Advances in Mathematics 309 (2017) 238–253

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

# An improvement to the Hasse–Weil bound and applications to character sums, cryptography and coding

Ronald Cramer [a], Chaoping Xing [b,*]

[a] CWI, Amsterdam & Mathematical Institute, Leiden University, The Netherlands
[b] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

*Article history:*
Received 5 September 2015
Received in revised form 1 September 2016
Accepted 17 January 2017
Communicated by Michel Van den Bergh

*MSC:*
11G20
11G10
11T23
94B05

*Keywords:*
Points
Algebraic curves
Abelian varities
Zeta function
Character sum
Codes
Nonlinearity

ABSTRACT

The Hasse–Weil bound is a deep result in mathematics and has found wide applications in mathematics, theoretical computer science, information theory etc. In general, the bound is tight and cannot be improved. However, for some special families of curves the bound could be improved substantially. In this paper, we focus on the Hasse–Weil bound for the curve defined by $y^p - y = f(x)$ over the finite field $\mathbb{F}_q$, where $p$ is the characteristic of $\mathbb{F}_q$. In 1993, Moreno–Moreno [7] gave an improvement to the Hasse–Weil bound for this family of curves. Recently, Kaufman and Lovett [4, FOCS2011] showed that the Hasse–Weil bound can be improved for this family of curves with $f(x) = g(x) + h(x)$, where $g(x)$ is a polynomial of degree $\ll \sqrt{q}$ and $h(x)$ is a sparse polynomial of arbitrary degree but bounded weight degree. The other recent improvement by Rojas-Leon and Wan [9, Math. Ann. 2011] shows that an extra $\sqrt{p}$ can be removed for this family of curves if $p$ is very large compared with polynomial degree of $f(x)$ and $\log_p q$.

In this paper, we focus on the most interesting case for applications, namely $p = 2$. We show that the Hasse–Weil bound for this special family of curves can be improved if $q = 2^n$ with odd $n \geqslant 3$ which is the same case where Serre [10] improved the Hasse–Weil bound. However, our improvement is greater than Serre's and Moreno–Morenao's

* Corresponding author.
*E-mail addresses:* ronald.cramer@cwi.nl (R. Cramer), xingcp@ntu.edu.sg (C. Xing).

http://dx.doi.org/10.1016/j.aim.2017.01.011
0001-8708/© 2017 Elsevier Inc. All rights reserved.

improvements for this special family of curves. Furthermore, our improvement works for $p = 2$ compared with the requirement of large $p$ by Rojas-Leon and Wan. In addition, our improvement finds interesting applications to character sums, cryptography and coding theory. The key idea behind is that this curve has the Hasse–Witt invariant 0 and we show that the Hasse–Weil bound can be improved for any curves with the Hasse–Witt invariant 0. The main tool used in our proof involves Newton polygon and some results in algebraic geometry.

© 2017 Elsevier Inc. All rights reserved.

## 1. Introduction

Let $\chi$ be a nontrivial additive character from $\mathbb{F}_q$ to the nonzero complex $\mathbb{C}^*$. The Weil bound for character sums states that, when the degree $m$ of a polynomial $f(x)$ is co-prime with $q$, then $|\mathbb{E}_{x\in\mathbb{F}_q}(\chi(f(x)))| \leqslant (m-1)/\sqrt{q}$. The Weil bound for character sums can be derived from the Hasse–Weil bound of a special family of algebraic curves, i.e., $y^p - y = f(x)$, where $p$ is the characteristic of $\mathbb{F}_q$. Therefore, any improvement on the Hasse–Weil bound of this family could lead to an improvement on the Weil bound for character sums. The Hasse–Weil bound is a deep result in mathematics and has found wide applications in mathematics, theoretical computer science, information theory etc. In general, the bound is tight and cannot be improved. However, in some special cases the bound could be improved substantially. For instance, when the ground filed size $q$ is small, the bound could be improved up to half of it. There have been various improvements on the Hasse–Weil bound. One of the most famous improvements is the Weil–Serre bound [10]. In 1993, Moreno–Moreno [7] gave an improvement to the Hasse–Weil bound for this family of curves. Recently, Kaufman and Lovett [4, FOCS2011] showed that the Weil bound for character sums can be improved for $f(x) = g(x) + h(x)$, where $g(x)$ is a polynomial of degree $\ll \sqrt{q}$ and $h(x)$ is a sparse polynomial of arbitrary degree but bounded weight degree. The other recent improvement by Rojas-Leon and Wan [9, Math. Ann. 2011] shows that an extra $\sqrt{p}$ can be removed if $p$ is very large compared with polynomial degree $m$ of $f(x)$ and $\log_p q$.

### 1.1. Our result

From now on in this paper, we assume that $q = 2^n$ for an odd integer $n \geqslant 3$. Consider the trace map Tr from $\mathbb{F}_q$ to $\mathbb{F}_2$ defined by $\alpha \mapsto \sum_{i=0}^{n-1} \alpha^{2^i}$. It is easy to see that $\mathrm{Tr}(\alpha^{2t}) = \mathrm{Tr}(\alpha^t)$. This implies that, for a polynomial $f(x) \in \mathbb{F}_q[x]$, one can find a polynomial $g(x) = \sum_{i=0}^{m} g_i x^i \in \mathbb{F}_q[x]$ such that $g_i$ are zero whenever $i \equiv 0 \bmod 2$ and $\mathrm{Tr}(f(\alpha)) = \mathrm{Tr}(g(\alpha))$. Thus, we only consider those polynomials with nonzero term $x^i$, where $\gcd(i, 2) = 1$.

Now let $f(x)$ be a polynomial of degree $m \geqslant 1$ over $\mathbb{F}_q$. Without loss of generality, we may assume that $\gcd(m, 2) = 1$. We consider the cardinality of the set

$$Z_f := \{\alpha \in \mathbb{F}_q : \ \mathrm{Tr}(f(\alpha)) = 0\}. \tag{1}$$

Then the Weil bound shows that

$$\left||Z_f| - \frac{q}{2}\right| \leqslant \frac{(m-1)\sqrt{q}}{2}. \tag{2}$$

The main result of this paper is given below.

**Theorem 1.1** *(MAIN RESULT). Let $g = (m-1)/2$ with $m \geqslant 3$, then one has*

$$\left||Z_f| - \frac{q}{2}\right| \leqslant \begin{cases} 2^{\lceil n/g \rceil - 1} \left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{\lceil n/g \rceil}} \right\rfloor & \text{if } g > 1 \\ 2^{(n-1)/2} \left\lfloor \frac{\lfloor 2\sqrt{q} \rfloor}{2^{(n+1)/2}} \right\rfloor & \text{if } g = 1. \end{cases} \tag{3}$$

One could not see how largely the bound (2) is improved in Theorem 1.1. Essentially, the bound (3) tells that the number $|Z_f| - \frac{q}{2}$ is divisible by $2^{\lceil n/g \rceil}$. We refer to Example 2.2, Sections 2.3 and 2.4 for numerical illustration.

