Journal of Computational and Applied Mathematics 259 (2014) 474–484

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Supersingular curves over finite fields and weight divisibility of codes

Cem Güneri[a], Gary McGuire[b,*]

[a] Faculty of Engineering and Natural Sciences, SabancıUniversity, Tuzla, 34956, Istanbul, Turkey
[b] School of Mathematical Sciences, University College Dublin, Ireland

ARTICLE INFO

Article history:
Received 26 November 2012
Received in revised form 19 December 2012

MSC:
11T23
11T71
94B27

Keywords:
Supersingular curve
Cyclic code
Quasi-cyclic code
Trace representation

ABSTRACT

Motivated by a recent article of the second author, we relate a family of Artin–Schreier type curves to a sequence of codes. We describe the algebraic structure of these codes, and we show that they are quasi-cyclic codes. We show that if the family of Artin–Schreier type curves consists of supersingular curves then the weights in the related codes are divisible by a certain power of the characteristic. We give some applications of the divisibility result, including showing that some weights in certain cyclic codes are eliminated in subcodes.

1. Introduction

For $q = 2^n$ and α a primitive element in $\mathbb{F}_q$, let $C^\perp$ be the binary cyclic code of length $2^n - 1$ with dual zeros $\alpha, \alpha^3, \alpha^{13}$. It is well known (see [1] for example) that the weights in $C^\perp$ are related to the number of $\mathbb{F}_q$-rational points of curves of the form

$$y^2 + y = ax + bx^3 + cx^{13}, \tag{1.1}$$

where $a, b, c \in \mathbb{F}_q$. In [1], the second author used the supersingularity of these curves to prove that, when n is odd, all the weights in $C^\perp$ are divisible by $2^{(n-1)/2}$. This was a very short proof of the same divisibility result that appeared in [2] with a rather long proof.

In fact, the only information used about curves of the form (1.1) in [1] was the divisibility of their number of affine $\mathbb{F}_q$-rational points by a power of 2, which is implied by their supersingularity. However, supersingularity tells more about the arithmetic of the curve. It implies divisibility by a certain power of the characteristic not only over the field of definition $\mathbb{F}_q$ but also over finite extensions of $\mathbb{F}_q$.

The purpose of this paper is to extend the work in [1] by utilizing all the arithmetic information that comes with supersingularity to obtain conclusions regarding a certain sequence of codes that we define. From a family of Artin–Schreier type curves

$$\mathcal{F} = \{y^r - y = \lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s} : \lambda_1, \ldots, \lambda_s \in \mathbb{F}_q\},$$

[*] Corresponding author. Tel.: +353 17165319.
E-mail addresses: guneri@sabanciuniv.edu (C. Güneri), gary.mcguire@ucd.ie (G. McGuire).

0377-0427/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
doi:10.1016/j.cam.2012.12.017

where r is a prime power and q is a power of r, we define a sequence C_j of $\mathbb{F}_r$-linear codes of increasing length. This establishes a new relation between curves and codes than the ones that have been explored so far (see [3–5]). Our main theorem (Theorem 3.1) shows that if $\mathcal{F}$ consists of supersingular curves, then the weights in C_j's satisfy certain divisibility conditions. In Section 4 we prove that C_j is quasi-cyclic of length $q^j - 1$ and index $(q^j - 1)/(q - 1)$ for all $j \geq 1$. In the same section, we also determine the algebraic structure of these quasi-cyclic codes completely by describing their constituents. In Section 5 we give some interesting consequences of our results. The main application is elimination of weights in subcodes of certain cyclic codes. Our results also have applications to permutation polynomials and divisibility properties of certain exponential sums. We conclude in Section 6 by addressing the converse question. Namely, we elaborate on whether one can conclude supersingularity of Artin–Schreier type curves from certain divisibility assumptions on codes.

2. Divisibility for supersingular curves

Let $q = p^m$ where p is an arbitrary prime and $m \geq 1$ is an integer. Let X be a curve defined over $\mathbb{F}_q$ with L-polynomial

$$L_X(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g} \in \mathbb{Z}[t], \tag{2.1}$$

where g is the genus of X. Let $N_j = N_j(X)$ denote the number of $\mathbb{F}_{q^j}$-rational points of X and set $S_j := N_j - (q^j + 1)$ for all $j \geq 1$. If we factor $L_X(t)$ as

$$L_X(t) = \prod_{i=1}^{2g} (1 - \omega_i t),$$

where the ω_i's are algebraic integers with $|\omega_i| = \sqrt{q}$, then we know that

$$S_j = -\sum_{i=1}^{2g} \omega_i^j, \quad \text{for all } j \geq 1 \text{ [6, Corollary 5.1.16].}$$

Then by Newton's identities [7, p. 245], [6, Corollary 5.1.17], we have the following relation between the coefficients of $L_X(t)$ and the numbers S_j:

$$a_0 = 1$$

$$S_i + a_1 S_{i-1} + \cdots + a_{i-1} S_1 - i a_i = 0, \quad \text{for } 1 \leq i \leq 2g \tag{2.2}$$

$$S_{2g+i} + a_1 S_{2g+i-1} + \cdots + a_{2g} S_i = 0, \quad \text{for } i \geq 1. \tag{2.3}$$

Given the L-polynomial as in (2.1) of a curve X over $\mathbb{F}_q$, consider the following set of points in $\mathbb{R}^2$

$$\left\{ \left(i, \frac{\operatorname{ord}_p(a_i)}{m} \right) : \ 0 \leq i \leq 2g, \ a_i \neq 0 \right\},$$

where $\operatorname{ord}_p(\cdot)$ denotes the p-adic valuation. The lower convex hull of these points is called the Newton polygon of X (see [8]). Note that $(0, 0)$ and $(2g, g)$ are respectively the initial and the terminal points of the Newton polygon. The ith slope is defined to be the slope of the line segment lying over the interval $[i - 1, i]$. The curve X is said to be supersingular if all $2g$ slopes of its Newton polygon are $1/2$ (see [9]). In other words, the Newton polygon is a straight line segment of slope $1/2$. Another equivalent definition is that the Jacobian of X is isogenous (over the algebraic closure of $\mathbb{F}_q$) to a product of supersingular elliptic curves. See [10] for details.

