ACADEMIC PRESS

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 9 (2003) 1–19

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Weight of duals of BCH codes and exponential sums

Eric Férard*

Université de la Polynésie Française, B.P. 6570, Polynésie 98702, France

Received 21 June 2000; revised 5 June 2001; accepted 25 February 2002
Communicated by Oscar Moreno

Abstract

We consider a binary BCH code C_m of length 2^m-1. If m is odd, we improve the bound on the distance of the dual of C_m previously given by Carlitz–Uchiyama, Serre and Moreno–Moreno.

1. Introduction

Let C_m be a binary BCH code of length $q-1=2^m-1$ with designed distance $\delta=2t+1$. The weight w of a non-zero codeword of the dual of C_m satisfies the Carlitz–Uchiyama bound

$$|w-2^{m-1}|\leq(t-1)2^{m/2}.$$

We shall only consider the case where m is odd. We attempt to improve this bound.

In [8], MacWilliams and Sloane suggest a stronger result

$$|w-2^{m-1}|\leq(t-1)2^{(m-1)/2}. \qquad (1)$$

One can show that this inequality is true for $\delta=3$, 5, 7. Moreover, when $\delta=3$, 5, 7, this bound is reached. Rodier [11] showed that this inequality is not true for codes

*Fax: 33-4-9126-9655.
E-mail address: eric.ferard@upf.pf.

PII: S1071-5797(02)00016-3

of designed distance $\delta = 9, 25, \ldots$. A similar result was independently obtained by Càceres and Moreno [2].

If p is a prime number and l an integer, we denote by $\mathbf{F}_{p^l}$ a finite field of order p^l. If K is a field and L a finite extension of K, we denote by $\mathrm{Tr}_{L/K}$ the trace from L to K.

Let c be a codeword of the dual of C_m. Its weight $w(c)$ is linked to the value of some exponential sums. Indeed, the codeword c can be written in the form

$$c = (\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(\alpha)))_{\alpha \in \mathbf{F}_q^*},$$

where f is a polynomial with coefficients in $\mathbf{F}_q$ of degree at most $2t-1$ and $f(0) = 0$ (see [8]). Since $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(\alpha^2) = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(\alpha)$, we can always suppose that f is zero or of odd degree. We define the exponential sum $S(f)$ by

$$S(f) = \sum_{x \in \mathbf{F}_q} (-1)^{\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(x))}.$$

Since the weight of c is the number of $\alpha \in \mathbf{F}_q$ such that $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(\alpha)) = 1$, we have

$$w(c) = \frac{q - S(f)}{2}.$$

If the degree of f is odd, the exponential sum $S(f)$ satisfies the Weil bound

$$|S(f)| \leq (\deg f - 1)\sqrt{q}.$$

We may note that this bound corresponds to the Carlitz–Uchiyama bound. To improve the Carlitz–Uchiyama bound, we have chosen to study the exponential sums and the Weil bound. We can deduce from (1) that we have

$$|S(f)| \leq (\deg f - 1)\sqrt{q}/\sqrt{2}$$

for polynomials of degree 1, 3 and 5. Moreover, this bound is reached. Therefore, we shall only consider polynomials of degree greater than or equal to 7.

The number of points N of the projective model of the curve $y^2 + y = f(x)$ over $\mathbf{F}_q$ is given by

$$N = q + 1 + S(f).$$

Therefore, in this particular case, we may also improve the Weil bound.

Let us fix some notations. If v is a real number, we denote by $[v]$ its integer part. Let u be an integer with binary expansion

$$u = \sum_{i=1}^{r} 2^{u_i}.$$

We define the binary weight $\sigma(u)$ of u by

$$\sigma(u) = r.$$

If $Q(x)$ is a polynomial with coefficients in $\mathbf{F}_q$, we define its binary weight $\sigma(Q)$ as being the maximum of the binary weights of the exponents of Q.

In 1984, Serre [15] improved the Weil bound as

$$|S(f)| \leq \frac{\deg f - 1}{2}[2\sqrt{q}].$$

Using the Serre method and the divisibility properties of the exponential sums Moreno and Moreno improved this last bound as

$$|S(f)| \leq (\deg f - 1)2^{\mu-1}[2^{1-\mu}\sqrt{q}],$$

where $\mu = [m/\sigma(f)]$.

2. Backgrounds on abelian varieties

Let p be a prime number. Let $\mathbf{Q}_p$ be the field of p-adic numbers. Let Ω be the completion of the algebraic closure of $\mathbf{Q}_p$. We denote by $\mathrm{ord}_p(\cdot)$ the valuation over Ω normalized by $\mathrm{ord}_p(p) = 1$. We denote by $|\cdot|_p$ the absolute value over Ω defined by $|x|_p = p^{-\mathrm{ord}_p(x)}$.

Let $P = \sum_{i=1}^{r} c_i t^i$ be a polynomial with coefficients in $\mathbf{Q}_p$. The Newton polygon of P is the convex hull of the points $(i, \mathrm{ord}_p\, c_i)$ (see [4]).

Proposition 1. *If a segment of the Newton polygon of P has a slope λ and horizontal length N, then P has precisely N roots y_i with $\mathrm{ord}_p(y_i) = -\lambda$ (counting multiplicities).*

Proof. See [4].

Put $q = p^m$. Let $k = \mathbf{F}_q$ be a finite field of q elements.

We now recall some results on abelian varieties. The reader is referred to Tate [17,18] and Waterhouse [19]. Let A be an abelian variety over k of dimension g. The characteristic polynomial h_A of the Frobenius endomorphism π_A of A over k is a monic of degree $2g$ over $\mathbf{Z}$. This polynomial determines the isogeny class of A.

Theorem 1 (Tate). *Two abelian varieties defined over k are isogenous if and only if their Frobenius endomorphisms have the same characteristic polynomial.*

Let $E = \mathrm{End}_k(A) \otimes \mathbf{Q}$ be the endomorphism algebra of A. It is a semisimple algebra with center $F = \mathbf{Q}[\pi_A]$.