### *1.2. Our technique*

Our technique for the improvement is through $L$-polynomials of algebraic curves with the Hasse–Witt invariant equal to 0. More precisely speaking, we show the improvement through two steps: (i) prove that the Hasse–Weil bound for the algebraic curve with the Hasse–Witt invariant 0 can be improved; (ii) show by the Deuring–Shafarevich Theorem that the curve $y^2 - y = f(x)$ has the Hasse–Witt invariant 0. Consequently, we obtain an improvement on the Weil bound for character sums.

Among the above three steps, the critical one is to show an improvement on the Hasse–Weil bound for the algebraic curve with the Hasse–Witt invariant 0. In order to achieve this, we analyze the Newton polygon of the characteristic polynomial of an abelian variety with Hasse–Witt invariant 0. Then we employ some fundamental results on factorization of the characteristic polynomial to obtain the desired result.

### *1.3. Comparison*

We mainly compare our improvement with those by Serre [10], Moreno–Moreno [7], Kaufman–Lovett [4, FOCS2011] and Rojas-Leon–Wan [9, Math. Ann. 2011].

The improvement by Serre applies to arbitrary algebraic curve over $\mathbb{F}_{2^n}$ with odd $n$, while our improvement only applies to the curve $y^2 - y = f(x)$ over $\mathbb{F}_{2^n}$ with odd $n$. On the other hand, our improvement is even greater than the one by Serre for this special family of curves. The method by Serre mainly employs some properties of algebraic numbers.

The improvement by Moreno and Moreno shows that $|Z_f| - \frac{q}{2}$ is divisible by $2^{\lceil n/m \rceil}$, while our result in fact shows that $|Z_f| - \frac{q}{2}$ is divisible by $2^{\lceil 2n/(m-1) \rceil}$. This leads to a better improvement.

The improvement by Kaufman and Lovett works for those polynomials with degree bigger than $\sqrt{q}$. Thus, the scenario is different. The main idea by Kaufman–Lovett uses the Deligne Theorem on multivariate polynomials.

The improvement by Rojas-Leon and Wan shows that, for number of points on the curve $y^p - y = f(x)$ over $\mathbb{F}_{p^n}$ with $f(x) \in \mathbb{F}_p[x]$, an extra $\sqrt{p}$ can be removed if $p$ is very large compared with polynomial degree $m$ of $f(x)$ and $n$. However, our improvement works for characteristic 2 which is not applicable in [9]. The idea of Rojas-Leon and Wan involves moment $L$-functions and Katz's work on $\ell$-adic monodromy calculations.

### *1.4. Organization*

Section 2 presents the main result and some applications to character sum, cryptography and coding theory. We also show that the Weil bound for character sums can be derived from the Hasse–Weil bound for $y^2 - y = f(x)$ in Section 2. We present the proof of the main result in Section 3 by adopting some results on the Newton polygon and abelian varieties.

## 2. Main result and applications

### *2.1. Main result*

The Hasse–Weil bound [15] provides an upper bound on the number of points of an algebraic curve over a finite field $\mathbb{F}_q$ in terms of its genus and the ground field size $q$. The bound was improved by Serre [10] when $q$ is not a square. The refined bound by Serre is now called the Weil–Serre bound. In this section, we show that the Weil–Serre bound can be further improved for a class of curves arising from trace when $q$ is not a square. Furthermore, several applications are provided for this improvement.

It is a well-known fact that the cardinality of $Z_f$ in (1) is equal to $(N_f - 1)/2$, where $N_f$ stands for the number of the $\mathbb{F}_q$-rational points on the Artin–Schreier type curve defined by

$$\mathcal{X}_f : \quad y^2 - y = f(x). \tag{4}$$

Note that the set of the $\mathbb{F}_q$-rational points on $\mathcal{X}_f$ is $\{P_\infty\} \cup \{(\alpha, \beta) \in \mathbb{F}_q^2 : \ \beta^2 - \beta = f(\alpha)\}$, where $P_\infty$ stands for the "points at infinity".

To see this, we note that $P_\infty$ can be discarded towards counting the cardinality of $Z_f$. Furthermore, an element $\alpha$ belongs to $Z_f$ if and only if there are 2 elements $\beta \in \mathbb{F}_q$ such that $(\alpha, \beta)$ are solutions of the equation (4).

When applying the Weil bound [15] to the curve $\mathcal{X}_f$, we have

$$|N_f - q - 1| \leqslant 2g\sqrt{q}, \tag{5}$$

where $g = (m-1)/2$ is the *genus* of $\mathcal{X}_f$. Serre [10] improved the above bound to the following Weil–Serre bound

$$|N_f - q - 1| \leqslant g\lfloor 2\sqrt{q} \rfloor. \tag{6}$$

It seems that the bound (6) is just a small improvement on the Weil bound. However, the improvement could be big if $m$ gets large. For instance, $q = 32$ and $m = 2001$, then the Weil bound gives $|N_f - q - 1| \leqslant 11{,}313$, while the Weil–Serre bound gives $|N_f - q - 1| \leqslant 11{,}000$.

Applying the Weil–Serre bound, we get the following bound on the cardinality $|Z_f|$

$$\left| |Z_f| - \frac{q}{2} \right| \leqslant \frac{g\lfloor 2\sqrt{q} \rfloor}{2}. \tag{7}$$

In this paper, we show that the bound (7) can be further improved. We repeat the main result of this paper that improves the above bound (7) as follows.

**Theorem 2.1** *(MAIN RESULT). Let $g = (m-1)/2$, then one has*

$$\left| |Z_f| - \frac{q}{2} \right| \leqslant \begin{cases} 2^{\lceil n/g \rceil - 1} \left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{\lceil n/g \rceil}} \right\rfloor & \text{if } g > 1 \\ 2^{(n-1)/2} \left\lfloor \frac{\lfloor 2\sqrt{q} \rfloor}{2^{(n+1)/2}} \right\rfloor & \text{if } g = 1. \end{cases} \tag{8}$$

The proof of Theorem 2.1 involves algebraic geometry and algebraic number theory and we leave the proof to the next section.

From the formula of (8), one cannot see the big difference between the Weil–Serre bound (7) and our bound (8). Let us use some examples to illustrate improvement.

**Example 2.2.**

(i) Let $q = 2^7 = 128$ and $m = \deg(f) = 5$, then the Weil–Serre bound (7) gives $||Z_f| - 64| \leqslant 22$, while the bound (8) gives $||Z_f| - 64| \leqslant 16$.

(ii) Now, we look at an example of relatively large parameters. Let $q = 2^{21}$ and $m = \deg(f) = 5$, then the Weil–Serre bound (7) gives $\left||Z_f| - 2^{20}\right| \leqslant 2896$, while the bound (8) gives $\left||Z_f| - 2^{20}\right| \leqslant 2048$.

From Example 2.2(iii), we can see that, for some parameters, there could be a big difference between the Weil–Serre bound (7) and our bound (8).