The following is an immediate consequence of the definition of supersingularity above and it will be used extensively.

Lemma 2.1. *A curve X over $\mathbb{F}_q$ with the L-polynomial $L_X(t) = 1 + \sum_{i=1}^{2g} a_i t^i$ is supersingular if and only if*

$$\operatorname{ord}_p(a_i) \geq \frac{i}{2} \operatorname{ord}_p(q), \quad \text{for all } i = 1, \ldots, 2g,$$

where p is the characteristic of $\mathbb{F}_q$.

This yields the following divisibility results on the S_j's, which will be used in the next section.

Theorem 2.2. *Let $q = p^m$ and X be a supersingular curve over $\mathbb{F}_q$ of genus g.*

(i) *If m is even then $p^{\frac{jm}{2}} \mid S_j$, for every $j \geq 1$.*
(ii) *If m is odd, then*

$$p^{\frac{jm}{2}} \Big| S_j, \quad \text{for all } j \geq 1 \text{ even},$$

$$p^{\frac{jm+1}{2}} \Big| S_j, \quad \text{for all } j \geq 1 \text{ odd}.$$

If $p = 2$, then we further have $2^{\frac{jm}{2}+1} \mid S_j$, for all $j \geq 1$ even.

Proof. Assume that m is even. Then by Lemma 2.1, we have

$$p^{\frac{im}{2}} \,\Big|\, a_i, \quad \text{for all } 1 \le i \le 2g. \tag{2.4}$$

Then by (2.2), we have $S_1 = a_1$ is divisible by $p^{\frac{m}{2}}$, and $S_2 = -a_1S_1 + 2a_2$ is divisible by $p^{\frac{2m}{2}} = p^m$. Continuing to use (2.2) and (2.4), we conclude that

$$p^{\frac{jm}{2}} \,\Big|\, S_j, \quad \text{for all } 1 \le j \le 2g. \tag{2.5}$$

For $j = 2g + 1$, we now use (2.3) to write

$$S_{2g+1} = -a_1S_{2g} - a_2S_{2g-1} - \cdots - a_{2g}S_1.$$

By (2.4) and (2.5), we conclude that $p^{\frac{(2g+1)m}{2}} \mid S_{2g+1}$. Then, we can conclude by induction that $p^{\frac{jm}{2}} \mid S_j$ for all $j > 2g$.

Now assume that m is odd. In this case Lemma 2.1 yields

$$p^{\frac{im}{2}} \,\Big|\, a_i, \quad \text{for all } 1 \le i \le 2g \text{ even,} \tag{2.6}$$

$$p^{\frac{im+1}{2}} \,\Big|\, a_i, \quad \text{for all } 1 \le i \le 2g \text{ odd.} \tag{2.7}$$

Then by (2.2), we have $S_1 = a_1$ is divisible by $p^{\frac{m+1}{2}}$. For $S_2 = -a_1S_1 + 2a_2$ and arbitrary prime p, note that a_1S_1 is divisible by $p^{\frac{2(m+1)}{2}} = p^{m+1}$, whereas $2a_2$ is divisible by $p^{\frac{2m}{2}} = p^m$. Hence, S_2 is divisible by p^m for a general prime. However, for $p = 2$, $2a_2$ is divisible by one higher power 2^{m+1} and hence the same conclusion holds for S_2. Continuing to use (2.2), (2.6) and (2.7), we reach the conclusion in the statement of this theorem for all $1 \le j \le 2g$ and for both an arbitrary prime p and the special case $p = 2$.

For $j = 2g + 1$, we use (2.3) to write

$$S_{2g+1} = -a_1S_{2g} - a_2S_{2g-1} - \cdots - a_{2g}S_1. \tag{2.8}$$

For a summand involving a_i with odd i on the right hand side of (2.8), the index of S_{2g+1-i} is even. By (2.7), a_i is divisible by $p^{\frac{im+1}{2}}$. We also know that S_{2g+1-i} is divisible by $p^{\frac{(2g+1-i)m}{2}}$ for an arbitrary prime p, and it is divisible by $2^{\frac{(2g+1-i)m}{2}+1}$ for $p = 2$. Hence, the product a_iS_{2g+1-i} is divisible by $p^{\frac{(2g+1)m+1}{2}}$ for an arbitrary prime p, and it is divisible by $2^{\frac{(2g+1)m+1}{2}+1}$ for $p = 2$. For a summand involving a_i with even i on the right hand side of (2.8), the index of S_{2g+1-i} is odd. By (2.6), a_i is divisible by $p^{\frac{im}{2}}$. On the other hand, S_{2g+1-i} is divisible by $p^{\frac{(2g+1-i)m+1}{2}}$. Hence the product a_iS_{2g+1-i} is divisible by $p^{\frac{(2g+1)m+1}{2}}$ for such summands. Hence, S_{2g+1} is divisible by $p^{\frac{(2g+1)m+1}{2}}$ for all primes.