There is a unique factorization of A, up to k-isogeny, into a product of powers of non-k-isogenous simple abelian varieties A_j. This factorization corresponds to the decomposition of E into simple factors E_j and therefore to the expression of its center F as a product of fields F_j. The F_j in turn correspond to the irreducible factors P_j of h_A over $\mathbf{Q}$. From the previous theorem we deduce the following result.

Theorem 2. *Let $h_A = \Pi P_j^{m_j}$ be the factorization of h_A in $\mathbf{Q}$. For each j, there exists an integer e_j dividing m_j and a simple abelian variety A_j over k, whose characteristic polynomial of the Frobenius endomorphism is P^{e_j}, such that A is isogenous to*

$$\Pi A_j^{m_j/e_j}.$$

We assume that A is simple. Then $F = \mathbf{Q}(\pi_A)$ is a field. Weil has shown that π_A is an algebraic integer such that for all embeddings $\phi : \mathbf{Q}(\pi_A) \to \mathbf{C}$, we have $|\phi(\pi_a)| = q^{1/2}$. We will call such an algebraic integer, a Weil number. Honda has made explicit the correspondence between Weil numbers and the simple abelian varieties over k.

Theorem 3 (Honda [3,18]). *There is a one-to-one correspondence between the isogeny classes of simple abelian varieties over k and the classes of conjugates over $\mathbf{Q}$ of Weil numbers.*

Since A is simple, the characteristic polynomial of π_A is equal to

$$h_A = P^e,$$

where P is a $\mathbf{Q}$-irreducible polynomial. Then the algebra of endomorphism E is an algebra of division of dimension e^2 over its center $F = \mathbf{Q}(\pi_A)$.

If v is a place of F, we denote by $\mathrm{inv}_v(E)$ the invariant of E at v (see [13]). If v is above p, we denote by $\mathrm{ord}_v(\cdot)$ the valuation on F associated to v normalized by $\mathrm{ord}_v(p) = 1$.

Theorem 4 (Tate). *Let A be a simple abelian variety over k. Let v be a place of F. Let F_v be the completion of F at v. The invariant of E at v is congruent to*

- *0 if v is complex or if v is lying over $l \neq p$,*
- *1/2 if v is real,*
- $\dfrac{\mathrm{ord}_v(\pi_A)[F_v : \mathbf{Q}_p]}{\mathrm{ord}_v(q)}$ *if v is lying over p,*

modulo $\mathbf{Z}$.

Proposition 2. *The sum of all the invariants of E is congruent to zero modulo $\mathbf{Z}$. The least common denominator of all the invariants of E is e.*

We note that if A is simple, the characteristic polynomial of π_A is not in general irreducible. It is so if and only if there are no real places in $\mathbf{Q}(\pi_A)$ and for each irreducible factor P_v of h_A over $\mathbf{Q}_p$, m divides $\mathrm{ord}_p\,(P_v(0))$.

The abelian variety A is no longer supposed to be simple. If $\omega_1, \bar{\omega}_1, \ldots, \omega_g, \bar{\omega}_g$ are the roots of h_A in $\mathbf{C}$, then the characteristic polynomial of π_A over $\mathbf{F}_{q^l}$ is given by

$$h_A^{(l)}(t) = \prod_{i=1}^{g} (t - \omega_i^l)(t - \bar{\omega}_i^l).$$

We shall say here that A is supersingular if $h_A^{(l)}(1)$ is prime to p for all positive integers l (cf. [12,20]). Oort gave another definition of a supersingular abelian variety: A is supersingular if A is isogenous over a finite extension of k to the power of a supersingular elliptic curve (see [6]). For abelian varieties of dimensions 1 and 2, these two definitions are equivalent. Note that if A is supersingular in Oort's meaning, then A is supersingular. But if A is an abelian variety of dimension greater than or equal to 3, the opposite is not true.

From now on in this section, we only consider the case where $p = 2$ and m is an odd integer. We shall need the list of all the characteristic polynomials of the Frobenius endomorphisms of simple supersingular abelian varieties of dimensions 1 and 2.

Proposition 3 (Deuring–Waterhouse [19]). *Let m be an odd integer. Let $q = 2^m$. The characteristic polynomials of the Frobenius endomorphisms of supersingular elliptic curves over $\mathbf{F}_q$ are*

(i) $t^2 \pm \sqrt{2q}t + q$,
(ii) $t^2 + q$.

Proposition 4 (Rück–Xing [21]). *Let m be an odd integer. Let $q = 2^m$. The characteristic polynomials of the Frobenius endomorphisms of supersingular simple abelian varieties of dimension 2 over $\mathbf{F}_q$ are*

(i) $t^4 \pm qt^2 + q^2$,
(ii) $t^4 \pm \sqrt{2q}t^3 + qt^2 \pm \sqrt{2q^3}t + q^2$,
(iii) $(t^2 - q)^2$.

Now, let us examine the case where the characteristic polynomial of the Frobenius endomorphism of an abelian variety has a real root.

Proposition 5 (Waterhouse [19]). *Let m be an odd integer. Let $q = 2^m$. Let A be an abelian variety over $\mathbf{F}_q$. If π_A has a real conjugate, then $(t^2 - q)^2$ divides $h_A(t)$ (in $\mathbf{Z}[t]$).*

3. Abelian varieties with quadratic Weil numbers

Let $q = p^m$. We generalize a result of Xing (see [20, Propositions 2 and 3]).