*2.2. Improvement on the Weil bound for character sum*

It is well known that every nontrivial additive character from $\mathbb{F}_q$ to $\mathbb{C}^*$ can be represented by $\chi_\beta(x) := \exp(2\pi i \mathrm{Tr}(\beta x)/2) = (-1)^{\mathrm{Tr}(\beta x)}$ for some $\beta \in \mathbb{F}_q^*$ (see [5]). Let $f(x)$ be a polynomial of degree $m$ over $\mathbb{F}_q$ with $\gcd(m, 2) = 1$ and put $g = (m-1)/2$. Then $\chi_\beta(f(x))$ is uniformly distributed when $\sqrt{q} \gg m$. More precisely speaking, the Weil bound gives the following bound on the expectation of $\chi_\beta(f(x))$:

$$|\mathbb{E}_{x\in\mathbb{F}_q}(\chi_\beta(f(x)))| = \left|\frac{1}{q}\sum_{\alpha\in\mathbb{F}_q}\chi_\beta(f(\alpha))\right| \leqslant \frac{m-1}{\sqrt{q}}. \tag{9}$$

Furthermore, applying the Weil–Serre bound (7) gives

$$|\mathbb{E}_{x\in\mathbb{F}_q}(\chi_\beta(f(x)))| \leqslant \frac{g\lfloor 2\sqrt{q}\rfloor}{q}. \tag{10}$$

Note that the expectation of $\chi_\beta(f(x))$ satisfies

$$\mathbb{E}_{x\in\mathbb{F}_q}(\chi_\beta(f(x))) = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q}\chi_\beta(f(\alpha)) = \sum_{a\in\mathbb{F}_2}\frac{M_{\beta f}(a)}{q}(-1)^a = \frac{1}{q}(2M_{\beta f}(0) - q) \tag{11}$$

with $M_{\beta f}(a)$ being the cardinality of the set $\{\alpha \in \mathbb{F}_q : \ \mathrm{Tr}(\beta f(\alpha)) = a\}$ and hence $M_{\beta f}(0) = |Z_{\beta f}|$. Now we apply the bound (8) to get an improvement to the bound (10).

**Theorem 2.3.** *Let $g = (m-1)/2$, then one has*

$$|\mathbb{E}_{\alpha\in\mathbb{F}_q}(\chi_\beta(f(\alpha)))| \leqslant \begin{cases} 2^{\lceil n/g\rceil - n}\left\lfloor \frac{g\lfloor 2\sqrt{q}\rfloor}{2^{\lceil n/g\rceil}}\right\rfloor & \text{if } g > 1, \\ 2^{(n+1)/2-n}\left\lfloor \frac{\lfloor 2\sqrt{q}\rfloor}{2^{(n+1)/2}}\right\rfloor & \text{if } g = 1 \end{cases} \tag{12}$$

*for any nonzero element $\beta \in \mathbb{F}_q$.*

**Proof.** By (11), we have

$$|\mathbb{E}_{x\in\mathbb{F}_q}(\chi_\beta(f(x)))| = \left|\frac{1}{q}(2M_{\beta f}(0) - q)\right| = \frac{2}{q}\left||Z_{\beta f}| - \frac{q}{2}\right|.$$

The desired result follows from Theorem 2.1. □

We illustrate our improvement by considering some small examples.

**Example 2.4.** Let us consider character sums for polynomials of degree 3 and 5, respectively.

(i) Let $q = 2^n$ with odd $n$ and let $f(x)$ be a polynomial of degree 3. By Theorem 2.3, for any nontrivial additive character $\chi$ from $\mathbb{F}_{2^n}$ to $\mathbb{C}^*$, one has $\left|\sum_{\alpha\in\mathbb{F}_q}\chi(f(\alpha))\right| \leqslant 2^{(n+1)/2}$. The Weil bound (9) gives an upper bound $2^{(n+2)/2}$, while the Weil–Serre bound (10) gives an upper bound between $2^{(n+1)/2}$ and $2^{(n+2)/2}$.

(ii) Let $q = 2^n$ with odd $n$ and let $f(x)$ be a polynomial of degree 5. By Theorem 2.3, for any nontrivial additive character $\chi$ from $\mathbb{F}_{2^n}$ to $\mathbb{C}^*$, one has $\left|\sum_{\alpha\in\mathbb{F}_q}\chi(f(\alpha))\right| \leqslant 2^{(n+3)/2}$. The Weil bound (9) gives an upper bound $2^{(n+4)/2}$, while the Weil–Serre bound (10) gives an upper bound between $2^{(n+3)/2}$ and $2^{(n+4)/2}$.

### *2.3. Application to cryptography*

In streamcipher, nonlinearity of a function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is an important measure [1]. The nonlinearity of a function $f(x)$ is defined as follows.

The Walsh transfer $W_f$ of $f(x)$ is defined by

$$W_f: \quad \mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\to\mathbb{C}; \qquad (a,b)\mapsto \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(af(x)+bx)}. \tag{13}$$

Then the Walsh spectrum of $f$ is the image set $\{W_f(a,b): \ a\in\mathbb{F}_{2^n}^*, \ b\in\mathbb{F}_{2^n}\}$. The nonlinearity, denoted by $\mathrm{NL}(f)$, of $f(x)$ is defined by

$$\mathrm{NL}(f) := 2^{n-1} - \frac{1}{2}\max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}}|W_f(a,b)|. \tag{14}$$

In fact, the Walsh transformation $W_f(a,b)$ is nothing but $2^n$ times the expectation of $\chi_1(af(x)+bx)$, i.e., $W_f(a,b) = 2^n\mathbb{E}_{x\in\mathbb{F}_{2^n}}(\chi_1(af(x)+bx))$. Thus, the nonlinearity $\mathrm{NL}(f)$ of $f(x)$ can be expressed in terms of the expectation of $\chi_1(af(x)+bx)$, i.e.,

$$\mathrm{NL}(f) = 2^{n-1} - 2^{n-1}\max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}}|\mathbb{E}_{x\in\mathbb{F}_{2^n}}(\chi_1(af(x)+bx))|. \tag{15}$$

For an odd $n$, it can be proved that $\mathrm{NL}(f)$ is upper-bounded by a number between $2^{n-1}-2^{(n-1)/2}$ and $2^{n-1}-2^{n/2-1}$ [1]. The value $2^{n-1}-2^{(n-1)/2}$ is called the quadratic bound because such nonlinearity can be achieved by quadratic polynomials [1]. If $\deg(f)=3$, i.e., the curves defined in (4) is an elliptic curve, then by Theorem 2.1 one has

$$\begin{aligned}\mathrm{NL}(f) &= 2^{n-1} - 2^{n-1}\max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}}|\mathbb{E}_{x\in\mathbb{F}_{2^n}}(\chi_1(af(x)+bx))|\\ &\geqslant 2^{n-1} - 2^{(n-1)/2}\left\lfloor\frac{\lfloor 2^{(n+2)/2}\rfloor}{2^{(n+1)/2}}\right\rfloor = 2^{n-1}-2^{(n-1)/2}.\end{aligned}$$

Hence, polynomials of degree 3 achieve the quadratic bound of nonlinearity. Previously, polynomials of degree 3 are usual candidates for functions with high nonlinearity. Now let us look at polynomials $f$ of degree 5. By Theorem 2.1, we have

$$\begin{aligned}\mathrm{NL}(f) &= 2^{n-1} - 2^{n-1} \max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} |\mathbb{E}_{x\in\mathbb{F}_{2^n}}(\chi_1(af(x)+bx))| \\ &\geqslant 2^{n-1} - 2^{(n-1)/2-1}\left\lfloor \frac{2\lfloor 2^{(n+2)/2}\rfloor}{2^{(n+1)/2}}\right\rfloor = 2^{n-1} - 2^{(n-1)/2}.\end{aligned}$$

Thus, polynomials of degree 5 also achieve the quadratic bound of nonlinearity. This enlarges the pool of functions with very high nonlinearity when people search for functions of large nonlinearity together with other cryptographic properties such as algebraic degree, algebraic immunity, etc. [1].