For $j = 2g + 2$, (2.3) yields

$$S_{2g+2} = -a_1S_{2g+1} - a_2S_{2g} - \cdots - a_{2g}S_2. \tag{2.9}$$

We analyze summands as above. For a summand involving a_i with odd i on the right hand side of (2.9), we have $p^{\frac{im+1}{2}} \mid a_i$ and $p^{\frac{(2g+2-i)m+1}{2}} \mid S_{2g+2-i}$. Hence the product a_iS_{2g+2-i} is divisible by $p^{\frac{(2g+2)m+2}{2}} = p^{\frac{(2g+2)m}{2}+1}$ for such summands. For a summand involving a_i with even i on the right hand side of (2.9), we have $p^{\frac{im}{2}} \mid a_i$. In this case, S_{2g+2-i} is divisible by $p^{\frac{(2g+2-i)m}{2}}$ for an arbitrary prime p and it is divisible by $2^{\frac{(2g+2-i)m}{2}+1}$ for $p = 2$. Hence the product a_iS_{2g+2-i} is divisible by $p^{\frac{(2g+2)m}{2}}$ for any p, and it is divisible by $2^{\frac{(2g+2)m}{2}+1}$ for $p = 2$. Therefore S_{2g+2} is divisible by $p^{\frac{(2g+2)m}{2}}$ in general and it is divisible by $2^{\frac{(2g+2)m}{2}+1}$ for $p = 2$. Now an induction argument proves the claim for all S_j with $j > 2g$. □

We next state a proposition which gathers together results showing that particular curves are supersingular. Proving that a given explicit curve is supersingular is usually difficult. We will use these results later for our applications.

Proposition 2.3. *The following curves, defined over $\mathbb{F}_{2^k}$ for any k, are supersingular.*

(1) $y^2 + y = \sum_{i=0}^{d} \lambda_i x^{2^i+1}$, $d \ge 1$,
(2) $y^2 + y = ax + bx^3 + cx^{13}$.

The first of these is proved in [3], the second in [11] which gives an argument due to Elkies. We remark that $y^2 + y = ax + bx^3 + cx^{13}$ is a curve of genus 6, and that genus 6 is the smallest genus in characteristic 2 that cannot be proved to be supersingular using the family (1).

3. Divisibility for codes

We wish to consider the most general case of Artin–Schreier curves, see (3.1), so we let $r = p^v$ and $q = r^u$ throughout, where p is a prime number and $u, v \geq 1$ are integers. Usually $v = 1$ in our examples. Assume that $1 \leq i_1 < \cdots < i_s < q$ are integers such that $\gcd(p, i_j) = 1$, for all j, and i_j's lie in distinct r-cyclotomic cosets modulo $q - 1$ (see Remark 3.3). Consider the family of Artin–Schreier type curves over $\mathbb{F}_q$:

$$\mathcal{F} = \{y^r - y = \lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s} : \lambda_1, \ldots, \lambda_s \in \mathbb{F}_q\}. \tag{3.1}$$

Since the i_j's are relatively prime to the characteristic, each equation, except the "trivial" one with $\lambda_k = 0$ for all k, defines an absolutely irreducible curve over $\mathbb{F}_q$.

For each $j \geq 1$, we denote the trace map from $\mathbb{F}_{q^j}$ to $\mathbb{F}_r$ as follows:

$$\begin{aligned} \mathrm{Tr}_j : \mathbb{F}_{q^j} &\longrightarrow \mathbb{F}_r \\ a &\longmapsto \sum_{t=0}^{ju-1} a^{r^t}. \end{aligned}$$

Let $X = X_{\lambda_1,\ldots,\lambda_s}$ be an arbitrary nontrivial member of $\mathcal{F}$ which is described by $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_q$. Note that X has r points with $x = 0$ and one point at infinity over the base field $\mathbb{F}_q$ or any extension of $\mathbb{F}_q$. Moreover, if there is an affine rational point (x_0, y_0) on X over $\mathbb{F}_q$ or an extension of $\mathbb{F}_q$, then there are r rational points over the same field whose x-coordinate is x_0 (namely, $(x_0, y_0 + \beta)$ for any $\beta \in \mathbb{F}_r$).

We associate with X the following vector of length $q^j - 1$ for every $j \geq 1$:

$$c_j = c_j(\lambda_1, \ldots, \lambda_s) := \left(\mathrm{Tr}_j\left(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}\right)\right)_{x \in \mathbb{F}_{q^j}^*}. \tag{3.2}$$

The vector c_j has entries in $\mathbb{F}_r$, and the entry in coordinate $x \in \mathbb{F}_{q^j}^*$ is obtained by evaluating the given trace expression at x. By Hilbert's Theorem 90, the Hamming weight of c_j is related to the number N_j of $\mathbb{F}_{q^j}$-rational points on X, for every $j \geq 1$:

$$w(c_j) = r^{ju} - 1 - \frac{N_j - (r+1)}{r}.$$

Equivalently, we have

$$r w(c_j) = r^{ju}(r-1) - S_j, \tag{3.3}$$

where $S_j = N_j - (r^{ju} + 1)$ as in Section 2.

Based on the discussion above, the following relates the family $\mathcal{F}$ to a sequence of $\mathbb{F}_r$-linear codes and yields conclusions on the weights of these codes when $\mathcal{F}$ consists of supersingular curves.

Theorem 3.1. *Assume that the family $\mathcal{F}$ in (3.1) consists of supersingular curves over $\mathbb{F}_q = \mathbb{F}_{p^{uv}}$. For each $j \geq 1$, define the $\mathbb{F}_r$-linear code of length $q^j - 1 = p^{juv} - 1$ as follows:*

$$C_j := \{(\mathrm{Tr}_j(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}))_{x \in \mathbb{F}_{q^j}^*} : \lambda_1, \ldots, \lambda_s \in \mathbb{F}_q\}. \tag{3.4}$$

(i) *If uv is even, then $p^{\frac{juv}{2} - v}$ divides all the weights in C_j for every j.*

(ii) *If uv is odd, then*

$p^{\frac{juv}{2} - v}$ divides all the weights in C_j for j even,

$p^{\frac{juv+1}{2} - v}$ divides all the weights in C_j for j odd.

If $p = 2$, then we further have that $2^{\frac{juv}{2} - v + 1}$ divides all the weights in C_j for j even.

