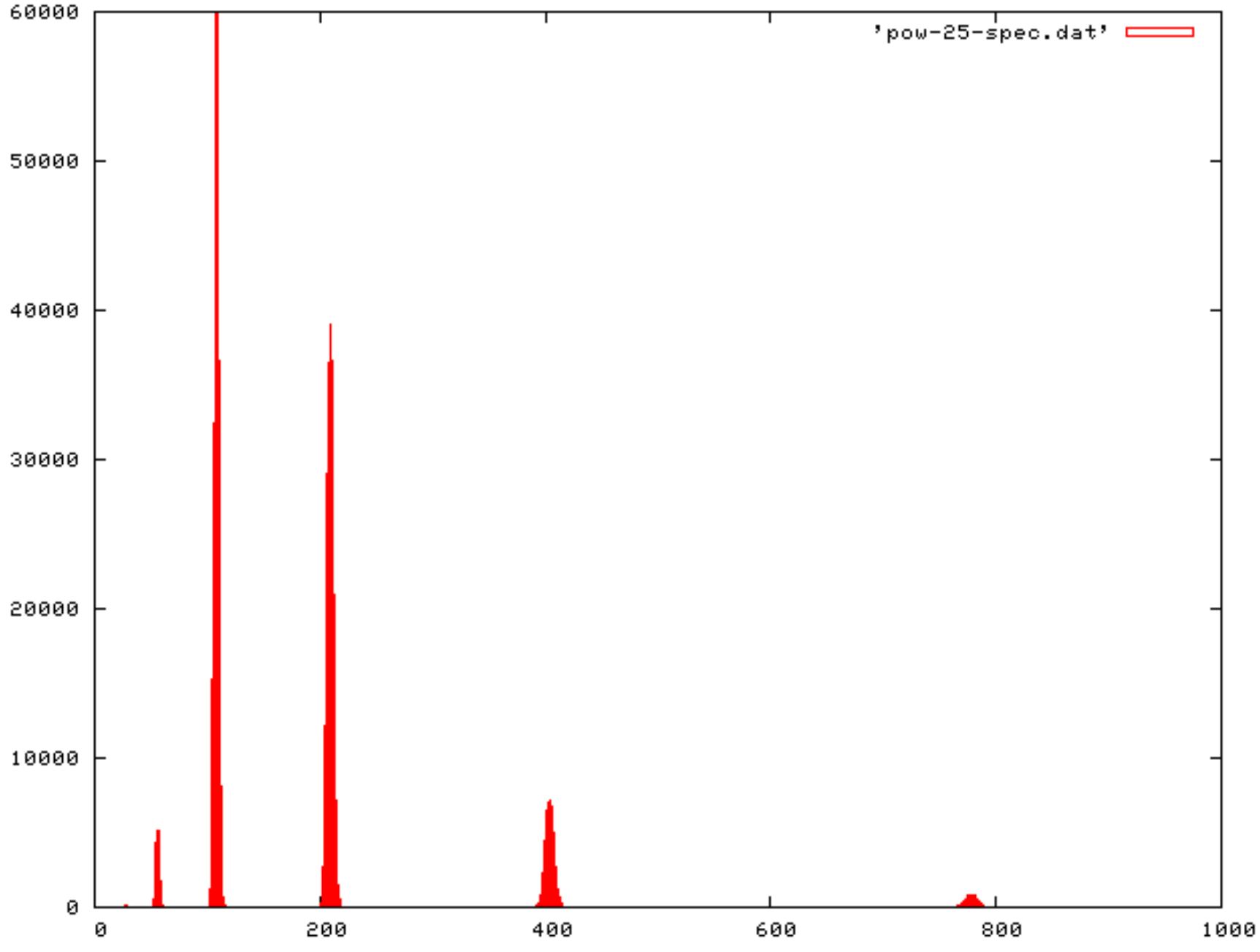
baby example m=8 (cont.)