Proposition 6. *Let e be an integer, $e \geqslant 3$. Let $h(t) = (t^2 + \beta t + q)^e$ be a polynomial with integer coefficients and $|\beta| < 2\sqrt{q}$. Then h is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety over $\mathbf{F}_q$ if and only if e divides m and if there exists an integer i, $1 \leqslant i < e/2$, prime to e such that*

$$\mathrm{ord}_p(\beta) = im/e.$$

Proof. Put $f = t^2 + \beta t + q$. We assume that h is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety A over $\mathbf{F}_q$. Let π be a root of f. Put $F = \mathbf{Q}(\pi)$ and $E = \mathbf{Q} \otimes \mathrm{End}_{\mathbf{F}_q}(A)$. Since F is totally imaginary, if v is a place which is not above p, the invariant of E at v is zero (Theorem 4). Hence, p splits in two places in F because the sum of all the invariants of E is congruent to zero modulo $\mathbf{Z}$ and e, which is greater than or equal to 3, is their least common denominator (Proposition 2). Therefore, f can be written as a product

$$f(t) = (t - y_1)(t - y_2)$$

with $y_1, y_2 \in \mathbf{Q}_p$. Denote by v_i the place corresponding to the embedding of F into $\mathbf{Q}_p$ which maps π on y_i. For $i = 1, 2$, we have

$$\mathrm{inv}_{v_i}(E) \equiv \mathrm{ord}_p(y_i)/m \bmod \mathbf{Z}.$$

Consider the Newton polygon of $t^2 + \beta t + q$. We assume that the point $(1, \mathrm{ord}_p(\beta))$ is a vertex, i.e. $\mathrm{ord}_p(\beta) < m/2$. Then we may suppose that $\mathrm{ord}_p(y_1) = \mathrm{ord}_p(\beta)$ and $\mathrm{ord}_p(y_2) = m - \mathrm{ord}_p(\beta)$. It follows that

$$\mathrm{inv}_{v_1}(E) \equiv \mathrm{ord}_p(\beta_i)/m \bmod \mathbf{Z}.$$

and

$$\mathrm{inv}_{v_2}(E) \equiv -\mathrm{ord}_p(\beta_i)/m \quad \mathbf{Z}.$$

Since e is the least common denominator of $\mathrm{inv}_{v_1}(E)$ and $\mathrm{inv}_{v_2}(E)$, there exists an integer $i \geqslant 1$ prime to e such that

$$\mathrm{ord}_p(\beta) = im/e.$$

Since $\mathrm{ord}_p(\beta) < m/2$, we have $i/e < 1/2$.

We assume now that the point $(1, \mathrm{ord}_p(\beta))$ is not a vertex, i.e. $\mathrm{ord}_p(\beta) \geqslant m/2$. Then we have

$$\mathrm{ord}_p(y_1) = \mathrm{ord}_p(y_2) = m/2 \quad \text{and} \quad \mathrm{inv}_{v_1}(E) = \mathrm{inv}_{v_2}(E) = \tfrac{1}{2},$$

which would contradict the hypothesis concerning e.

Conversely, let β be an integer such that $|\beta| < 2\sqrt{q}$. Suppose that e divides m and that there exists an integer i, $1 \leq i < e/2$, prime to e such that $\mathrm{ord}_p(\beta) = im/e$. Let π be a root of h. By Theorem 3, we can associate a simple abelian variety over $\mathbf{F}_q$ to π. The characteristic polynomial of the Frobenius endomorphism of this variety is equal to the r-power of the minimal polynomial of π over $\mathbf{Q}$ where r is the least common denominator of all the invariants of E at the places of $F = \mathbf{Q}(\pi)$ (Proposition 2).

Since $\mathrm{ord}_p(\beta) < m/2$, the point $(1, \mathrm{ord}_p(\beta))$ is the only vertex (except the ones on the axis) of the Newton polygon of $t^2 + \beta t + q$. Hence, there are two places v_1 and v_2 above p and

$$\mathrm{inv}_{v_1}(E) \equiv i/e \bmod \mathbf{Z},$$

$$\mathrm{inv}_{v_2}(E) \equiv -i/e \bmod \mathbf{Z}.$$

Since the invariants of E at the places which are not above p are zero, we have $r = e$. Therefore, h is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety over $\mathbf{F}_q$. $\square$

The abelian varieties described in this proposition are supersingular.

4. Bound on exponential sums

We now assume that $p = 2$ and m is an odd integer.

Let f be a polynomial over $\mathbf{F}_q$ of degree $2g + 1$. Let a be the binary weight of f. We suppose that $a \geqslant 3$ and $m \geqslant a$. Let $\mu = [m/a]$. Since $a \geqslant 3$ and $m \geqslant a$, we have $0 < \mu < m/2$.

Theorem 5 (Litsyn et al. [7]). *Let f be a polynomial over $\mathbf{F}_q$. Then*

$$\mathrm{ord}_2\, S(f) \geq m/\sigma(f).$$

For any positive integer r, we denote

$$S_r = \sum_{x \in \mathbf{F}_{q^r}} (-1)^{\mathrm{Tr}_{\mathbf{F}_{q^r}/\mathbf{F}_2}(f(x))}.$$

Let J be the Jacobian of the curve $y^2 + y = f(x)$ over $\mathbf{F}_q$. It is an abelian variety of dimension g. Let $h = \sum_{i=0}^{2g} a_i t^{2g-i}$ be the characteristic polynomial of the Frobenius endomorphism of J over $\mathbf{F}_q$. Let $\omega_1, \bar{\omega}_1, \ldots, \omega_g, \bar{\omega}_g$ be the roots of h in $\mathbf{C}$. Weil has shown that

$$S_r = -\sum_{i=1}^{g}(\omega_i^r + \bar{\omega}_i^r)$$

for any positive integer r.

