Bent functions, Kloosterman sums and point counting

Jean-Pierre Flori, Sihem Mesnager and Gérard Cohen

ANSSI, University of Paris 8 and Télécom ParisTech

November 4, 2011

Outline

Boolean functions

A Boolean function is a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

Polynomial form

f has a unique trace expansion of the form:

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)} \left(a_j x^j \right) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}} \quad ,$$

where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class modulo $2^n - 1$,$o(j)$ the size of the coset and $\epsilon = \mathrm{wt}(f) \pmod 2$.

Bentness

A Boolean function f is said to be **bent** if it has maximum **non-linearity** $2^{n-1} - 2^{n/2-1}$, i.e. is as far as possible of all affine functions.

Walsh-Hadamard transform

Walsh-Hadamard transform

For $\omega \in \mathbb{F}_{2^n}$, the Walsh-Hadamard transform of f at ω is

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\omega x)} .$$

(Hyper)-bentness can be characterized using the Walsh-Hadamard transform.

- **Bentness:** A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$.
- **Hyper-Bentness:** A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime with $2^n - 1$.

Computing the Walsh-Hadamard transform

The **Walsh-Hadamard transform** can be computed quite easily and efficiently: algorithm in $O(2^m m^2)$ bit operations and $O(2^m m)$ memory, cache efficient, ridiculously small constant [Arn10].

Already implemented in **Sage** [S$^+$11] (using Cython [BCS10]). However there are some drawbacks with the current implementation:

1. returns the opposite of the transform;
2. limited to 32 bits;
3. returns a Python array.

Some improvements provided in Trac ticket #11450.

Binary Kloosterman Sums

The binary Kloosterman sums on $\mathbb{F}_{2^m}$ are

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)}, \quad a \in \mathbb{F}_{2^m} \quad .$$

Remark:
The function $a \mapsto K_m(a)$ is the **Walsh-Hadamard transform** of the function $\mathrm{Tr}_1^m(1/x)$.
Therefore, all values of Kloosterman sums can be computed at once using a fast Walsh-Hadamard transform.

Characterization using the Value 0

(Hyper)-bentness can be characterized using such sums. It is known since 1974 that the zeros of $K_m(a)$ give rise to bent functions.

Proposition (Monomial functions[Dil74, LW90, Lea06, CG08])

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be defined as

$$f(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right), \ \gcd(r, 2^m+1) = 1 \ .$$

Then f is hyper-bent iff $K_m(a) = 0$.

Several other families admit a similar characterization [Mesar].

Characterization using the Value 4

It is only in 2009 that Mesnager has shown that the value 4 leads to similar contructions [Mes11].

Proposition ([Mes11])

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be defined as

$$f(x) = \mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right), \ \gcd(r, 2^m+1) = 1 \ .$$

If m is odd, then f is hyperbent iff $K_m(a) = 4$. If m is even, this is a necessary condition.

More families are described in the same paper [Mes11].

Classical divisibility results

Divisibility of Kloosterman sums has been studied for a long time.

Proposition ([LW90])

Let $m \geq 3$ be a positive integer. The set $\{K_m(a), a \in \mathbb{F}_{2^m}\}$ is the set of all the integer multiples of 4 in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$.

Most classical results arise from the study of the link between **exponential sums** and **coset weight distribution** [HZ99, CHZ09].

Proposition ([HZ99])

Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}$. Then $K_m(a) \equiv 0 \pmod 8$ if and only if $\mathrm{Tr}_1^m(a) = 0$.

These conditions can be used to filter out the a's to test while performing a random search.

Further divisibility properties mod 3.

Proposition ([HZ99])

Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Suppose that there exists $t \in \mathbb{F}_{2^m}^*$ such that $a = b^4 + b^3$.