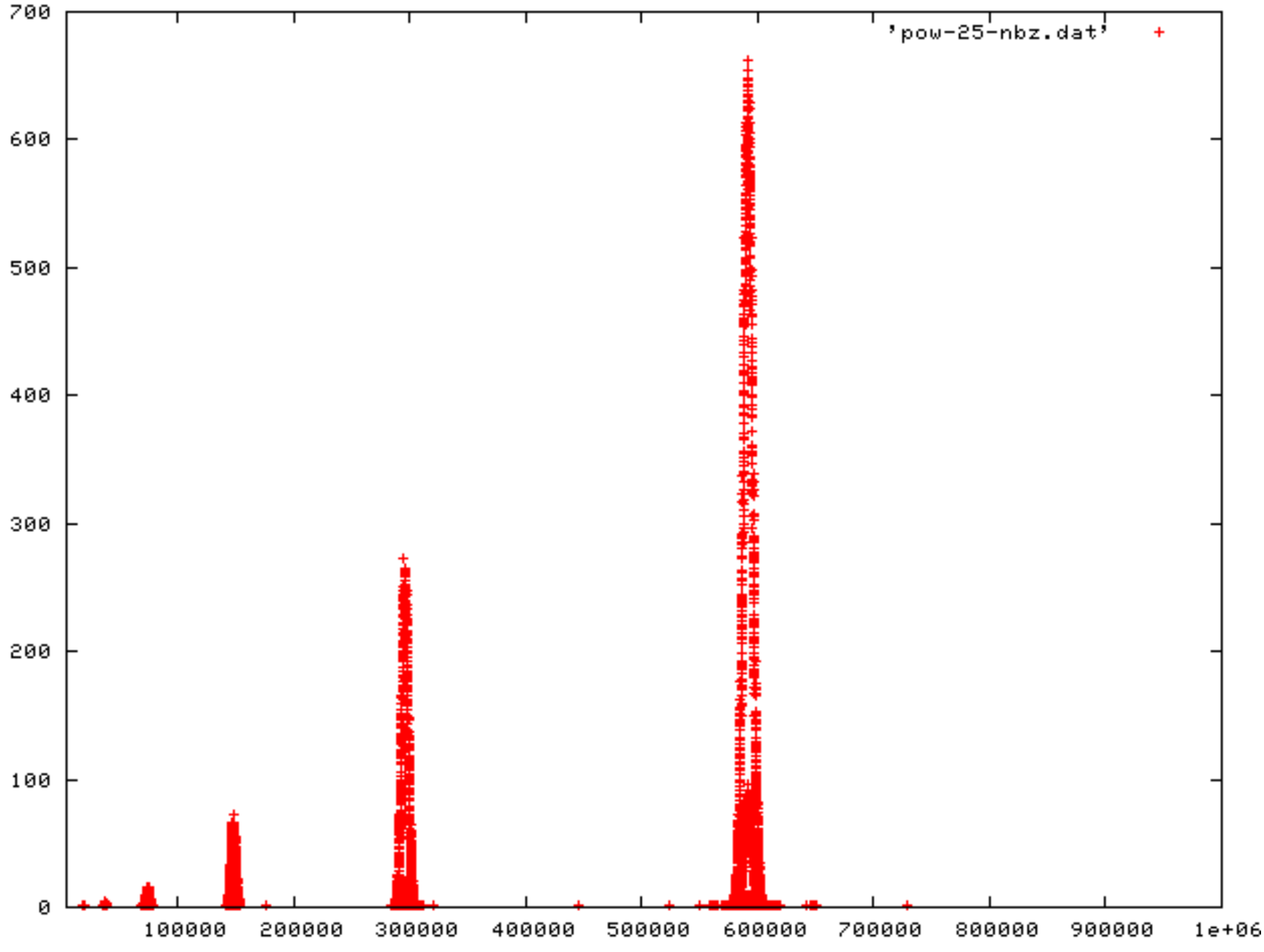
45	120 [-16], 136 [16]
51	255 [0], 1 [256]
53	96 [-16], 60 [0], 96 [16], 4 [64]
55	1 [-64], 80 [-16], 90 [0], 80 [16], 5 [64]
63	1 [-32], 24 [-24], 24 [-16], 72 [-8], 24 [0], 48 [8], 36 [16], 27 [32]
85	255 [0], 1 [256]
87	1 [-32], 72 [-16], 108 [0], 72 [16], 3 [96]
95	1 [-64], 40 [-24], 40 [-8], 85 [0], 40 [8], 40 [24], 10 [32]
111	1 [-32], 24 [-24], 24 [-16], 72 [-8], 24 [0], 48 [8], 36 [16], 27 [32]
119	255 [0], 1 [256]
127	8 [-28], 16 [-24], 8 [-20], 18 [-16], 24 [-12], 16 [-8], 32 [-4],
	17 [0],16 [4], 20 [8], 16 [12], 16 [16], 16 [20], 20 [24], 8 [28], 5 [3

Checking conjectures...