### *2.4. Application to coding*

Many codes such as BCH codes, classical Goppa codes and Reed–Muller codes can be realized as trace codes. In fact, every cyclic code can be represented as a trace code in a natural way [17].

Let $\mathcal{P} := \{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ be a subset of $\mathbb{F}_q$ of cardinality $N$. For a polynomial $f(x) \in \mathbb{F}_q[x]$, we denote by $\mathrm{Tr}_{\mathcal{P}}(f)$ the vector $(\mathrm{Tr}(f(\alpha_1)), \mathrm{Tr}(f(\alpha_2)), \ldots, \mathrm{Tr}(f(\alpha_N)))$. For an $\mathbb{F}_2$-subspace $V$ of $\mathbb{F}_q[x]$, we denote by $\mathrm{Tr}_{\mathcal{P}}(V)$ the trace code $\{\mathrm{Tr}_{\mathcal{P}}(f) : f \in V\}$. Let us warm up by looking at a small example first.

**Example 2.5.** Consider the binary code $\mathrm{Tr}_{\mathcal{P}}(V)$, where $\mathcal{P}$ consists of all elements in $\mathbb{F}_{128}$, and $V = \{f(x) \in \mathbb{F}_{128}[x] : \deg(f) \leqslant 5\}$. Given the fact that $\mathrm{Tr}_{\mathcal{P}}(x) = \mathrm{Tr}_{\mathcal{P}}(x^2) = \mathrm{Tr}_{\mathcal{P}}(x^4)$, it is easy to see that $\mathrm{Tr}_{\mathcal{P}}(V)$ has a basis $\{(1,1,\ldots,1)\} \cup \{\mathrm{Tr}_{\mathcal{P}}(\alpha_i x^j)\}_{1\leqslant i\leqslant 7, j=1,3,5}$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_7\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_{128}$. Thus, $\mathrm{Tr}_{\mathcal{P}}(V)$ is a binary $[128, 22]$-linear code. To see the minimum distance, let $f$ be a nonzero polynomial of degree $m$ with $m \leqslant 5$ and $\gcd(m, 2) = 1$. By the Weil–Serre bound (7), we know that the number of zeros of $\mathrm{Tr}_{\mathcal{P}}(f)$ can be at most $64 + 22 = 86$, thus we get a lower bound on minimum distance, i.e., $d \geqslant 128 - 86 = 42$. However, by our bound in Theorem 2.1, we get a lower bound $d \geqslant 128 - (64 + 16) = 48$. This achieves the best-known bound [2]. In fact, the software *Magma* verifies that this code indeed has minimum distance 48. In other words, our bound (8) is tight in this case.

Next we study dual codes of primitive BCH codes.

**Example 2.6.** Let $\alpha$ be a primitive element of $\mathbb{F}_q$ and let $\mathrm{BCH}(t)$ be a $t$-error correcting binary BCH code of length $N = q-1 = 2^n-1$. Then by Delsarte's Theorem [6], the dual $\mathrm{BCH}(t)^\perp$ can be represented as the trace code $\mathrm{Tr}_{\mathcal{P}}(V)$ [13], where $\mathcal{P}$ consists of all $q-1$ nonzero elements of $\mathbb{F}_q$, and $V$ is the $\mathbb{F}_q$-vector space generated by $\{1, x, x^2, \ldots, x^t\}$. If $i$ is divisible by 2, then $\mathrm{Tr}_{\mathcal{P}}(x^i) = \mathrm{Tr}_{\mathcal{P}}(x^{i/2})$. Thus, $\mathrm{BCH}(t)^\perp$ is generated by $\{(1,1,\ldots,1)\} \cup \{\mathrm{Tr}_{\mathcal{P}}(\alpha_i x^j) : 1 \leqslant j \leqslant t,\ 2 \nmid j,\ 1 \leqslant i \leqslant n\}$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_q$. Hence, the dimension of $\mathrm{BCH}(t)^\perp$ is at most $1 + n(t - \lfloor t/2\rfloor)$. On the other hand, if $t < \sqrt{q}$, then by the Weil–Serre bound (7), $\mathrm{Tr}_{\mathcal{P}}(f) \neq 0$ for any $f \in V \setminus \{0\}$ with $\gcd(\deg(f), 2) = 1$. This implies that the dimension of $\mathrm{BCH}(t)^\perp$ is exactly $1+n(t-\lfloor t/2\rfloor)$

for $t < \sqrt{q}$. By the bound (8), we obtain a lower bound on minimum distance of $\mathrm{BCH}(t)^{\perp}$, namely

$$d\left(\mathrm{BCH}(t)^{\perp}\right) \geqslant \begin{cases} 2^n - 1 - 2^{n-1} - 2^{\lceil n/g \rceil - 1}\left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{\lceil n/g \rceil}} \right\rfloor & \text{if } g > 1 \\ 2^n - 1 - 2^{n-1} - 2^{\lceil (n-1)/2 \rceil}\left\lfloor \frac{\lfloor 2\sqrt{q} \rfloor}{2^{(n+1)/2}} \right\rfloor & \text{if } g = 1, \end{cases} \tag{16}$$

where $g = (t-1)/2$ if $2 \nmid t$ and $g = (t-2)/2$ if $2|t$.

Let us illustrate the parameters of our code by looking at some numerical results. Taking $t = 4$ and $n = 5$, we get a binary $[31, 11, \geqslant 11]$-linear code. This is a best possible code in the sense that for given length 31 and dimension 11, the minimum distance can not be improved [2].

If $t = 4$ and $n = 7$, then we get a binary $[127, 15, \geqslant 55]$-linear code. It is a best-known code [2].