- If m is odd, then $K_m(a) \equiv 1 \pmod 3$.
- If m is even, then $K_m(a) \equiv 0 \pmod 3$ if $\mathrm{Tr}_1^m(b) = 0$ and $K_m(a) \equiv -1 \pmod 3$ if $\mathrm{Tr}_1^m(b) = 1$.

Proposition ([CHZ09])

Let $a \in \mathbb{F}_{2^m}^*$. Then we have:

- If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$. This is equivalent to $a = \frac{b}{(1+b)^4}$ for some $b \in \mathbb{F}_{2^m}^*$.
- If m is even, then $K_m(a) \equiv 1 \pmod 3$ if and only if $a = b^3$ for some b such that $\mathrm{Tr}_2^m(b) \neq 0$.

Equations

Here are some specific results to elliptic curves in even characteristic.

- E is **ordinary** iff $j(E) \neq 0$.
- It can then be described as

$$E : y^2 + xy = x^3 + bx^2 + a \ ,$$

  with $a \neq 0$ and $j(E) = 1/a$.
- Moreover its first **division polynomials** are [Kob90, BSS00]

$$f_1(x) = 1, \quad f_2(x) = x,$$
$$f_3(x) = x^4 + x^3 + a, \quad f_4(x) = x^6 + ax^2 \ .$$

Quadratic twist

If E is ordinary, then the quadratic twist $\widetilde{E}$ is an elliptic curve with the same j-invariant as E, but **non-isomorphic** to it over $\mathbb{F}_q$ (it becomes so over $\mathbb{F}_{q^2}$).
It can be given by the **Weierstrass equation**

$$\widetilde{E} : y^2 + xy = x^3 + \widetilde{b}x^2 + a \ ,$$

where $\widetilde{b}$ is any element of $\mathbb{F}_q$ such that $\mathrm{Tr}_1^m\left(\widetilde{b}\right) = 1 - \mathrm{Tr}_1^m(b)$ [Eng99].
The **number of points** of a curve and its quadratic twist are closely related [Eng99, BSS00]:

$$\#E + \#\widetilde{E} = 2q + 2 \ .$$

Curves with a given number of points

The cardinality of a curve is given by the trace of its **Frobenius**:

$$\#E = q + 1 - t \ .$$

If E is **ordinary**, then $2 \nmid t$ and the endomorphism ring of E is an order in $K = \mathbb{Q}[\alpha]$ containing the order $\mathbb{Z}[\alpha]$ of discriminant Δ where $\alpha = \frac{t+\sqrt{\Delta}}{2}$ and $\Delta = t^2 - 4q$.
This implies that the number of such curves is given by the Kronecker class number [Sch87, Cox89]

$$H(\Delta) = \sum_{\mathbb{Z}[\alpha] \subset \mathcal{O} \subset K} h(\mathcal{O}) \ .$$

It can be computed using more classical quantities as

$$H(\Delta) = h(\mathcal{O}_K) \sum_{d|f} \frac{d}{[\mathcal{O}_K^* : \mathcal{O}]} \prod_{p|d} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right) \ .$$

Elliptic curves and Kloosterman sums

The first result above is in fact proved using elliptic curves!

Theorem ([LW87, KL89])

Let $m \geq 3$ be any positive integer, $a \in \mathbb{F}_{2^m}^*$ and $E_m(a)$ the elliptic curve defined over $\mathbb{F}_{2^m}$ by the equation

$$E_m(a) : y^2 + xy = x^3 + a \ .$$

Then

$$\# E_m(a) = 2^m + K_m(a) \ .$$

The theory of elliptic curve can be used much further. For example, the fact that the Kloosterman sums are divisible by 4 is nothing but the fact that every such elliptic curves has a 4-**torsion point**.

Refining HZ Result

Proposition

Let $a \in \mathbb{F}_{2^m}^*$.

- If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
- If m is even, then:
  - $K_m(a) \equiv 0 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 0$;
  - $K_m(a) \equiv -1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 1$.