Proof. By (3.3) and the definition of C_j, the quantities S_j (for all $j \geq 1$) attached to every curve $X \in \mathcal{F}$ determine the weight of one codeword in C_j. Moreover, this is a one-to-one correspondence between the members of $\mathcal{F}$ and all the codewords in these codes. Rewriting (3.3) as

$$p^v w(c_j) = p^{juv}(p^v - 1) - S_j, \tag{3.5}$$

we obtain the conclusions of this theorem from Theorem 2.2. □

Remark 3.2. Note that the sequence C_j of codes can be defined for any family $\mathcal{F}$ of Artin–Schreier type curves in (3.1). The supersingularity assumption on $\mathcal{F}$ yields the weight divisibility result in Theorem 3.1 for C_j.

Remark 3.3. For each $j \geq 1$, consider the $\mathbb{F}_r$-linear code of length $q^j - 1$

$$\tilde{C}_j := \{(\mathrm{Tr}_j(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}))_{x \in \mathbb{F}^*_{q^j}} : \lambda_1, \ldots, \lambda_s \in \mathbb{F}_{q^j}\}.$$

Since the i_j's lie in distinct r-cyclotomic cosets mod $q - 1$, they also lie in distinct r-cyclotomic cosets mod $q^j - 1$. Hence, $\tilde{C}_j$ is the cyclic code with dual zeros $\alpha_j^{i_1}, \ldots, \alpha_j^{i_s}$, where α_j is a primitive element of $\mathbb{F}_{q^j}$. Our codes C_j are subcodes of these cyclic codes.

4. Algebraic structure of the codes

Our aim in this section is to understand the algebraic structure of the codes C_j in Theorem 3.1.

4.1. Background on quasi-cyclic codes

We follow [12] for the basics on quasi-cyclic codes. A linear code which is invariant under the shift of codewords by ℓ units is called a quasi-cyclic (QC) code of index ℓ, if ℓ is the smallest positive number with this property. This is a generalization of classical cyclic codes since index 1 QC codes are cyclic.

Let C be a QC code over $\mathbb{F}_r$ of length $m\ell$ and index ℓ, where m is relatively prime to r. We can think of the codewords of C as $m \times \ell$ arrays

$$c = \begin{pmatrix} c_{00}, \ldots, c_{0,\ell-1} \\ c_{10}, \ldots, c_{1,\ell-1} \\ \vdots \\ c_{m-1,0}, \ldots, c_{m-1,\ell-1} \end{pmatrix}. \tag{4.1}$$

It is clear that being closed under the shift by ℓ units amounts to being closed under row shift.

Let us set $R := \mathbb{F}_r[x]/\langle x^m - 1\rangle$. To c as in (4.1), we associate an element of R^ℓ

$$(c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell, \tag{4.2}$$

where for each $0 \leq j \leq \ell - 1$,

$$c_j(x) := c_{0j} + c_{1j}x + c_{2j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R.$$

Then we can think of C as an additive subgroup of R^ℓ. Note that being closed under row shift amounts to being closed under coordinatewise multiplication by x in R^ℓ. Hence, a QC code C is an R-submodule of R^ℓ.

Since m is relatively prime to r, the polynomial $x^m - 1$ factors into distinct irreducible polynomials in $\mathbb{F}_r[x]$ as

$$x^m - 1 = b_1(x)b_2(x)\cdots b_n(x). \tag{4.3}$$

Roots of $b_i(x)$'s are powers of a fixed primitive mth root of unity ξ. Let us choose nonnegative integers u_i so that $b_i(\xi^{u_i}) = 0\, u_i$ for each $i = 1, 2, \ldots, n$. Hence by the Chinese Remainder Theorem we have a ring isomorphism

$$R \cong \bigoplus_{i=1}^{n} \mathbb{E}_i, \tag{4.4}$$

where $\mathbb{E}_i := \mathbb{F}_r[x]/\langle b_i(x)\rangle = \mathbb{F}_r(\xi^{u_i})$ is an extension field of $\mathbb{F}_r$ for each i. This implies that

$$R^\ell \cong \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_n^\ell. \tag{4.5}$$

Hence, a QC code $C \subset R^\ell$ can be viewed as an $(\mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_n)$-submodule of $\mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_n^\ell$ and as such let us suppose C decomposes as

$$C = D_1 \oplus \cdots \oplus D_n, \tag{4.6}$$

where D_i is a linear code of length ℓ over $\mathbb{E}_i$, for each i. These length ℓ linear codes over various extensions of $\mathbb{F}_r$ are called the constituents (see [13]) of C.

The next result gives a trace representation for QC codes.

Theorem 4.1 ([12, Theorem 5.1]). *Assume that $x^m - 1$ factors into irreducibles as in (4.3) and adopt all the notation above. Let U_i denote the r-cyclotomic coset mod m corresponding to $\mathbb{E}_i$ for all $i = 1, \ldots, n$ (i.e. corresponding to the powers of ξ among the roots of $b_i(x)$). Fix representatives $u_i \in U_i$ from each cyclotomic coset.*

Let D_i over $\mathbb{E}_i$ be a linear code of length ℓ for all i. For codewords $\beta_i \in D_i$ and for each $0 \leq g \leq m - 1$, let

$$c_g = c_g(\beta_1, \ldots, \beta_n) := \sum_{i=1}^{n} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_r}\left(\beta_i \xi^{-gu_i}\right), \tag{4.7}$$

where the traces are applied to vectors coordinatewise so that c_g is a vector of length ℓ over $\mathbb{F}_r$ for all $0 \le g \le m-1$. Then the code

$$C = \left\{ (c_0(\beta_1,\ldots,\beta_n),\ldots,c_{m-1}(\beta_1,\ldots,\beta_n)) = \begin{pmatrix} c_0(\beta_1,\ldots,\beta_n) \\ c_1(\beta_1,\ldots,\beta_n) \\ \vdots \\ c_{m-1}(\beta_1,\ldots,\beta_n) \end{pmatrix} : \beta_i \in D_i, \right\} \tag{4.8}$$

is a QC code over $\mathbb{F}_r$ of length $m\ell$ and index ℓ.