**Example 2.7.** In this example, we consider the duals of classical Goppa codes. Let $q = 2^n$ and let $L = \mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$. Let $g(x)$ be a polynomial of degree $t$ with $\gcd(t, 2) = 1$ and $g(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, q$. Then the classical Goppa code $\Gamma(L, g)$ defined by

$$\Gamma(L, g) = \left\{ (c_1, c_2, \ldots, c_q) \in \mathbb{F}_2^n : \sum_{i=1}^{q} \frac{c_i}{x - \alpha_i} \equiv 0 \bmod g(x) \right\}$$

is a binary linear code of length $q = 2^n$. By Delsarte's Theorem [6], the dual $\Gamma(L, g)^{\perp}$ can be represented as the trace code $\{(\mathrm{Tr}(v_1 f(\alpha_1)), (\mathrm{Tr}(v_1 f(\alpha_1)), \ldots, (\mathrm{Tr}(v_1 f(\alpha_q))) : f \in \mathbb{F}_q[x],\ \deg(f) \leqslant t-1\}$, where $v_i = g(\alpha_i)$ [13]. It is clear that $\Gamma(L, g)^{\perp}$ is equivalent to $\mathrm{Tr}_{\mathcal{P}}(V)$, where $\mathcal{P}$ consists of all $q$ elements of $\mathbb{F}_q$, and $V$ is the $\mathbb{F}_q$-vector space generated by $\{1, x, x^2, \ldots, x^{t-1}\}$. In the same way, we have that the dimension of $\Gamma(L, g)^{\perp}$ is exactly $1 + n(t - \lfloor (t-1)/2 \rfloor)$ for $t < \sqrt{q}$. By the bound (8), we obtain a lower bound on minimum distance of $\Gamma(L, g)^{\perp}$, namely

$$d\left(\Gamma(L, g)^{\perp}\right) \geqslant \begin{cases} 2^n - 2^{n-1} - 2^{\lceil n/g \rceil - 1}\left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{\lceil n/g \rceil}} \right\rfloor & \text{if } g > 1 \\ 2^n - 2^{n-1} - 2^{\lceil (n-1)/2 \rceil}\left\lfloor \frac{\lfloor 2\sqrt{q} \rfloor}{2^{(n+1)/2}} \right\rfloor & \text{if } g = 1, \end{cases} \tag{17}$$

where $g = (t-2)/2$ if $2 \nmid (t-1)$ and $g = (t-3)/2$ if $2|(t-1)$.

Taking $t = 5$ and $n = 7$, we get a binary $[128, 15, \geqslant 56]$-linear code. This is a best possible code in the sense that for given length 128 and dimension 15, the minimum distance can not be improved [2].

## 3. Proof of the main result

The main objective of this section is to provide a proof of our Main Theorem 2.1 by adopting some results from algebraic number theory and abelian varieties.

### 3.1. Newton polygon

Denote by $\mathbb{Q}_2$ the 2-adic field. It is the completion field of the rational field $\mathbb{Q}$ at prime 2. The unique discrete valuation in $\mathbb{Q}_2$ is again denoted by $\nu_2$. The Newton polygon of a polynomial $u(x) \in \mathbb{Q}_2[x]$ over the local field $\mathbb{Q}_2$ provides information on factorization of $u(x)$ over $\mathbb{Q}_2$. We briefly describe the Newton polygon method in this subsection. The reader may refer to [16, Section 3.1] for the details.

Let $u(x) = u_0 + u_1 x + \cdots + u_m x^m$ be a polynomial over $\mathbb{Q}_2$ with $u_0 u_m \neq 0$. For each $0 \leqslant i \leqslant m$, we assign a point in $\mathbb{R}^2$ as follows: (i) if $u_i \neq 0$, take the point $(i, \nu_2(u_i))$; (ii) if $u_i = 0$, we ignore the point $(i, \infty)$. In this way, we form an envelope for the set of points $\{(i, \nu_2(u_i)) : \ i = 0, 1, 2, \ldots, m\}$. The polygon thus determined is called the *Newton polygon*.

**Lemma 3.1.** *Suppose $(r, \nu_2(u_r)) \leftrightarrow (s, \nu_2(u_s))$ with $s > r$ is a segment of the Newton polygon of $u(x)$ with slope $-k$. Then $u(x)$ has exactly $s - r$ roots $\alpha_1, \alpha_2, \ldots, \alpha_{s-r}$ with $\nu_2(\alpha_1) = \nu_2(\alpha_2) = \cdots = \nu_2(\alpha_{s-r}) = k$. Moreover, the polynomial $a(x) := \prod_{i=1}^{s-r}(x - \alpha_i)$ belongs to $\mathbb{Q}_2[x]$.*

Now if $h(x) \in \mathbb{Q}_2[x]$ is an irreducible factor of $a(x)$ in the above lemma, then $\nu_2(h(0)) = k \deg(h(x)) \leqslant k \deg(a(x)) = k(s - r)$.

### 3.2. Weil number

**Definition 3.2.**

(i) An algebraic number $\omega$ is called a $q$-Weil number if $\omega$ and all $\mathbb{Q}$-conjugates of $\omega$ have absolute value $\sqrt{q}$ (by a $\mathbb{Q}$-conjugate of $\omega$, we mean a root of the minimal polynomial of $\omega$ over $\mathbb{Q}$).

(ii) A monic polynomial $\Phi(T)$ over $\mathbb{Z}[T]$ is called a $q$-Weil polynomial if it has an even degree and all its roots are $q$-Weil numbers.

(iii) The Hasse–Witt invariant of a $q$-Weil polynomial $\Phi(T) = \sum_{i=0}^{2g} c_{2g-i} T^i \in \mathbb{Z}[t]$ is defined to be the maximal $j \in [0, g]$ such that $c_j \not\equiv 0 \bmod 2$.

**Lemma 3.3.** *A $q$-Weil polynomial $\Phi(t)$ must have the form*

$$\sum_{i=0}^{2g} c_{2g-i} t^i \in \mathbb{Z}[t] \text{ with } c_{2g} = q^g \text{ and } c_{2g-i} = q^i c_i \text{ for all } i = 0, 1, \ldots, g. \tag{18}$$

**Proof.** First, note that the product of two polynomials of the form (18) still has the form (18). Hence, it is sufficient to show that an irreducible $q$-Weil polynomial $\Phi(T)$ over $\mathbb{Z}$ has the form (18). Let $\omega$ be a root of $\Phi(T)$. If $\omega$ is a real number, we must have

$\omega = \sqrt{q}$ or $-\sqrt{q}$. Thus, $\Phi(T) = (T - \sqrt{q})(T + \sqrt{q}) = T^2 - q$. In this case, $\Phi(T)$ has the form (18).