Idea of the proof:

1. One way is given by [HZ99].
2. For the other way, look at the 3-division polynomial of E or $\widetilde{E}$.

Basic search algorithm

The above discussion already gives an **efficient method** to find specific values of Kloosterman sums.

1. Pick a random $a \in \mathbb{F}_{2^m}$.
2. Transform it to have a given shape.
3. Check for additional divisibility properties.
4. Compute the cardinality of $E_m(a)$.

The computation of the cardinality is indeed **quadratic** in m [Har02, Ver03]:

$$O(m^2 \log^2 m \log \log m) \quad .$$

Finding zeros

The condition of the Lachaud-Wolfmann theorem is

$$\#E_m(a) = 2^m \quad .$$

Then, as a group

$$E_m(a) \simeq \mathbb{Z}/2^m\mathbb{Z} \quad ,$$

and half its points have exact order 2^m.

From these facts, Lisoněk [Lis08] deduced that to check that $E_m(a)$ indeed has a such structure it is enough to **take a random point** and **check it has order exactly 2^m**. If a such point is found, then the Hasse-Weil theorem ensures that $E_m(a)$ is indeed of cardinality 2^m. This gives an **efficient probabilistic algorithm** to find zeros of Kloosterman sums and he could find zeros of Kloosterman sums for m up to 64.

Sylow group

Ahmadi and Granger subsequently built an efficient deterministic algorithm from the above observations [AG11].
Rather than computing the number of points of the randomly chosen curves, it is indeed enough to compute the size of the 2-Sylow subgroup of $E_m(a)$. This can be efficiently done by **point halving**.

The **average bit complexity** for one curve is

$$O(m \log m \log \log m)$$

whereas it is

$$O(m^2 \log^2 m \log \log m)$$

for point counting.

Extending to the value 4

Looking for the value 4, the cardinality of the curve has a way less special form:

$$\#E_m(a) = 2^m + 4 = 4(2^{m-2} + 1) \ ,$$

and the cardinality of the twisted curve is not better

$$\#\widetilde{E}_m(a) = 2^m - 2 = 2(2^{m-1} - 1) \ .$$

We can however deduce from these equalities some **filtering properties**.

- $K_m(a) \equiv 4 \pmod 8$, so that $\mathrm{Tr}_1^m(a) = 1$;
- $K_m(a) \equiv 1 \pmod 3$, so that:
    - if m is odd, then a can be written as $t^4 + t^3$;
    - if m is even, then a can be written as t^3 with $\mathrm{Tr}_2^m(t) \neq 0$.

Algorithm for m odd

Input: A positive odd integer $m \geq 3$
Output: An element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$

```
1  a ←_R F_{2^m}
2  a ← a^3(a + 1)
3  if Tr_1^m(a) = 0 then
4      Go to step 1
5  P ←_R E_m(a)
6  if [2^m + 4]P ≠ 0 then
7      Go to step 1
8  if #E_m(a) ≠ 2^m + 4 then
9      Go to step 1
10 return a
```

Implementation for m odd

Some reasonably **efficient point counting** on $\mathbb{F}_{2^n}$ is needed.

- Easy solution: use Magma.
- Less easy solution: use Yeoh's GP script [Yeo].
- Harder solution: use Sage with Trac ticket #11448 or #11548.
- Hardest solution: implement it in a C library and interface it from Sage.

As a result of our experiments, we found that the following value of a for $m = 55$ gives a value 4 of binary Kloosterman sum.

The finite field $\mathbb{F}_{2^{55}}$ is represented as $\mathbb{F}_2[x]/(x^{55} + x^{11} + x^{10} + x^9 + x^7 + x^4 + 1)$; a is then given as

$$\begin{aligned} a = x^{53} + x^{52} + x^{51} + x^{50} + x^{47} + x^{43} + x^{41} + x^{38} + x^{37} + x^{35} \\ + x^{33} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} \\ + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^{5} \quad . \end{aligned}$$

Some **caching management** problems in Sage are somehow limiting. See Trac tickets #715 and #11521.

m Even

In the case where m is **even**, the condition given by Mesnager has only been shown to be necessary. It is of interest to check computationally whether counterexamples can be found for **small** values of m.