Lemma 1. *For $i = 1, \ldots, 2g, 2^{i\mu}$ divides a_i.*

Proof. We follow the proof of Ax (see [1]). Let $L(t,f) = \exp(\sum_{r=1}^{\infty} S_r t^r/r)$.
This function is equal to

$$L(t,f) = \prod_{i=1}^{g}(1-\omega_i t)(1-\bar{\omega}_i t).$$

By logarithmic differentiation of $L(t,f)$, we obtain

$$\sum_{r=1}^{\infty} S_r t^{r-1} = -\sum_{i=1}^{g}\left(\frac{\omega_i}{1-\omega_i t} + \frac{\bar{\omega}_i}{1-\bar{\omega}_i t}\right).$$

By Theorem 5, the dyadic absolute value $|S_r|_2$ of S_r is lower than $2^{-\mu r}$ for any positive integer r. If $|t|_2 < 2^{\mu}$, the left-hand side converges in Ω. It follows that $|\omega_i| \leq 2^{-\mu}$ and $|\bar{\omega}_i| \leq 2^{-\mu}$ for $i = 1, \ldots, g$. $\square$

By this lemma, since $\mu \geq 1$, J is supersingular.

We deduce from this lemma that $\omega_i/2^{\mu}$ and $\bar{\omega}_i/2^{\mu}$ are algebraic integers. We may apply to them the Serre method to improve the Weil bound (see [15] or [9]). Put $M = [2^{1-\mu}\sqrt{q}]$ and $x_i = M + 1 + (\omega_i + \bar{\omega}_i)/2^{\mu}$ for $i = 1, \ldots, g$. The numbers x_i are totally positive algebraic integers. Therefore, $\prod x_i$ is a strictly positive integer. By the mean inequality, we have

$$\frac{\sum x_i}{g} \geq \left(\prod x_i\right)^{1/g} \geq 1.$$

This implies

$$S(f) \leq g \cdot 2^{\mu} M.$$

Lemma 2. *Let f_1 be a polynomial over $\mathbf{F}_q$ of degree r. Then there exists a polynomial f_2 over $\mathbf{F}_q$ of degree r such that*

$$S(f_1) = -S(f_2).$$

Proof. Since the trace $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}$ is surjective, there exists $\mathbf{F}_q$ such that $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(\alpha) = 1$. Then $S(f_1) = -S(f_1 + a)$. This proves the lemma. $\square$

We deduce from the lemma the following result.

Theorem 6 (Moreno and Moreno [9,10]). *Let f be a polynomial over $\mathbf{F}_q$ of odd degree. Then*

$$|S(f)| \leq (\deg f - 1) \cdot 2^{[m/\sigma(f)]-1}[2^{1-[m/\sigma(f)]}\sqrt{q}].$$

5. The defect

Let l be a non-negative integer. We say that f has *defect* l if

$$S(f) = g \cdot 2^{\mu} M - l \cdot 2^{\mu}.$$

If f has defect 0 (respectively 1, 2), then $\sum x_i = g$ (respectively $g+1, g+2$). The list of families $(\alpha_i)_{i=1,\dots,g}$ of totally positive algebraic integers such that $\sum \alpha_i = g$, $g+1$ or $g+2$ is known (see [5,14,16]). Hence the family (x_i) is in this list. We deduce the possibilities for the characteristic polynomial of the Frobenius endomorphism of J. We shall use it to prove that $|S(f)|$ is different from $g \cdot 2^{\mu} M - 2^{\mu}$ and $g \cdot 2^{\mu} M - 2^{\mu+1}$ in most of the cases. If f has defect 0, then all the x_i are equal to 1. Hence, the characteristic polynomial of the Frobenius endomorphism of J is

$$h(t) = (t^2 + 2^{\mu} M t + q)^g.$$

We now need a lemma.

Lemma 3. *Let α be a positive integer. Then*

(i) $[2^{\alpha}\sqrt{2}] \neq 2^{\alpha}$ *if* $\alpha \neq 1$,
(ii) $[2^{\alpha}\sqrt{2}] \neq 2^{\alpha} + 1$ *if* $\alpha \neq 2$,
(iii) $[2^{\alpha}\sqrt{2}] \neq 2^{\alpha} + 2$,
(iv) $[2^{\alpha}\sqrt{2}] \neq 2^{\alpha-1} + 1$ *if* $\alpha \neq 1$,
(v) $[2^{\alpha}\sqrt{2}] \neq 2^{\alpha-2} + 1$,
(vi) $[2^{\alpha}\sqrt{2}] \geq 2$.

Proof. It suffices to notice that $M \geq 2^{\alpha} + 2^{\alpha-2} + 2^{\alpha-3}$ for $\alpha \geq 3$. The lemma is an immediate consequence of this inequality. $\square$

5.1. Defect 0

Let us examine the case where $|S(f)| = g2^{\mu}M$. We may assume that $S(f) = g2^{\mu}M$ (Lemma 2). As mentioned at the beginning of this section, the characteristic polynomial of the Frobenius endomorphism of J is

$$h(t) = (t^2 + 2^{\mu}Mt + q)^g.$$

By Theorem 2, there exists an integer d dividing g and a simple supersingular abelian variety A over $\mathbf{F}_q$ such that J is isogenous to A^d. If we write $e = g/d$, the characteristic polynomial of the Frobenius endomorphism of A is

$$h_A(t) = (t^2 + 2^{\mu}Mt + q)^e.$$

If $e = 1$, $t^2 + 2^{\mu}Mt + q$ is the characteristic polynomial of the Frobenius endomorphism of a supersingular elliptic curve if and only if $m = 1 + 2\mu$ (Proposition 3 and Lemma 3). Moreover, e is different from 2 because $(t^2 + 2^{\mu}Mt + q)^2$ is not the characteristic polynomial of the Frobenius endomorphism of a supersingular simple abelian variety over $\mathbf{F}_q$ of dimension 2 (Proposition 4). We shall study the case $e \geqslant 3$.

Let b be the greatest odd integer dividing g. By Proposition 6, e divides m. But, by assumption, m is odd, hence e is odd and must divide b. Since $e \geqslant 3$, we have $\gcd(b, m) \geqslant 3$.

We will consider two cases according to whether m is a multiple of the binary weight a of f or not.