If $\omega$ is not a real number, we may assume that all $\mathbb{Q}$-conjugates of $\omega$ are $\{\omega_1, \bar{\omega}_1, \ldots, \omega_g, \bar{\omega}_g\}$, where $\bar{\omega}_i$ are complex conjugate of $\omega_i$. By definition of a $q$-Weil polynomial, we have $\Phi(T) = \prod_{i=1}^{g}(T-\omega_i)(T-\bar{\omega}_i)$ and $|\omega_i| = |\bar{\omega}_i| = \sqrt{q}$ for all $1 \leqslant i \leqslant g$. The desired result follows from the following identity

$$\frac{T^{2g}}{q^g}\Phi\left(\frac{q}{T}\right) = \frac{T^{2g}}{q^g}\prod_{i=1}^{g}\left(\frac{q}{T} - \omega_i\right)\left(\frac{q}{T} - \bar{\omega}_i\right) = \prod_{i=1}^{g}\left(T - \frac{q}{\omega_i}\right)\left(T - \frac{q}{\bar{\omega}_i}\right) = \Phi(T).$$

Note that we use the fact that $\frac{q}{\omega_i} = \bar{\omega}_i$ in the above identity. □

**Lemma 3.4.** *Let $\Phi(T)$ be a $q$-Weil polynomial with Hasse–Witt invariant equal to 0 and let $\Psi(T)$ be a divisor of $\Phi(T)$ which is also a $q$-Weil polynomial. Then $\Psi(T)$ has Hasse–Witt invariant equal to 0 as well.*

**Proof.** Let $\Phi(T) = \sum_{i=0}^{2g} c_{2g-i}T^i \in \mathbb{Z}[t]$ and let $\Psi(T) = \sum_{i=0}^{2r} a_{2r-i}T^i \in \mathbb{Z}[T]$. Put $\Phi(T)/\Psi(T) = \sum_{i=0}^{2s} b_{2s-i}T^i \in \mathbb{Z}[T]$. Then $r + s = g$.

Suppose that $\Psi(T)$ has Hasse–Witt invariant bigger than 0. Let $i$ be the largest index such that $\nu_2(a_i) = 0$. Then $1 \leqslant i \leqslant r$. Let $j$ be the largest index such that $\nu_2(b_j) = 0$ for some $0 \leqslant j \leqslant s$. Consider

$$c_{i+j} = \sum_{k+\ell=i+j} a_k b_\ell = a_i b_j + \sum_{k+\ell=i+j,(k,\ell)\neq(i,j)} a_k b_\ell. \tag{19}$$

Every term in the summation of the above equation (19) is divisible by 2, while $a_i b_j$ is not divisible by 2. Thus, $c_{i+j}$ is not divisible by 2. This is a contradiction to our condition. □

### *3.3. Algebraic curves and Hasse–Witt invariants*

Assume that $\mathcal{X}$ is an absolutely irreducible, projective and smooth algebraic curve over $\mathbb{F}_q$ of genus $g$. Then it can be regarded as a curve over $\mathbb{F}_{q^i}$ for any $i \geqslant 1$. Denote by $N_{\mathcal{X}}(i)$ the number of $\mathbb{F}_{q^i}$-rational points. Then one can define the zeta function of $\mathcal{X}$ by

$$\zeta_{\mathcal{X}}(T) := \exp\left(\sum_{i=1}^{\infty}\frac{N_{\mathcal{X}}(i)}{T^i}\right). \tag{20}$$

It was proved by Weil [15] that $\zeta_{\mathcal{X}}(T)$ is a rational function of the form $\frac{L_{\mathcal{X}}(T)}{(1-T)(1-qT)}$, where $L_{\mathcal{X}}(T) \in \mathbb{Z}[T]$ is a polynomial of degree $2g$. Furthermore, $L_{\mathcal{X}}(0) = 1$ and every reciprocity root of $L_{\mathcal{X}}(T)$ has absolute value $\sqrt{q}$.

If we write $L_{\mathcal{X}}(T) = \sum_{i=0}^{2g} a_i T^i$, then $a_0 = L_f(0) = 1$ and $a_{i+g} = q^i a_i$ for every $0 \leqslant i \leqslant g$. In particular, the leading coefficient $a_{2g} = q^g$.

We need some preliminaries and background on algebraic geometry, in particular, abelian varieties. The reader may refer to [11,14,8] for some basic results on curves and abelian varieties.

For an algebraic curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g$, we denote by $\mathcal{J}_\mathcal{X}$ the Jacobian of $\mathcal{X}$. Then $\mathcal{J}_\mathcal{X}$ is an abelian variety of dimension $g$ over $\mathbb{F}_q$. Let $\mathcal{J}_\mathcal{X}(\mathbb{F}_q)$ and $\mathcal{J}_\mathcal{X}(\overline{\mathbb{F}}_q)$ be the groups of the $\mathbb{F}_q$-rational points and $\overline{\mathbb{F}}_q$-rational points on $\mathcal{X}$, respectively.

**Definition 3.5.** Denote by $\mathcal{J}_\mathcal{X}[2]$ the subgroup of the 2-torsion points of $\mathcal{J}_\mathcal{X}(\overline{\mathbb{F}}_q)$, then one has $|\mathcal{J}_\mathcal{X}[2]| = 2^r$ for some integer $r$ with $0 \leqslant r \leqslant g$. The integer $r$ is called the Hasse–Witt invariant of $\mathcal{X}$, denoted by $i_\mathcal{X}$.

For each abelian variety $A$ of dimension $g$ over $\mathbb{F}_q$, we can consider the Frobenius morphism $\pi_A$ which sends every coordinate of a point on this variety to its $q$th power. For any prime $\ell \neq 2$, the Tate module $T_\ell A$ is a vector space of dimension $2g$ over the local field $\mathbb{Q}_\ell$. Thus, the Frobenius morphism $\pi_A$ induces a vector morphism $(\pi_A)_\ell$ on $T_\ell A$. The characteristic polynomial $\Phi_A$ of $(\pi_A)_\ell$ is a polynomial of degree $2g$ over $\mathbb{Q}_\ell$. In fact, $\Phi_A$ is defined over the integer ring $\mathbb{Z}$. This characteristic polynomial is called the characteristic polynomial of $A$ (see [14,8]). Furthermore, if $A$ is the Jacobian of an algebraic curve $\mathcal{X}/\mathbb{F}_q$, then the characteristic polynomial of $A$ is in fact the reciprocal polynomial of the $L$-polynomial of $\mathcal{X}$.

The following result given in [12] characterizes $i_\mathcal{X}$ in terms of the characteristic polynomial of $\mathcal{J}_\mathcal{X}$.

**Proposition 3.6.** *Let $\Phi_\mathcal{X}(t) = \sum_{i=0}^{2g} a_{2g-i}t^i$ be the characteristic polynomial of $\mathcal{J}_\mathcal{X}$. Then $i_\mathcal{X}$ is equal to the Hasse–Witt invariant of $\Phi_\mathcal{X}(t)$.*

**Theorem 3.7** *(Deuring–Shafarevich (see e.g. [3])). Let $E, F$ be the function fields of two curves $\mathcal{X}/\overline{\mathbb{F}}_q$ and $\mathcal{Y}/\overline{\mathbb{F}}_q$, respectively. Assume that $E/F$ is a Galois extension of function fields and the Galois group of this extension is a 2-group. Then*

$$i_\mathcal{X} - 1 = [E : F](i_\mathcal{Y} - 1) + \sum_{P \in \mathcal{Y}} \sum_{\substack{Q \in \mathcal{X} \\ Q|P}} (e(Q|P) - 1).$$

**Lemma 3.8.** *The Hasse–Witt invariant $i_{\mathcal{X}_f}$ for the curve $\mathcal{X}_f$ defined in (4) is 0.*

**Proof.** Let $F$ be the rational function field $\overline{\mathbb{F}}_q(x)$ of the projective line and let $E$ be the function field $\overline{\mathbb{F}}_q(\mathcal{X}_f)$ of $\mathcal{X}_f$. The only ramified point is the unique point $\infty$ lying over the pole of $x$. Moreover, the ramification index is 2. Thus, by the Deuring–Shafarevich Theorem, we have

$$i_{\mathcal{X}_f} - 1 = [E : F](0 - 1) + 2 - 1 = 2 \times (0 - 1) + 2 - 1 = -1,$$

i.e., $i_{\mathcal{X}_f} = 0$. □

### 3.4. Abelian varieties

We introduce a few definitions now.