Conversely, every QC code of length $m\ell$ and index ℓ is obtained through this construction.

4.2. Our codes are quasi-cyclic

Next, we observe that the linear codes C_j in Theorem 3.1 are QC codes.

Theorem 4.2. *For each $j \ge 1$, the code C_j defined in (3.4) is a length $q^j - 1$ QC code over $\mathbb{F}_r$ of index $\ell_j := (q^j-1)/(q-1)$.*

Proof. Let $\alpha_j \in \mathbb{F}_{q^j}$ be a primitive element. Then we can write C_j as follows:

$$C_j = \{(\mathrm{Tr}_j(\lambda_1\alpha_j^{ki_1} + \cdots + \lambda_s\alpha_j^{ki_s}))_{0\le k\le q^j-2} : \lambda_1,\ldots,\lambda_s \in \mathbb{F}_q\}.$$

If Nr_j denotes the norm map from $\mathbb{F}_{q^j}$ to $\mathbb{F}_q$, then it is easy to see that $\mathrm{Nr}_j(\alpha_j) = \alpha_j^{\ell_j}$ is a primitive element of $\mathbb{F}_q$, and the number ℓ_j is the smallest exponent of α_j such that $\alpha_j^{\ell_j}$ lies in $\mathbb{F}_q$. Let T denote the shift operator on vectors (i.e. $T(v_0,\ldots,v_n) = (v_n, v_0,\ldots,v_{n-1})$). If $c = c(\lambda_1,\ldots,\lambda_s)$ denotes the following codeword in C_j

$$c = \left(\mathrm{Tr}_j\left(\lambda_1\alpha_j^{ki_1} + \cdots + \lambda_s\alpha_j^{ki_s}\right)\right)_{0\le k\le q^j-2}, \tag{4.9}$$

then we have

$$\begin{aligned} Tc &= \left(\mathrm{Tr}_j\left(\lambda_1\alpha_j^{(k-1)i_1} + \cdots + \lambda_s\alpha_j^{(k-1)i_s}\right)\right)_{0\le k\le q^j-2} \\ &= \left(\mathrm{Tr}_j\left(\lambda_1\alpha_j^{-i_1}\alpha_j^{ki_1} + \cdots + \lambda_s\alpha_j^{-i_s}\alpha_j^{ki_s}\right)\right)_{0\le k\le q^j-2}. \end{aligned}$$

Hence,

$$\begin{aligned} T^{\ell_j}c &= \left(\mathrm{Tr}_j\left(\lambda_1\alpha_j^{(k-\ell_j)i_1} + \cdots + \lambda_s\alpha_j^{(k-\ell_j)i_s}\right)\right)_{0\le k\le q^j-2} \\ &= \left(\mathrm{Tr}_j\left(\lambda_1\alpha_j^{-\ell_j i_1}\alpha_j^{ki_1} + \cdots + \lambda_s\alpha_j^{-\ell_j i_s}\alpha_j^{ki_s}\right)\right)_{0\le k\le q^j-2} \\ &= c\left(\lambda_1\alpha_j^{-\ell_j i_1},\ldots,\lambda_s\alpha_j^{-\ell_j i_s}\right). \end{aligned}$$

Note that $\lambda_1\alpha_j^{-\ell_j i_1},\ldots,\lambda_s\alpha_j^{-\ell_j i_s}$ all lie in $\mathbb{F}_q$ since $\alpha_j^{\ell_j}$ lies in $\mathbb{F}_q$. Hence, $T^{\ell_j}c \in C_j$. Moreover, ℓ_j is the smallest power of α_j such that $\alpha_j^{\ell_j} \in \mathbb{F}_q$. Therefore, ℓ_j is the minimal number such that the ℓ_j shift of $c \in C_j$ lies again in C_j. This proves the claim. □

4.3. Identifying the constituent codes

We start with realizing a codeword $c \in C_j$ in (4.9) as a $(q-1)\times\ell_j$ array. As noted in the proof of Theorem 4.2, $\mathrm{Nr}_j(\alpha_j) = \alpha_j^{\ell_j}$ is a primitive element of $\mathbb{F}_q$. We set $\xi := \alpha_j^{-\ell_j}$, which is also a primitive element in $\mathbb{F}_q$. Then,

$$c = \mathrm{Tr}_j\begin{pmatrix} \sum_{t=1}^{s}\lambda_t\alpha_j^{0i_t}, \sum_{t=1}^{s}\lambda_t\alpha_j^{i_t}, \ldots, \sum_{t=1}^{s}\lambda_t\alpha_j^{(\ell_j-1)i_t} \\ \sum_{t=1}^{s}\lambda_t\alpha_j^{\ell_j i_t}, \sum_{t=1}^{s}\lambda_t\alpha_j^{(\ell_j+1)i_t}, \ldots, \sum_{t=1}^{s}\lambda_t\alpha_j^{(2\ell_j-1)i_t} \\ \vdots \\ \sum_{t=1}^{s}\lambda_t\alpha_j^{(q-2)\ell_j i_t}, \sum_{t=1}^{s}\lambda_t\alpha_j^{((q-2)\ell_j+1)i_t}, \ldots, \sum_{t=1}^{s}\lambda_t\alpha_j^{((q-1)\ell_j-1)i_t} \end{pmatrix}$$

$$= \mathrm{Tr}_j \begin{pmatrix} \sum_{t=1}^{s} \lambda_t \xi^{-0i_t}, \sum_{t=1}^{s} (\lambda_t \alpha_j^{i_t}) \xi^{-0i_t}, \ldots, \sum_{t=1}^{s} (\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-0i_t} \\ \sum_{t=1}^{s} \lambda_t \xi^{-i_t}, \sum_{t=1}^{s} (\lambda_t \alpha_j^{i_t}) \xi^{-i_t}, \ldots, \sum_{t=1}^{s} (\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-i_t} \\ \vdots \\ \sum_{t=1}^{s} \lambda_t \xi^{-(q-2)i_t}, \sum_{t=1}^{s} (\lambda_t \alpha_j^{i_t}) \xi^{-(q-2)i_t}, \ldots, \sum_{t=1}^{s} (\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-(q-2)i_t} \end{pmatrix}$$