Proposition 7. *We assume that a divides m and that $|S(f)| = g \cdot 2^{\mu}M$. If M is odd, then a divides b. If M is even, then*

$$\mathrm{ord}_2\ M \geq \mu/b.$$

Proof. By Proposition 6, there exists an integer $i, 1 \leq i < e/2$, prime to e such that

$$\mu + \mathrm{ord}_2\ M = im/e. \tag{2}$$

We assume that M is odd. Equality (2) gives

$$e = ia.$$

Since i is prime to e, we have $e = a$.

We assume that M is even. We deduce from (2) that

$$\mathrm{ord}_2\ M = \mu(ai - e)/e.$$

Since M is even, we have $ai > e$ and

$$\mathrm{ord}_2\ M \geq \mu/e \geq \mu/b.$$

We have also shown that if $|S(f)| = g \cdot 2^{\mu} M$ and M is odd, then the invariants of E at the two places above 2 are $1/a$ and $-1/a$.

Proposition 8. *We assume that a does not divide m. We write* $m = a\mu + r$ *with* $0 < r < a$. *We suppose that* $|S(f)| = g \cdot 2^{\mu} M$. *If M is odd, then g is even and there exists an integer i,* $1 \leq i < b/a$, *such that i divides* μ *and* μ *divides ir. In particular, we have* $\mu < br/a$. *If M is even, then*

$$\operatorname{ord}_2 M > \mu/b.$$

Proof. By Proposition 6, there exists an integer i, $1 \leq i < e/2$, prime to e such that

$$\operatorname{ord}_2 M + \mu = \frac{im}{e}.$$

It implies that

$$\operatorname{ord}_2 M = \frac{(ia - e)\mu + ir}{e}. \tag{3}$$

We assume that M is odd. Since i is prime to e, we deduce from the first equality that i divides μ. Equality (3) implies that

$$(e - ia)\mu = ir.$$

Hence $e > ia$ and μ divides ir. On the other hand, by Theorem 5, the order of $S(f)$ is greater than or equal to $\mu + 1$. Therefore, g must be even.

We assume that M is even. Then we have $ia > e$. Indeed, if $ia \leq e$, then, by (3), we have

$$(e - ia)\mu \leq ir - e.$$

This implies $ir \geqslant e$ and $r \geqslant a$. There is a contradiction.

Since $ia > e$, we deduce from (3) that

$$\operatorname{ord}_2 M \geq \frac{\mu + r}{e} > \frac{\mu}{b}.$$

5.2. Defect 1

We now consider the case where $|S(f)| = g \cdot 2^{\mu} M - 2^{\mu}$.

Proposition 9. *If* $m \neq 3 + 2\mu$, *then*

$$|S(f)| \neq g \cdot 2^{\mu} M - 2^{\mu}.$$

Proof. Let $b_i = \omega_i + \bar{\omega}_i$. Weil has shown that

$$|b_i| \leq 2\sqrt{q} \tag{4}$$

for $i = 1, \dots, g$. Hence, all the polynomials $t^2 + b_i t + q$ have a negative or zero discriminant.

Assume that $S(f) = g \cdot 2^\mu M - 2^\mu$. Up to a permutation, we have

$$(b_i)_{i=1,\dots,g} = \begin{cases} -2^\mu(M-1, M, \dots, M), \\ -2^\mu(M+\varepsilon_1, M+\varepsilon_2, M, \dots, M), \end{cases}$$

where $\varepsilon_1 = (-1+\sqrt{5})/2$ and $\varepsilon_2 = (-1-\sqrt{5})/2$. Hence, h is one of the following polynomials:

$$h(t) = \begin{cases} (t^2 + 2^\mu(M-1)t + q)(t^2 + 2^\mu Mt + q)^{g-1}, \\ (t^2 + 2^\mu(M+\varepsilon_1)t + q)(t^2 + 2^\mu(M+\varepsilon_2)t + q)(t^2 + 2^\mu Mt + q)^{g-2}. \end{cases}$$

Assume that $h(t) = (t^2 + 2^\mu(M-1)t + q)(t^2 + 2^\mu Mt + q)^{g-1}$. The factor $(t^2 + 2^\mu(M-1)t + q)$ must correspond to a supersingular elliptic curve over $\mathbf{F}_q$ (Theorem 2). By Proposition 3, $2^\mu(M-1)$ is equal to 0 or $\sqrt{2q}$. By Lemma 3, we have $m = 3 + 2\mu$.

We suppose that

$$h = (t^2 + 2^\mu(M+\varepsilon_1)t + q)(t^2 + 2^\mu M + \varepsilon_2)t + q)(t^2 + 2^\mu Mt + q)^{g-2}.$$

The roots of h are totally imaginary (see (4) and Proposition 5). Since $\varepsilon_1, \varepsilon_2$ are all the conjugates of ε_1, the polynomial

$$P = (t^2 + 2^\mu(M+\varepsilon_1)t + q)(t^2 + 2^\mu(M+\varepsilon_2)t + q)$$

is irreducible over $\mathbf{Q}$. This polynomial must correspond to a simple supersingular abelian variety of dimension 2 (Theorem 2). By Proposition 4, P is equal to

$$t^4 + \sqrt{2q}t^3 + qt^2 + \sqrt{2q^3}t + q.$$

Looking at the coefficients of t^3, we see that

$$2^{(m+1)/2} = 2^\mu(2M-1).$$

Such a relation is clearly impossible. There is a contradiction. This concludes the proof of the proposition. $\square$

We may note that the condition $m \neq 3 + 2\mu$ is false for only a finite number of m and a. Indeed, we have $m = 3 + 2\mu$ if and only if the couple (m, a) is in

$$\{(5,3),(7,3),(9,3),(5,4),(5,5)\}.$$

5.3. Defect 2

We examine the case where $|S(f)| = g \cdot 2^{\mu} M - 2^{\mu+1}$. If v is a real number, we denote by $\{v\}$ its fractional part.