The problem of computing all elements giving a specific value, rather than looking for one, must be handled differenly. A **fast Walsh-Hadamard transform** should be used.

Moreover, to test all functions in the family defined by Mesnager:

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \quad ,$$

it is enough to set $b = 1$ and test **one** a in each cyclotomic class.

Algorithm for m even

The test algorithm is as follows:

1. Compute $\{| K_m(a) \mid a \in \mathbb{F}_{2^m}\}$ with a fast Walsh-Hadamard transform of $\mathrm{Tr}\, m1/x$.
2. Select one a in each cyclotomic class such that $K_m(a) = 4$.
3. For each a compute the corresponding Boolean function.
4. For each function check its bentness using a fast Walsh-Hadamard transform.

In step 2 it is possible to efficiently test one and only one a in each cyclotomic class using **necklaces** [Duv88, RSW92, Rus03].
Step 3 is the most **time** consuming one.
Step 4 is the most memory consuming one.

Experimental Results

The implementation was made using Sage [S+11] and Cython [BCS10], performing direct calls to Givaro [DGG+08], NTL [Sho08] and gf2x [BGTZ08] libraries for efficient manipulation of finite field elements and construction of Boolean functions.

m	Nb. of cyclotomic classes	Time	All bent?
4	1	<1s	yes
6	1	<1s	yes
8	2	<1s	yes
10	3	4s	yes
12	6	130s	yes
14	8	3000s	yes
16	14	82000s	yes
18	20	-	-

Thank you for your attention.

Charpin-Gong criterion

Charpin and Gong [CG08] gave the following characterization of hyperbentness for a large class of Boolean functions.

Theorem ([CG08])

Let

$$f_{a_r}(x) = \sum_{r \in R} \mathrm{Tr}_1^n \left(a_r x^{r(2^m-1)} \right) \quad ,$$

$a_r \in \mathbb{F}_{2^m}$, *where* $R \subseteq S$. *Let* $g_{a_r}(x) = \sum_{r \in R} \mathrm{Tr}_1^m \left(a_r D_r(x) \right)$. *Then* f_{a_r} *is hyperbent iff*

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi \left(\mathrm{Tr}_1^m \left(x^{-1} \right) + g_{a_r}(x) \right) = 2^m - 2\,\mathrm{wt}(g_{a_r}) - 1 \quad .$$

Mesnager criterion

Mesnager [Mes10] gave a characterization of hyperbentness for another large class of Boolean functions

Theorem ([Mes10])

Let m be odd, b a primitive element of $\mathbb{F}_4^*$ and

$$f_{a_r,b}(x) = \sum_{r\in R} \mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(b x^{\frac{2^n-1}{3}}\right) .$$

Then $f_{a_r,b}$ is hyperbent iff

1. $$\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi\left(g_{a_r}(D_3(x))\right) = -2;$$
2. $$\sum_{x\in\mathbb{F}_{2^m}^*} \chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right) + g_{a_r}(D_3(x))\right) = 2^m - 2\,\mathrm{wt}(g_{a_r}\circ D_3) + 3.$$

Lisoněk's idea

Lisoněk [Lis08] extended the ideas of Lachaud and Wolfmann to reformulate the Charpin-Gong criterion in terms of hyperelliptic curves.

Proposition

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function such that $f(0) = 0$, $g = \mathrm{Tr}_1^m(f)$ and G_f be the (affine) curve defined over $\mathbb{F}_{2^m}$ by

$$G_f : y^2 + y = f(x) \ .$$

Then

$$\sum_{x \in \mathbb{F}_{2^m}^*} \chi(g(x)) \, (= 2^m - 1 - 2\,\mathrm{wt}(g)) = -2^m - 1 + \#G_f \ .$$

Reformulation of CG criterion

Applied to CG criterion we get the following characterization.