$$= \mathrm{Tr}_1 \begin{pmatrix} \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t) \xi^{-0i_t}, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{i_t}) \xi^{-0i_t}, \ldots, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-0i_t} \\ \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t) \xi^{-i_t}, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{i_t}) \xi^{-i_t}, \ldots, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-i_t} \\ \vdots \\ \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t) \xi^{-(q-2)i_t}, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{i_t}) \xi^{-(q-2)i_t}, \ldots, \sum_{t=1}^{s} \mathrm{Tr}^j(\lambda_t \alpha_j^{(\ell_j-1)i_t}) \xi^{-(q-2)i_t} \end{pmatrix},$$

where Tr^j denotes the trace map from $\mathbb{F}_{q^j}$ to $\mathbb{F}_q$. Note that we use $\mathbb{F}_q$-linearity of Tr^j and the fact that $\mathrm{Tr}_j = \mathrm{Tr}_1 \circ \mathrm{Tr}^j$ above. Now, set

$$\beta_1 = \left(\mathrm{Tr}^j(\lambda_1 \alpha_j^{ei_1})\right)_{0 \le e \le \ell_j - 1}, \beta_2 = \left(\mathrm{Tr}^j(\lambda_2 \alpha_j^{ei_2})\right)_{0 \le e \le \ell_j - 1}, \ldots, \beta_s = \left(\mathrm{Tr}^j(\lambda_s \alpha_j^{ei_s})\right)_{0 \le e \le \ell_j - 1}.$$

Observe that each β_i lies in $\mathbb{F}_q^{\ell_j}$. Then, with the notation of Theorem 4.1 we can write c as

$$\begin{pmatrix} c_0(\beta_1, \ldots, \beta_s) \\ c_1(\beta_1, \ldots, \beta_s) \\ \vdots \\ c_{q-2}(\beta_1, \ldots, \beta_s) \end{pmatrix},$$

where for all $g = 0, 1, \ldots, q-2$, we have

$$c_g = c_g(\beta_1, \ldots, \beta_s) = \sum_{t=1}^{s} \mathrm{Tr}_1\big(\beta_t \xi^{-gi_t}\big).$$

Note that $m = q - 1$ for all of the codes C_j. The polynomial $x^{q-1} - 1$ splits in $\mathbb{F}_q$. Therefore, each field $\mathbb{E}_i$ is an intermediate field of the extension $\mathbb{F}_q/\mathbb{F}_r$. If for some $k \in \{1, \ldots, s\}$, the r-cyclotomic coset mod $q - 1$ for i_k has length strictly less than $u = [\mathbb{F}_q : \mathbb{F}_r]$ (i.e. $\mathbb{E}_k \subsetneq \mathbb{F}_q$), then we can write the corresponding summand above as

$$\mathrm{Tr}_1\big(\beta_k \xi^{-gi_k}\big) = \mathrm{Tr}_{\mathbb{E}_k/\mathbb{F}_r}\big(\beta_k' \xi^{-gi_k}\big),$$

where

$$\beta_k' = \left(\mathrm{Tr}_{\mathbb{F}_{q^j}/\mathbb{E}_k}\big(\lambda_k \alpha_j^{ei_k}\big)\right)_{0 \le e \le \ell_j - 1} \in \mathbb{E}_k^{\ell_j}.$$

Hence, we obtain the following result from Theorem 4.1.

Theorem 4.3. *Let $j \ge 2$ and C_j be the QC code defined in (3.4). For $k \in \{1, \ldots, s\}$,*

(i) *if $\mathbb{E}_k = \mathbb{F}_q$, then the corresponding constituent $D_k \subset \mathbb{F}_q^{\ell_j}$ is*

$$D_k = \{(\mathrm{Tr}^j(\lambda \alpha_j^{ei_k}))_{0 \le e \le \ell_j - 1} : \lambda \in \mathbb{F}_q\}.$$

(ii) *if $\mathbb{E}_k \subsetneq \mathbb{F}_q$, then the corresponding constituent $D_k \subset \mathbb{E}_k^{\ell_j}$ is*

$$D_k = \{(\mathrm{Tr}_{\mathbb{F}_{q^j}/\mathbb{E}_k}(\lambda \alpha_j^{ei_k}))_{0 \le e \le \ell_j - 1} : \lambda \in \mathbb{F}_q\}.$$

We note that those constituents which are defined over $\mathbb{F}_q$ have dimension 0 or 1.

5. Applications

We present some applications of Theorem 3.1 to some specific codes here, and one application to permutation polynomials. Note that Oort (see [10]) has shown that there are no hyperelliptic supersingular curves of genus 3 in characteristic 2. So our first two applications concern genus 2 and 4. Let us also note that if we choose $q = r^u$ big enough, then r-cyclotomic cosets modulo $q - 1$ have cardinality u. This fact will be used below.

5.1. BCH codes and subcodes

Let α be a primitive element in the finite field $\mathbb{F}_q$, where $q = 2^u$. The binary cyclic code of length $2^u - 1$ with three zeros $\alpha, \alpha^3, \alpha^5$ has dimension $2^u - 1 - 3u$, and minimum distance 7, and is called the binary 3-error-correcting BCH code. If u is odd, the dual code of this BCH code is known to have five nonzero weights, which are

$$2^{u-1}, 2^{u-1} \pm 2^{(u-1)/2}, 2^{u-1} \pm 2^{(u+1)/2}, \tag{5.1}$$

and the weight distribution is determined. If u is even, the dual code of this BCH code is known to have seven nonzero weights, which are

$$2^{u-1}, 2^{u-1} \pm 2^{u/2-1}, 2^{u-1} \pm 2^{u/2}, 2^{u-1} \pm 2^{u/2+1}, \tag{5.2}$$

and the weight distribution is known here too (see [7, Chapter 21]).