Proposition 10. *If the following conditions are satisfied,*

(i) $m \neq 1 + 2\mu, m \neq 3 + 2\mu$,
(ii) $\mu \neq m/3$ or $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7) \approx 0.8019$,

then

$$|S(f)| \neq g \cdot 2^{\mu}\ M - 2^{\mu+1}.$$

Proof. Let $b_i = \omega_i + \bar{\omega}_i$.

Assume that $S(f) = g \cdot 2^{\mu} M - 2^{\mu+1}$. Up to a permutation, we have

$$(b_i)_{i=1,\dots,g} = \begin{cases} -2^{\mu}(M,\dots,M,M-2), \\ -2^{\mu}(M,\dots,M,M-1,M-1), \\ -2^{\mu}(M,\dots,M,M+\sqrt{2}-1,M-\sqrt{2}-1), \\ -2^{\mu}(M,\dots,M,M+\sqrt{3}-1,M-\sqrt{3}-1), \\ -2^{\mu}(M,\dots,M,M-1,M+\varepsilon_1,M+\varepsilon_2), \\ -2^{\mu}(M,\dots,M,M,M+\varepsilon_1,M+\varepsilon_2,M+\varepsilon_1,M+\varepsilon_2), \\ -2^{\mu}(M,\dots,M,M+\delta_1,M+\delta_2,M+\delta_3), \end{cases}$$

where $\delta_1 = 1 - 4\cos^2(\pi/7), \delta_2 = 1 - 4\cos^2(2\pi/7)$ and $\delta_3 = 1 - 4\cos^2(3\pi/7)$. We denote by h_j the polynomial corresponding to the jth g-uple (b_i) for $j = 1,\dots,7$. We know that h is one of these polynomials.

We note that the fifth case has been examined in the previous proof.

We assume that $h = h_6$. We have seen in the proof of Proposition 9 that

$$P = (t^2 + 2^{\mu}(M+\varepsilon_1)t + q)(t^2 + 2^{\mu}(M+\varepsilon_2)t + q)$$

Is irreducible over $\mathbf{Q}$ and is not the characteristic polynomial of the Frobenius endomorphism of a supersingular abelian variety of dimension 2. Therefore, the polynomial P^2 must correspond to a simple supersingular abelian variety of dimension 4 (Theorem 2). We expand P to get

$$P = t^4 + B_1 t^3 + B_2 t^2 + qB_1 t + q^2$$

with $B_1 = 2^{\mu}(2M - 1)$ and $B_2 = 2q + 2^{2\mu}(M^2 - M - 1)$. Xing [20] showed that if P^2 is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety of dimension 4 and if $0 < \mathrm{ord}_2 B_1 < m/2$, then m is even. One can check that $\mathrm{ord}_2(B_1) = \mu$. By assumption, we have $0 < \mathrm{ord}_2(B_1) < m/2$. There is a contradiction.

We assume that $h = h_7$. Put $P = \prod_{k=1}^{3}[t^2 + 2^{\mu}(M + \delta_k)t + q]$. The roots of P are totally imaginary (see (4) and Proposition 5). Hence, we have

$$2^{\mu}(M + 1 - 4\cos^2(3\pi/7)) < 2\sqrt{q},$$

i.e.

$$\{2^{1-\mu}\sqrt{q}\} > 1 - 4\cos^2(3\pi/7).$$

Since δ_1, δ_2, δ_3 are all the conjugates of δ_1, the polynomial P is irreducible over $\mathbf{Q}$. Hence P is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety of dimension 3 (Theorem 2). It happens if and only if $\frac{\mathrm{ord}_2\ d(0)}{m}$ is an integer for each irreducible factor $d(t)$ of P over $\mathbf{Q}_2$. We shall consider the Newton polygon of P.

The polynomial P can be written as

$$P = t^6 + B_1 t^5 + B_2 t^4 + B_3 t^3 + qB_2 t^2 + q^2 B_1 t + q^3$$

with

$$\begin{aligned} B_1 &= 2^{\mu}(3M - 2), \\ B_2 &= 3q + 2^{2\mu}(3M^2 - 4M - 1), \\ B_3 &= 2^{\mu+1}q(3M - 2) + 2^{3\mu}(M^3 - 2M^2 - M + 1). \end{aligned}$$

Since $\mu < m/2$, the point $(3, \mathrm{ord}_2\, B_3) = (3, 3\mu)$ is the only vertex (except the ones on the axis). Therefore, the polynomial P can be written as a product of two polynomials of degree 3 in $\mathbf{Q}_2$:

$$P(t) = P_1(t)P_2(t).$$

Moreover, the roots of P_1 (respectively of P_2) have μ (respectively $m - \mu$) for valuation.

We shall show that the polynomial P has no roots in $\mathbf{Q}_2$. Indeed, let x be an element of $\mathbf{Q}_2$ of valuation $m - \mu$. The terms B_3x^3, qB_2x^2, q^3 (respectively $B_3x^3, q^2B_1x^2, q^3$) have $3m$ for valuation if M is even (respectively if M is odd), whereas the terms $x^6, B_1x^5, B_2x^4, q^2B_1x^2$ (respectively $x^6, B_1x^5, B_2x^4, qB_2x^2$) have a valuation strictly greater than $3m$ if M is even (respectively if M is odd). If follows that $P(x)$ has $3m$ for valuation and so is non-zero. In a similar manner, one can prove that if x is a μ-valuation element of $\mathbf{Q}_2$, then $P(x)$ is non-zero.

Since P has no roots in $\mathbf{Q}_2$, P_1 and P_2 are the irreducible factors of P over $\mathbf{Q}_2$. Hence, P is the characteristic polynomial of the Frobenius endomorphism of a simple abelian variety of dimension 3 if and only if $\mu = m/3$ $(0<\mu<m/2)$.