Theorem ([Lis11])

Let H_{a_r} and G_{a_r} be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$H_{a_r} : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(x) \quad ,$$

$$G_{a_r} : y^2 + y = \sum_{r \in R} a_r D_r(x) \quad .$$

Then f_{a_r} is hyperbent if and only if

$$\#H_{a_r} - \#G_{a_r} = -1 \quad .$$

Complexity

The smooth projective models of the curves H_{a_r} and G_{a_r} are hyperelliptic. The polynomial defining H_{a_r} (respectively G_{a_r}) is of degree $r_{max} + 2$ (respectively r_{max}), so the curve is of genus $(r_{max} + 1)/2$ (respectively $(r_{max} - 1)/2$). The complexity for testing a Boolean function in this family is then dominated by the computation of the cardinality of a curve of genus $(r_{max} + 1)/2$, which is polynomial in m for a fixed r_{max} (and so fixed genera for the curves H_{a_r} and G_{a_r}).

Theorem

Let H be an hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exist an algorithm to compute the cardinality of H in

$$O(g^3m^3(g^2 + \log^2 m \log\log m)\log gm \log\log gm)$$

bit operations and $O(g^4m^3)$ memory.

Reformulation of Mesnager criterion

Theorem

Let $H^3_{a_r}$ and $G^3_{a_r}$ be the (affine) curves defined over $\mathbb{F}_{2^m}$ by

$$H^3_{a_r} : y^2 + xy = x + x^2 \sum_{r \in R} a_r D_r(D_3(x)) \ ,$$

$$G^3_{a_r} : y^2 + y = \sum_{r \in R} a_r D_r(D_3(x)) \ .$$

If b is a primitive element of $\mathbb{F}_4$, then $f_{a_r,b}$ is hyperbent if and only if

$$\# H^3_{a_r} - \# G^3_{a_r} = 3 \ .$$

We have to compute the cardinalities of two curves of genera $(3r_{max} + 1)/2$ and $(3r_{max} - 1)/2$.

Little trick

Using the fact that $x \mapsto D_3(x) = x^3 + x$ is a permutation when m is odd.

Theorem

If b is a primitive element of $\mathbb{F}_4$, then $f_{a_r,b}$ is hyperbent if and only if

$$\#G_{a_r}^3 - \frac{1}{2}\left(\#G_{a_r} + \#H_{a_r}\right) = -\frac{3}{2} \quad .$$

This is slightly more efficient.

References I

Omran Ahmadi and Robert Granger.
An efficient deterministic test for Kloosterman sum zeros.
CoRR, abs/1104.3882, 2011.

J. Arndt.
Matters Computational: Ideas, Algorithms, Source Code.
Springer, 2010.

R. Bradshaw, C. Citro, and D.S. Seljebotn.
Cython: the best of both worlds.
CiSE 2011 Special Python Issue, page 25, 2010.

Richard P. Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann.
Faster multiplication in GF(2)[x].
In Alfred J. van der Poorten and Andreas Stein, editors, *ANTS*, volume 5011 of *Lecture Notes in Computer Science*, pages 153–166. Springer, 2008.

I. F. Blake, G. Seroussi, and N. P. Smart.
Elliptic curves in cryptography, volume 265 of *London Mathematical Society Lecture Note Series*.
Cambridge University Press, Cambridge, 2000.
Reprint of the 1999 original.

References II

Pascale Charpin and Guang Gong.
Hyperbent functions, Kloosterman sums, and Dickson polynomials.
IEEE Transactions on Information Theory, 54(9):4230–4238, 2008.