We computed the spectrum of all power functions, up to $m = 25$, are true:

- Sarwate-Pursley conjecture
- Helleseth conjecture
- Dobbertin conjecture
- Leander conjecture
- Langevin-Véron conjecture


'pow-25-spec.dat'
60000
50000
40000
30000
20000
10000
0
0
200
400
600
800
1000


'pow-25-nbz.dat'
700
600
500
400
300
200
100
0
100000
200000
300000
400000
500000
600000
700000
800000
900000
1e+06

Conjecture VI is false

Indeed, we found exactely 3 counter-examples to the conjecture VI, they are in dimension 24.
Note that all the other exponents satisfy the conjecture!

- $s = 1198373$: 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],
- $s = 2396747$: 45060 [-6656], 311232 [-5888], 934020 [-5120], 1560000 [-4352], 1559568 [-3584], 939720 [-2816], 104576 [-2304], 310866 [-2048], 623844 [-1536], 44424 [-1280], 1560024 [-**768**], 2077547 [0], 1556040 [**768**], 620064 [1536], 102840 [2048], 105248 [2304], 520656 [2816], 1042056 [3584],

Checking Dobbertin conjecture

An exponent s is said ν-divisible if

$$\forall a \in L, \quad 2^{\nu} | \hat{f}_s(a),$$

$$\exists a \in L, \quad 2^{\nu} || \hat{f}_s(a).$$

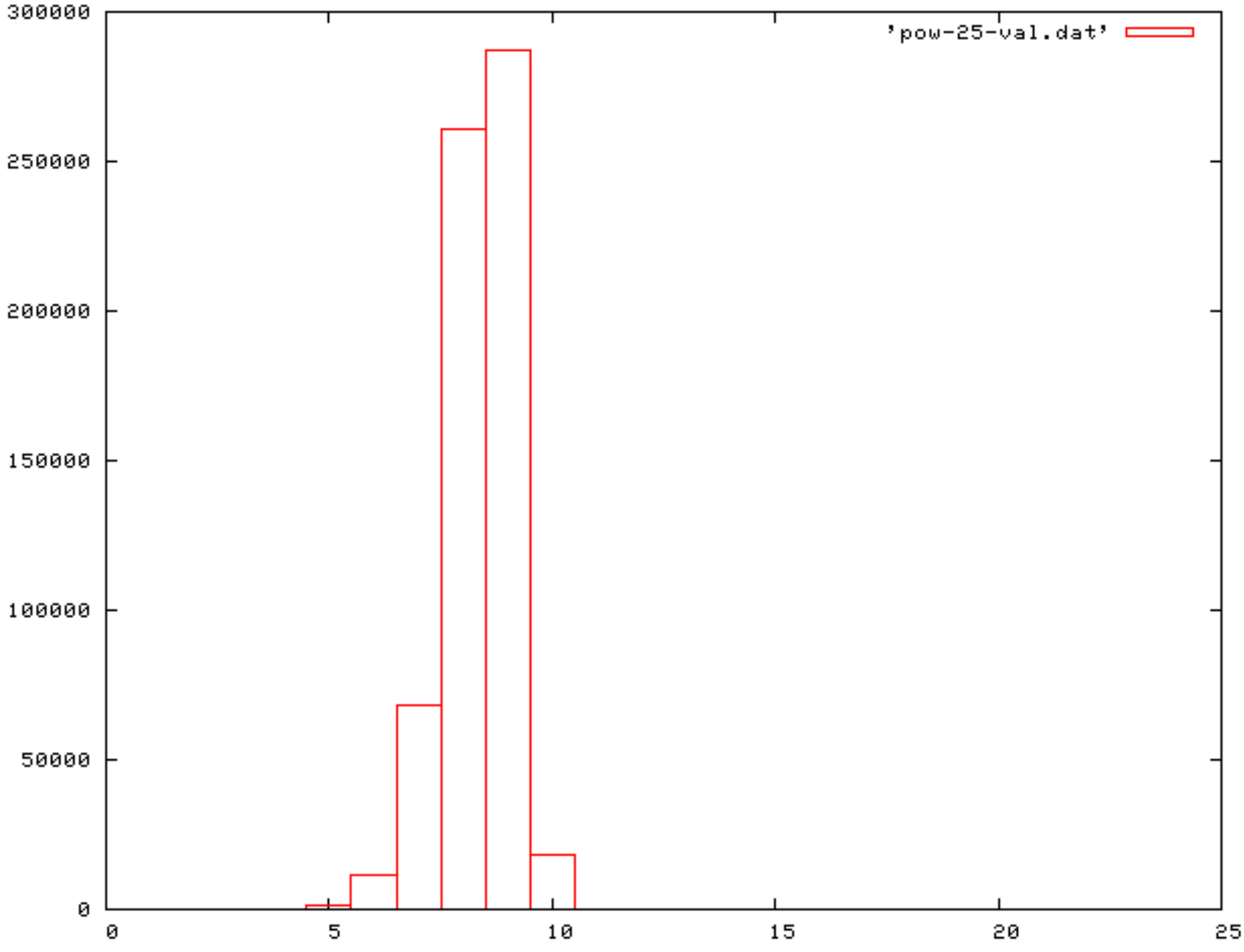
If s is a good exponent then it is $\frac{m+1}{2}$-divisible.