The trace description of the dual code of this BCH code of length $q - 1$ states that all codewords have the form

$$c(\lambda_1, \lambda_2, \lambda_3) = \left(\mathrm{Tr}_1(\lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5)\right)_{x \in \mathbb{F}_q^*}$$

for $\lambda_i \in \mathbb{F}_q$. As we described in Section 3, this code is the first in a sequence of binary quasi-cyclic codes C_j of lengths $q^j - 1$, defined by

$$C_j := \left\{ \left(\mathrm{Tr}_j \left(\lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5\right)\right)_{x \in \mathbb{F}_{q^j}^*} : \lambda_i \in \mathbb{F}_q \right\}. \tag{5.3}$$

These codes correspond to the hyperelliptic curves

$$y^2 + y = \lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5$$

which are known to be supersingular, and have genus 2 provided $\lambda_3 \neq 0$ (see Proposition 2.3). Moreover by Remark 3.3, C_j is a subcode in the dual $\tilde{C}_j$ of the binary 3-error correcting BCH code of length $q^j - 1$.

We wish to point out an interesting consequence of Theorem 3.1.

Theorem 5.1. *Let $q = 2^u$, where u is odd. Continuing with the notation of this subsection, the code C_j (for any even j) does not contain a codeword of weight $2^{ju-1} \pm 2^{ju/2-1}$.*

Proof. Note again that C_j is a subcode of $\tilde{C}_j$, which is the dual of the BCH code of length $2^{ju} - 1$. By (5.2), possible weights in C_j are

$$2^{ju-1}, 2^{ju-1} \pm 2^{ju/2-1}, 2^{ju-1} \pm 2^{ju/2}, 2^{ju-1} \pm 2^{ju/2+1}.$$

However, by Theorem 3.1, all weights in the subcode C_j are divisible by $2^{ju/2}$. It follows that the weights $2^{ju-1} \pm 2^{ju/2-1}$ do not occur in C_j. □

Theorem 3.1 has therefore shown that for even j, the quasi-cyclic subcode C_j of the length $2^{ju} - 1$ dual-BCH code has a higher weight divisibility than one might expect, and this divisibility eliminates certain weights. We do not know any other way of proving this. We note that weights are not eliminated in C_j when j is odd. We also remark that the minimum weight is not among the eliminated weights, so the subcode does not have a higher minimum weight than the original cyclic code.

5.2. Genus 4 curves and subcodes

Let α be a primitive element in the finite field $\mathbb{F}_q$, where $q = 2^u$. The binary cyclic code of length $2^u - 1$ with four zeros $\alpha, \alpha^3, \alpha^5, \alpha^9$, has dimension $2^u - 1 - 4u$. If u is odd, the dual code of this code is known to have seven nonzero weights [14, Theorem 4] and (3.3), which are

$$2^{u-1}, 2^{u-1} \pm 2^{(u-1)/2}, 2^{u-1} \pm 2^{(u+1)/2}, 2^{u-1} \pm 2^{(u+3)/2}. \tag{5.4}$$

By a similar argument to [14], one can show that if u is even, the dual code has weights

$$2^{u-1}, 2^{u-1} \pm 2^{u/2-1}, 2^{u-1} \pm 2^{u/2}, 2^{u-1} \pm 2^{u/2+1}, 2^{u-1} \pm 2^{u/2+2}. \tag{5.5}$$

Following Section 3, these codes correspond to the curves

$$y^2 + y = \lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5 + \lambda_4 x^9$$

which are known to be supersingular, (see Proposition 2.3). Therefore we can apply Theorem 3.1, and we conclude that if $q = 2^u$ with u odd, then the quasi-cyclic codes C_j for j even have all weights divisible by $q^{j/2}$. Therefore they do *not* have the weights $q^{j-1} \pm q^{j/2-1}$ that one might expect from (5.5).

5.3. Higher genus

Let α be a primitive element in the finite field $\mathbb{F}_q$, where $q = 2^u$. The binary cyclic code of length $2^u - 1$ with three zeros $\alpha, \alpha^3, \alpha^{13}$, has dimension $2^u - 1 - 3u$. Curves (1.1) corresponding to the dual code are of genus 6 and they are supersingular (see Proposition 2.3). This is the motivating example given in the introduction. If u is odd, it was shown in [2] that the dual code has the same weight distribution as the 3-error-correcting BCH code. When u is even, this is still an open problem and the weight distribution is not known. If we apply Theorem 3.1 to the sequence of codes C_j (for odd u), we conclude (as in Sections 5.1 and 5.2) that the weights $q^{j-1} \pm q^{j/2-1}$ do not occur in C_j when j is even.

For some higher genus examples, from Proposition 2.3 the curves

$$y^2 + y = \sum_{i=0}^{d} \lambda_i x^{2^i+1}$$

are supersingular, where the λ_i come from a finite field of characteristic 2. These are curves of genus 2^{d-1}. Sections 5.1 and 5.2 are the $d = 2$ and $d = 3$ cases, respectively. For a general d, one can draw similar conclusions to those in Sections 5.1 and 5.2 from Theorem 3.1. The codes here are subcodes of the second-order Reed–Muller code, because the exponents have the form $2^i + 1$, and the weight distributions of such codes have been studied before (see [7] for details).

5.4. Linearized polynomials as permutation polynomials

We wish to point out an unusual consequence of our results for a class of linearized polynomials. Let $a, b, c \in \mathbb{F}_q$, where $q = 2^u$, and let

$$S_j := \sum_{x \in \mathbb{F}_{q^j}} (-1)^{\mathrm{Tr}_j(ax+bx^3+cx^5)}.$$

If we let X be the curve over $\mathbb{F}_q$ defined by the equation

$$y^2 + y = ax + bx^3 + cx^5,$$

then the sum S_j above is equal to $N_j - (q^j + 1)$. Hence, the notation is consistent with the notation of Section 2.