Pascale Charpin, Tor Helleseth, and Victor Zinoviev.
Divisibility properties of classical binary Kloosterman sums.
Discrete Mathematics, 309(12):3975–3984, 2009.

David A. Cox.
Primes of the form $x^2 + ny^2$.
A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989.
Fermat, class field theory and complex multiplication.

Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi, Jean-Louis Roch, and Gilles Villard.

Givaro-3.2.13rc1: C++ library for arithmetic and algebraic computations, September 2008.

http://ljk.imag.fr/CASYS/LOGICIELS/givaro/.

John Francis Dillon.
Elementary Hadamard Difference Sets.
ProQuest LLC, Ann Arbor, MI, 1974.
Thesis (Ph.D.)–University of Maryland, College Park.

References III

Jean-Pierre Duval.
Génération d'une section des classes de conjugaison et arbre des mots de Lyndon de longueur bornée.
Theor. Comput. Sci., 60:255–283, 1988.

Andreas Enge.
Elliptic Curves and Their Applications to Cryptography: An Introduction.
Springer, 1st edition, August 1999.

Robert Harley.
Asymptotically optimal p-adic point-counting.
Email to NMBRTHRY list, December 2002.
http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343.

Tor Helleseth and Victor Zinoviev.
On linear Goethals codes and Kloosterman sums.
Des. Codes Cryptography, 17(1-3):269–288, 1999.

Nicholas Katz and Ron Livné.
Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3.
C. R. Acad. Sci. Paris Sér. I Math., 309(11):723–726, 1989.

References IV

Neal Koblitz.
Constructing elliptic curve cryptosystems in characteristic 2.
In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 1990.

N. G. Leander.
Monomial bent functions.
IEEE Transactions on Information Theory, 52(2):738–743, 2006.

Petr Lisonek.
On the connection between Kloosterman sums and elliptic curves.
In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008.

Petr Lisoněk.
Hyperbent functions and hyperelliptic curves.
Talk given at Arithmetic, Geometry, Cryptography and Coding Theory (AGCT-13), March 2011.

Gilles Lachaud and Jacques Wolfmann.
Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2.
C. R. Acad. Sci. Paris Sér. I Math., 305(20):881–883, 1987.

References V

Gilles Lachaud and Jacques Wolfmann.
The weights of the orthogonals of the extended quadratic binary Goppa codes.
IEEE Transactions on Information Theory, 36(3):686Ð692, 1990.

Sihem Mesnager.
Hyper-bent boolean functions with multiple trace terms.
In M. Anwar Hasan and Tor Helleseth, editors, *WAIFI*, volume 6087 of *Lecture Notes in Computer Science*, pages 97–113. Springer, 2010.

Sihem Mesnager.
A new class of bent and hyper-bent Boolean functions in polynomial forms.
Des. Codes Cryptography, 59(1-3):265–279, 2011.

Sihem Mesnager.
Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials.
IEEE Transactions on Information Theory, To appear.

Frank Ruskey, Carla D. Savage, and Terry Min Yih Wang.
Generating necklaces.
J. Algorithms, 13(3):414–430, 1992.

References VI

Frank Ruskey.
Combinatorial Generation.
Unpublished manuscript, 2003.
Working Version (1j-CSC 425/520).

W. A. Stein et al.
Sage Mathematics Software (Version 4.7).
The Sage Development Team, 2011.
`http://www.sagemath.org`.

René Schoof.
Nonsingular plane cubic curves over finite fields.
J. Comb. Theory, Ser. A, 46(2):183–211, 1987.

Victor Shoup.
NTL 5.4.2: A library for doing number theory, March 2008.
`www.shoup.net/ntl`.

Frederik Vercauteren.
Computing zeta functions of curves over finite fields.
PhD thesis, Katholieke Universiteit Leuven, 2003.

References VII

Yeoh.
GP/Pari implementation of point counting in characteristic 2.
http://pages.cs.wisc.edu/~yeoh/nt/satoh-fgh.gp.