We are left with cases 1, 2, 3 and 4. In the first case, it can be shown that $(t^2 + 2^\mu(M-2)t + q)$ is the characteristic polynomial of the Frobenius endomorphism of a supersingular elliptic curve if and only if $m = 1 + 2\mu$. For cases 2, 3 and 4, one can show that $(t^2 + 2^\mu(M-1)t+q)^2, (t^2 + 2^\mu(M+\sqrt{2}-1)t+q), (t^2+2^\mu(M-\sqrt{2}-1)t+q)$, $(t^2+2^\mu(M+\sqrt{3}-1)t+q)(t^2+2^\mu(M-\sqrt{3}-1)t+q)$ are the characteristic polynomials of the Frobenius endomorphisms of some supersingular abelian varieties only if $m = 3+2\mu$, $m = 1+2\mu, m = 1+2\mu$, respectively. □

We may observe that condition (i) is satisfied if and only if the couple (m, a) is not in

$$\{(3,3),(5,3),(7,3),(9,3),(5,4),(5,5)\}.$$

5.4. Summing up

We summarize our results.

Theorem 7. *Let m be an odd integer and $q = 2^m$. Let f be a polynomial over $\mathbf{F}_q$ of degree $2g+1$. Let a be the binary weight of f. We assume that $a\geqslant 3$ and $m \geq a$. We write $\mu = [m/a]$ and $M = [2^{1-\mu}\sqrt{q}]$. Let b be the greatest odd integer dividing g. We assume that the following conditions are satisfied*:

(i) $m \neq 1+2\mu, m\neq 3+2\mu$,
(ii) $\mu \neq m/3$ or $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$.

If one of the following conditions is satisfied,

(iii) *g is prime to m*,
(iv) *a divides m, M is odd and a does not divide b*,
(v) *a divides m, M is even and* $\mathrm{ord}_2 M < \mu/b$,
(vi) *a does not divide m, M is odd there does not exist an integer i, $1\leqslant i< b/a$, such that i divides μ and μ divides $i(m-a\mu)$*,
(vii) *a does not divide m, M is even and $ord_2 M \leqslant \mu/b$*,
(viii) *a does not divide m and gM is odd*,

then

$$|S(f)| \leq g\cdot 2^\mu M - 3\cdot 2^\mu.$$

Moreover, if m is not a multiple of μ *and* gM *is even, then*

$$|S(f)| \leq g \cdot 2^{\mu} M - 4 \cdot 2^{\mu}.$$

Proof. The first assertion follows immediately from Propositions 6–8. For the second assertion, it is enough to observe that, by Theorem 5,

$$\mathrm{ord}_2\, S(f) \geq \mu + 1$$

if m is not a multiple of μ. $\square$

6. Examples

In this section, we assume that condition (i) of Theorem 7 is satisfied.

We assume that f is a polynomial of degree $2^a + 1, a \geqslant 3$. Note that $g = 2^{a-1}$ and $b = 1$. Suppose that if $a = 3$, then m is not a multiple of 3. Condition (ii) of Theorem 7 is satisfied. Hence

$$|S(f)| \leq 2^{\mu+a-1} M - 3 \cdot 2^{\mu},$$

and if m is not a multiple of 3,

$$|S(f)| \leq 2^{\mu+a-1}\ M - 4 \cdot 2^{\mu}.$$

We will consider in more detail those cases in which f is a polynomial of degree 7, 9, 11, 13.

First, let us suppose that m is a multiple of 3. Let $m = 3\mu$.

We assume that f is a polynomial of degree 7. If $|S(f)| = 3 \cdot 2^{\mu} M$, then J is a simple abelian variety ($e = g = 3$) and, by Proposition 6, M is odd. We are aware that such a situation occurs for small values of μ. More precisely, $|S(x^7)| = 3 \cdot 2^{\mu} M$, for $\mu = 3$, 5,13. On the other hand, if M is even and $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$, then

$$|S(f)| \leq 3 \cdot 2^{\mu}\ M - 3 \cdot 2^{\mu}.$$

If f is a polynomial of degree 9 and $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$, then

$$|S(f)| \leq 4 \cdot 2^{\mu}\ M - 3 \cdot 2^{\mu}.$$

If $\mu = 5$, we have $q = 2^{15}$ and $M = 11$. In this case, the above bound is reached; we have

$$S(x^9 + x^7) = 4 \cdot 2^{\mu} M - 3 \cdot 2^{\mu} = 1312.$$

A strengthened result can be obtained. By Propositions 6 and 9, we may assume that $S(f) = 4 \cdot 2^{\mu} M - 2^{\mu+1}$. We use the same notations as in the proof of Proposition 10.

By this proof, the characteristic polynomial of the Frobenius endomorphism of the Jacobian of the curve $y^2 + y = f(x)$ over $\mathbf{F}_q$ is equal to

$$(t^2 + 2^{\mu} M t + q) \prod_{k=1}^{3} [t^2 + 2^{\mu}(M + \delta_k)t + q].$$

We have only studied the factor $\prod_{k=1}^{3} [t^2 + 2^{\mu}(M + \delta_k)t + q]$. But the polynomial $t^2 + 2^{\mu} M t + q$ must be the characteristic polynomial of the Frobenius endomorphism of a supersingular elliptic curve over $\mathbf{F}_q$. It is so if and only if $m = 2\mu + 1$. Now we have supposed that $m \neq 2\mu + 1$, therefore

$$|S(f)| \leq 4 \cdot 2^{\mu} M - 3 \cdot 2^{\mu}$$

without assuming $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$.

We assume that f is a polynomial of degree 11. If $|S(f)| = 5 \cdot 2^{\mu} M$, then J is a simple abelian variety of dimension 5. By Proposition 6, 5 divided μ and

$$\operatorname{ord}_2 M = 3i\mu/5 - \mu$$

with $i = 1$ or 2. From this equality, we deduce that $\operatorname{ord}_2 M = \mu/5$. If $\operatorname{ord}_2 M \neq \mu/5$ and $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$, we have

$$|S(f)| \leq 5 \cdot 2^{\mu} M - 3 \cdot 2^{\mu}.$$

As in the case of a polynomial of degree 9, it can be shown that this inequality remains true if the condition $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$ is not satisfied.