Gauss sums

$$\hat{f}_s(a) = 1 + \frac{1}{q-1} \sum_{\chi \in \widehat{L^\times}} \tau_L(\chi^d)\tau_L(\bar{\chi})\bar{\chi}(a^d)$$

By Stickelberger theorem, the divisibility of s is equal to

$$\min_{0<j<q-1} \mathrm{wt}\,(j) + \mathrm{wt}\,(-js)$$


'pow-25-val.dat'
300000
250000
200000
150000
100000
50000
0
0
5
10
15
20
25

Divisibility

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
13	79
15	3
25	1

Sieving good exponents

If we run over all the pairs (x, y) such that $\mathrm{wt}(x) + \mathrm{wt}(y) \leq \frac{m-1}{2}$ then all the exponents

$$\frac{y}{x}$$

are bad.

All the exponent collected after sieving have the form

$$s = \frac{2^r + 1}{2^s + 1}$$

except a few exceptions.

Exceptions

m	d	bits	spec size
19	529	0000000001000010001	*
	481	0000000000111100001	5
	767	0000000001011111111	5
	20165	0000100111011000101	5
21	1535	0000000000101111111	5
	1985	0000000000111111000001	5
	161323	0001001110110001010111	5
23	2081	0000000000010000100001	*
	1985	0000000000001111111000001	5
	3071	0000000000001011111111111	5
	645307	0001001110110001011011	5
25	6143	0000000000001011111111111	5
	8065	0000000000001111111000001	5
	2581111	0001001110110001001110111	5

Exceptions

m	d	bits	spec size
27	8065	000000000000001111110000001	5
	12287	000000000000010111111111111	5
	10324441	000100111011000100111011001	5
29	24575	000000000000010111111111111	5
	32513	000000000000001111111000000001	5
	41298235	000100111011000101001001110111	5
31	32513	000000000000000011111110000001	5
	49151	000000000000000101111111111111	5
	82595525	000010011101100010011011000101	5
33	98303	000000000000000010111111111111111	?
	130561	000000000000000011111111000000001	?
	660764203	000100111011000100111011000101011	?
	925070009	000110111001000110111001010111001	?
	1265184173	001001011011010010010110110101101	?

Conclusion

Dobbertin conjecture on good exponents is true up to $m \leq 33$. The numerical experimentation suggests the following strategy for a proof :

- Prove the conjecture for the exponent of the form

$$s = \frac{2^r + 1}{2^s + 1}$$

- Determine the form of the exceptions.
- Prove the conjecture for the exceptions.

Conclusion

It is possible to extend the sieving method to determine the J-set of all the exponents. With this information, we can determine all the *bent* exponents i.e. all the pairs (b, s) such that the spectrum of bx^s is

$$\pm 2^{\frac{m}{2}}$$

for $m \leq 28$.