**Definition 3.9.**

(i) An abelian variety is called elementary or simple if it has no subvarieties.
(ii) Two abelian varieties over $\mathbb{F}_q$ are said to be isogenous if they have the same characteristic polynomial.
(iii) The Hasse–Witt invariant of an Abelian variety is defined to be the Hasse–Witt invariant of its characteristic polynomial.

The characteristic polynomial of an abelian variety over $\mathbb{F}_q$ is a $q$-Weil polynomial. Thus, by Lemma 3.3 the characteristic polynomial of an abelian variety over $\mathbb{F}_q$ of dimension $g$ has the form $\sum_{i=0}^{2g} a_{2g-i}T^i \in \mathbb{Z}[T]$ with $a_0 = 1$ and $a_{2g-i} = q^{g-i}a_i$ for $i = 0, 1, \ldots, g$. The following well-known result (see [14]) provides information on factorization of characteristic polynomials of an abelian varieties.

**Theorem 3.10.** *Every abelian variety is isogenous to a product of elementary abelian varieties, i.e., the characteristic polynomial of every abelian variety is a product of characteristic polynomials of elementary abelian varieties.*

In view of the above theorem, it is sufficient to consider elementary abelian varieties in our case (see [14]).

**Theorem 3.11** *(Tate–Honda). There is one-to-one correspondence between isogeny classes of elementary abelian varieties over $\mathbb{F}_q$ and conjugacy classes of $q$-Weil numbers. More precisely, a polynomial $\Phi(T)$ is the characteristic polynomial of an elementary abelian variety over $\mathbb{F}_q$ if and only if $\Phi(T) = r(T)^e$ for some irreducible polynomial $r(T) \in \mathbb{Z}[T]$ with all roots being $q$-Weil numbers and $e$ is the least common denominators of $\nu_2(h(0))/n$, where $h(T)$ runs through all irreducible factors over $\mathbb{Q}_2$.*

### 3.5. Abelian varieties with Hasse–Witt invariants 0

The following result plays a crucial role.

**Theorem 3.12.** *Let $\Phi_A(T) = \sum_{i=0}^{2g} b_{2g-i}T^i \in \mathbb{Z}[T]$ be the characteristic polynomial of an elementary abelian variety $A$ with Hasse–Witt invariant equal to 0. If the dimension $g$ of $A$ is bigger than 1, then $\nu_2(b_1) \geqslant n/g$.*

**Proof.** By Theorem 3.11, we know that every elementary abelian variety $A$ has the characteristic polynomial of the form $\Phi_A(T) = r(T)^e$ for an integer $e \geqslant 1$ and a monic irreducible polynomial $r(T)$ over $\mathbb{Z}$.

If $r(T)$ has a real root, then this root must be $\pm\sqrt{q}$. In this case, we have that $r(T) = (T - \sqrt{q})(T + \sqrt{q}) = T^2 - q$. Hence, $b_1 = 0$ and the desired result follows.

Now we assume that all roots of $r(T)$ are not real. Then it is clear that the degree of $r(T)$ is even. Let $r(T) = \sum_{i=0}^{2r} a_{2r-i}T^i$ with $g = er$. To analyze $\nu_2(a_i)$, we look at the Newton polygon of $r(T)$. By our assumption, we know that $\nu_2(a_i) > 0$ for all $1 \leqslant i \leqslant r$.

Define the set

$$I := \{1 \leqslant i \leqslant r : \ \nu_2(a_i) \geqslant in/2\}$$

and

$$J := \{1 \leqslant j \leqslant r : \ \nu_2(a_j) < jn/2\}.$$

If $1 \in I$, then $\nu_2(a_1) \geqslant n/2 \geqslant n/g$. Hence, $\nu_2(b_1) = \nu_2(e) + \nu_2(a_1) \geqslant n/g$.

Now assume that $1 \in J$. We claim the following.

There exists $1 \leqslant i \leqslant r$ such that

$$\frac{\nu_2(a_i)}{i} < \min_{r+1 \leqslant \ell \leqslant 2r} \left\{ \frac{\nu_2(a_\ell)}{\ell} \right\}. \tag{21}$$

First of all, $\nu_2(a_1) < n/2 = \nu_2(q^r)/2r = \nu_2(a_{2r})/2r$. Hence, to prove the inequality (21), it is sufficient to prove that for every $\ell \in \{r+1, r+2, \ldots, 2r-1\}$, there exists $j \in J$ such that $\nu_2(a_\ell)/\ell > \nu_2(a_j)/j$. Note that, since $I \cup J = \{1, 2, \ldots, r\}$, thus $\ell = 2r - k$ with $k$ in $I \setminus \{r\}$ or in $J$.

Then for every $i \in I \setminus \{r\}$ and $j \in J$, we have

$$\frac{\nu_2(a_{2r-j})}{2r-j} = \frac{\nu_2(a_j) + (r-j)n}{2r-j} > \frac{\nu_2(a_j)}{j}$$

and

$$\frac{\nu_2(a_{2r-i})}{2r-i} = \frac{\nu_2(a_i) + (r-i)n}{2r-i} \geqslant \frac{n}{2} > \frac{\nu_2(a_j)}{j}.$$

Our claim follows.