We assume that f is a polynomial of degree 13. Suppose that $|S(f)| = 6 \cdot 2^{\mu} M$. Since $g = 2b = 2 \cdot 3$ and m is odd, J is isogenous to the square of a simple abelian variety of dimension 3. We come down to the case of degree 7. If M is even and $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$, then

$$|S(f)| \leq 6 \cdot 2^{\mu} M - 3 \cdot 2^{\mu}.$$

In this case, one can also see that the condition $\{2^{1-\mu}\sqrt{q}\} \leq 1 - 4\cos^2(3\pi/7)$ is unnecessary.

Assume that m is not a multiple of 3. In the same way, we can show the following results. If f is a polynomial of degree 7, 9 or 13, then

$$|S(f)| \leq (\deg f - 1) \cdot 2^{\mu-1} M - 3 \cdot 2^{\mu}.$$

Appendix

Tables 1–4 give the Serre–Weil bound, the Moreno–Moreno bound and the results obtained in Section 6. A star denotes that the bound is reached.

Table 1
Degree 7

μ	$m = 3\mu$	$M = [2^{1-\mu}\sqrt{q}]$	$3 \cdot [2\sqrt{q}]$	$3 \cdot 2^{\mu} M$	Section 6
3	9	5	135	120*	120*
5	15	11	1086	1056*	1056*
7	21	22	8688	8448	8064
9	27	45	69,510	69,120	69,120
11	33	90	556,089	552,960	546,816
13	39	181	4,448,730	4,448,256*	4,448,256*
15	45	362	35,589,849	35,586,048	35,487,744

Table 2
Degree 9

μ	$m = 3\mu$	$M = [2^{1-\mu}\sqrt{q}]$	$4 \cdot [2\sqrt{q}]$	$4 \cdot 2^{\mu} M$	Section 6
3	9	5	180	160	152
5	15	11	1448	1408	1312*
7	21	22	11,584	11,264	10,880
9	27	45	92,680	92,160	90,624
11	33	90	741,452	737,280	731,136
13	39	181	5,931,640	5,931,008	5,906,432
15	45	362	47,453,132	47,448,064	47,349,760

Table 3
Degree 11

μ	$m = 3\mu$	$M = [2^{1-\mu}\sqrt{q}]$	$5 \cdot [2\sqrt{q}]$	$5 \cdot 2^{\mu} M$	Section 6
3	9	5	225	200	192
5	15	11	1810	1760	1664
7	21	22	14,480	14,080	13,696
9	27	45	115,850	115,200	113,664
11	33	90	926,815	921,600	915,456
13	39	181	7,414,550	7,413,760	7,389,184
15	45	362	59,316,415	59,310,080	59,211,776

Table 4
Degree 13

μ	$m = 3\mu$	$M = [2^{1-\mu}\sqrt{q}]$	$6 \cdot [2\sqrt{q}]$	$6 \cdot 2^{\mu} M$	Section 6
3	9	5	270	240	240
5	15	11	2172	2112	2112
7	21	22	17,376	16,896	16,512
9	27	45	139,020	138,240	138,240
11	33	90	1,112,178	1,105,920	1,099,776
13	39	181	8,897,460	8,896,512	8,896,512
15	45	362	71,179,698	71,172,096	71,073,792

References

[1] J. Ax, Zeroes of polynomials over finite fields, Amer. J. Math. 86 (1964) 255–261.
[2] A. Cáceres, O. Moreno, On the estimation of minimum distance of duals of BCH codes, Congr. Numer. 81 (1991) 205–208.
[3] T. Honda, Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Japan 20 (1968) 83–95.
[4] N. Koblitz, p-Adic Numbers, p-Adic Analysis, and Zeta-Functions, 2nd Edition, Springer, New York, 1984.
[5] K. Lauter, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, Institut de Mathématiques de Luminy, preprint, 1999, pp. 99–29.
[6] K.-Z. Li, F. Oort, Moduli of Supersingular Abelian Varieties, Springer, Berlin, 1998.
[7] S. Litsyn, C.J. Moreno, O. Moreno, Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables, Appl. Algebra Eng. Comm. Comput. 5 (1994) 105–116.
[8] F.J. MacWilliams, N.J.A. Sloane, in: The Theory of Error-Correcting Codes. II, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam, 1977.
[9] O. Moreno, C.J. Moreno, The MacWilliams–Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes, IEEE Trans. Inform. Theory 40 (1994) 1894–1907.
[10] O. Moreno, C.J. Moreno, A p-adic Serre bound, Finite Fields Appl. 4 (1998) 201–217.
[11] F. Rodier, Minoration de certaines sommes exponentielles binaires, Coding Theory and Algebraic Geometry, Luminy, 1991, Springer, Berlin, 1992, pp. 199–209.
[12] M. Rosen, The asymptotic behavior of the class group of a function field over a finite field, Arch. Math. (Basel) 24 (1973) 287–296.
[13] J.-P. Serre, Local class field theory, Algebraic Number Theory, Proceedings of Instructional Conference, Brighton, 1965, Thompson, Washington, DC, 1967, pp. 128–161.
[14] J.-P. Serre, Rational Points on Curves over Finite Fields, Notes by F. Gouvêa of Lectures at Harvard University, 1985.
[15] J.-P. Serre, Résumé des cours de 1983–1984, Oeuvres, Vol. III, 1986.
[16] C. Smyth, Totally positive algebraic integers of small trace, Ann. Inst. Fourier (Grenoble) 34 (1984) 1–28.
[17] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.
[18] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), Sém. Bourbaki 352 (1968/1969).
[19] W.C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. (4) 2 (1969) 521–560.
[20] C. Xing, The characteristic polynomials of abelian varieties of dimensions three and four over finite fields, Sci. China Ser. A. 37 (1994) 147–150.
[21] C. Xing, On supersingular abelian varieties of dimension two over finite fields, Finite Fields Appl. 2 (1996) 407–421.