Now let $0 \leqslant i \leqslant r$ be the largest index such that

$$\frac{\nu_2(a_i)}{i} = \min_{1 \leqslant j \leqslant 2r} \left\{ \frac{\nu_2(a_j)}{j} \right\},$$

then $(2r - i, \nu_2(a_i)) \longleftrightarrow (2r, 0)$ forms a segment in the Newton Polygon of $r(T)$ with slope $-\nu_2(a_i)/i$. Assume that $h(t)$ is an irreducible factor of $r(T)$ in $\mathbb{Q}_2[t]$ corresponding to this segment. Then we have $\nu_2(h(0)) \leqslant \frac{\nu_2(a_i)}{i} \times (2r - (2r - i)) = \nu_2(a_i)$. Assume that

$\frac{\nu_2(h(0))}{n} = \frac{k}{\ell}$ with $\gcd(k,\ell) = 1$. Then by the Tate–Honda theorem, i.e., Theorem 3.11, we have $e \geqslant \ell$ and

$$\nu_2(a_i) \geqslant \nu_2(h(0)) = n \times \frac{\nu_2(h(0))}{n} = \frac{kn}{\ell} \geqslant \frac{kn}{e} \geqslant \frac{n}{e}. \tag{22}$$

Since $(2r-i, \nu_2(a_i)) \longleftrightarrow (2r, 0)$ forms a segment in the Newton Polygon of $h(t)$, the slope $-\nu_2(a_1)$ of the segment $(2r-1, \nu_2(a_1)) \longleftrightarrow (2r,0)$ is at most the slope $-\nu_2(a_i)/i$ of the segment $(2r-i, \nu_2(a_i)) \longleftrightarrow (2r,0)$, i.e.,

$$\nu_2(a_1) \geqslant \frac{\nu_2(a_i)}{i} \geqslant \frac{n}{ie} \geqslant \frac{n}{re} = \frac{n}{g}.$$

Hence, $\nu_2(b_1) \geqslant \nu_2(e) + \nu_2(a_1) \geqslant \frac{n}{g}$. This completes the proof. □

**Corollary 3.13.** *Assume that $\tilde{L}(T)$ is the reciprocal polynomial of the $L$-polynomial of an algebraic curve $\mathcal{X}$ over $\mathbb{F}_q$. Let $\tilde{L}(T)$ have the canonical factorization into product $\prod r(T)^e$. If the Hasse–Witt invariant of $\mathcal{X}$ is 0, then $\nu_P(a_1) \geqslant n/g$, where $r(T)^e = \sum_{i=0}^{2g} a_{2g-i}T^i$ with $g > 1$.*

### *3.6. Proof of the main result*

Let $L_f(T) = \sum_{i=0}^{2g} a_i T^i$ be the $L$-polynomial of $\mathcal{X}_f$. By abuse of notation, the reciprocal polynomial $\tilde{L}_f(T) = \sum_{i=0}^{2g} a_i T^{2g-i}$ of $L_f(T)$ is called the *characteristic polynomial* of $\mathcal{X}_f$ (in fact, $\tilde{L}_f(T)$ is the characteristic polynomial of the Jacobian of the curve $\mathcal{X}_f$). Then it is clear that every root of $\tilde{L}_f(T)$ is a Weil number and $\tilde{L}_f(T)$ is a $q$-Weil Polynomial.

**Theorem 3.14.** *Let $\tilde{L}_f(T) = \sum_{i=0}^{2g} a_{2g-i}T^i \in \mathbb{Z}[T]$ be the characteristic polynomial of the curve $\mathcal{X}_f$ defined in (4) with $g = (m-1)/2$. Then we have*

$$\nu_2(a_1) \geqslant \begin{cases} \left\lceil \frac{n}{g} \right\rceil & \text{if } g > 1 \\ \frac{n+1}{2} & \text{if } g = 1. \end{cases}$$

**Proof.** By Lemma 3.8, we know that $\tilde{L}_f(T)$ is a $q$-Weil polynomial with Hasse–Witt invariant equal to 0. The case $g = 1$ follows from [14, Theorem 4.1]. Now assume that $g \geqslant 2$. Factorize $\tilde{L}_f(T)$ into a product $\prod_{i=1}^{k} \Phi_i(T)$ of co-prime $q$-Weil polynomials such that every $\Phi_i(T)$ is a power of an irreducible polynomial over $\mathbb{Q}$. Let $\Phi_i(T) = \sum_{j=0}^{2g_i} a_{i,2g_i-j}T^j$. Then we have $\nu_2(a_{i,1}) \geqslant \min\{n/g_i, (n+1)/2\} \geqslant n/g$ for all $i = 1, 2, \ldots, k$. Thus, we have $\nu_2(a_1) = \nu_2\left(\sum_{i=1}^{k} a_{i,1}\right) \geqslant \min_{1 \leqslant i \leqslant k}\{\nu_2(a_{i,1})\} \geqslant n/g$. □

**Proof of the Main Result (Theorem 2.1).** Let $\tilde{L}_f(t) = \sum_{i=0}^{2g} a_{2g-i}T^i \in \mathbb{Z}[T]$ be the characteristic polynomial of $\mathcal{X}_f$ with $g = (m-1)/2$. First we note that $|N_f - q - 1| = |a_1|$. Combining Theorem 3.14 and the Weil–Serre bound, we get

$$|N_g - q - 1| \leqslant \begin{cases} 2^{\lceil n/g \rceil} \left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{\lceil n/g \rceil}} \right\rfloor & \text{if } g > 1 \\ 2^{(n+1)/2} \left\lfloor \frac{g\lfloor 2\sqrt{q} \rfloor}{2^{(n+1)/2}} \right\rfloor & \text{if } g = 1. \end{cases}$$

The desired result follows from the fact that $|Z_f| = (N_f - 1)/2$. □

## References


[1] C. Carlet, Boolean functions for cryptography and error-correcting codes, Book Chapter in: Boolean Models and Methods in Mathematics, Computer Science and Engineering, 2010, pp. 257–397.
[2] M. Grassl, Code tables: bounds on the parameters of various types of codes, http://www.codetables.de/, March 2015.
[3] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves of Finite Fields, Princeton Ser. Appl. Math., 2008.
[4] T. Kaufman, S. Lovett, New extension of the Weil bound for character sums with applications to coding, in: 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS), 2011, pp. 788–796.
[5] R. Lidl, H. Niederreiter, Finite Fields, Addison–Wesley, Reading, MA, 1983, now distributed by Cambridge University Press.
[6] F.I. MacWilliams, N.I.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[7] O. Moreno, C.J. Moreno, An Elementary Proof of a Partial Improvement to the Ax–Katz Theorem, Lecture Notes in Comput. Sci., vol. 673, 1993, pp. 257–268.
[8] D. Mumford, Abelian Varieties, Mumbai, 2008.
[9] A. Rojas-Leon, D. Wan, Improvements of the Weil bound for Artin–Schreier curves, Math. Ann. 351 (2011) 417–442.
[10] J.-P. Serre, Rational Points on Curves over Finite Fields, Lecture Notes, Harvard University, 1985.
[11] I.R. Shafarevich, Basic Algebraic Geometry I, second edition, Springer, 1995.
[12] H. Stichtenoth, Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers, Arch. Math. 33 (1979) 357–360.
[13] H. Stichtenoth, C. Voss, Generalized Hamming weights of trace codes, IEEE Trans. Inform. Theory 40 (1994) 554–558.
[14] W. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) 2 (1969) 521–560.
[15] A. Weil, Sur les courbes algebriques et les varietes qui s'en deduisent, Actual. Sci. Ind., vol. 1041, Hermann, Paris, 1948.
[16] E. Weiss, Algebraic Number Theory, McGaw–Hill, New York, 1963.
[17] J. Wolfmann, New Bounds on Cyclic Codes from Algebraic Curves, Lecture Notes in Comput. Sci., vol. 388, Springer-Verlag, New York, 1988, pp. 47–62.