Squaring S_j, and for notational purposes letting $\chi_j(t) = (-1)^{\mathrm{Tr}_j(t)}$, gives

$$S_j^2 = \sum_{x,y \in \mathbb{F}_{q^j}} \chi_j(ax + bx^3 + cx^5 + ay + by^3 + cy^5).$$

Substituting $y = x + w$ and rearranging (using Galois invariance of the trace) we get

$$S_j^2 = \sum_{w \in \mathbb{F}_{q^j}} \chi_j(aw + bw^3 + cw^5) \left(\sum_{x \in \mathbb{F}_{q^j}} \chi_j(x^8 L_{b,c}(w)) \right), \tag{5.6}$$

where

$$L_{b,c}(w) = c^4 w^{16} + b^4 w^8 + b^2 w^2 + cw.$$

The inner sum has the form $\sum_{x \in \mathbb{F}_{q^j}} \chi_j(xL)$, and is a character sum over a group because χ_j is a character of the additive group of $\mathbb{F}_{q^j}$. This sum is therefore 0 unless $L_{b,c}(w) = 0$. Furthermore, the number of roots of $L_{b,c}(w)$ in $\mathbb{F}_{q^j}$ will determine the value of S_j.

Theorem 5.2. *Let $q = 2^u$ with u odd. The linearized polynomial*

$$L_{b,c}(w) = c^4 w^{16} + b^4 w^8 + b^2 w^2 + cw, \quad b, c \in \mathbb{F}_q$$

is not a permutation polynomial on $\mathbb{F}_{q^j}$ for j even.

Proof. By Theorem 7.9 in [15] $L_{b,c}(w)$ is a permutation of $\mathbb{F}_{q^j}$ if and only if the only root of $L_{b,c}(w)$ in $\mathbb{F}_{q^j}$ is 0. The only root of $L_{b,c}(w)$ in $\mathbb{F}_{q^j}$ is 0 if and only if $S_j^2 = q^j$, by (5.6). By Theorem 2.2 this is impossible because S_j would not be divisible by the required power of 2. □

Other similar theorems can be proved, where instead of using the polynomials $ax + bx^3 + cx^5$ (of Section 5.1) one can use more general polynomials $\sum_{i=0}^{d} \lambda_i x^{2^i+1}$ (of Section 5.3).

5.5. Exponential sum divisibility

For a field $\mathbb{F}_q$ of characteristic p, exponential sums of the form

$$\sum_{x\in\mathbb{F}_q} \chi(f(x))$$

where $f(x) \in \mathbb{F}_q[x]$ and χ is an additive character on $\mathbb{F}_q$, have been much studied (see [15] Chapter 5 for example). The p-divisibility of such sums is closely related to the divisibility of the number of rational points on Artin–Schreier type curves and to weight divisibility in codes. There are papers such as Moreno–Moreno [16] on this topic, proving that a certain power of p will divide the values of the sums as $f(x)$ ranges over a certain family of polynomials. Theorem 3.1 shows that for some (supersingular) families of polynomials $f(x)$, exponential sums of the type

$$\sum_{x\in\mathbb{F}_{q^j}} \chi(f(x))$$

where $f(x) \in \mathbb{F}_q[x]$ can have higher divisibility than they would have if $f(x) \in \mathbb{F}_{q^j}[x]$.

As an example to illustrate this, in [16] Moreno–Moreno consider the sum

$$S = \sum_{x\in\mathbb{F}_q} (-1)^{\mathrm{Tr}(f(x))},$$

where $q = 2^{3u}$, Tr denotes the trace from $\mathbb{F}_q$ to $\mathbb{F}_2$ and $f(x) \in \mathbb{F}_q[x]$ is of the form

$$f(x) = \lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5 + \alpha x^7 + \lambda_4 x^9. \tag{5.7}$$

Note that $S = N - (q+1)$, where N denotes the number of $\mathbb{F}_q$-rational points on the curve

$$y^2 + y = \lambda_1 x + \lambda_2 x^3 + \lambda_3 x^5 + \alpha x^7 + \lambda_4 x^9. \tag{5.8}$$

As mentioned in Section 5.3, (5.8) defines a supersingular curve if $\alpha = 0$. In that case Moreno–Moreno conclude in [16, Theorem 3] that S is divisible by 2^{u+1}.

If we now consider the same sum (or the curve) with coefficients from the subfield $\mathbb{F}_{2^u}$ (i.e. $f(x) \in \mathbb{F}_{2^u}[x]$) and again with $\alpha = 0$, then Theorem 2.2 implies that $S = S_3$ is divisible by $2^{(3u-1)/2}$ if u is odd and it is divisible by $2^{(3u-2)/2}$ if u is even. This shows a marked increase in the divisibility, from (approximately) the cube root of the field size to the square root.

More generally, following Section 5.3, the sums

$$\sum_{x\in\mathbb{F}_{q^j}} (-1)^{\mathrm{Tr}_j\left(\sum \lambda_i x^{2^i+1}\right)}$$

are divisible by a higher power of 2 when the λ_i's are in $\mathbb{F}_q$, than when the λ_i's are in $\mathbb{F}_{q^j}$.

We are not aware of another method to obtain such conclusions on exponential sums where the coefficients of polynomials involved come from a subfield.

6. The converse

One may ask whether the converse of Theorem 3.1 holds. In other words, is it possible to prove the supersingularity of certain Artin–Schreier type curves by proving that the related codes C_j satisfy certain divisibility conditions? This would be a very interesting application of coding theory since proving that a certain type of curve is supersingular is usually nontrivial. We outline some cases where the converse is true.

Theorem 6.1. *For $q = 2^u$ with u odd, let the family $\mathcal{F}$ be as in (3.1). For each $j \geq 1$, define the $\mathbb{F}_2$-linear code of length $q^j - 1 = 2^{ju} - 1$ as follows:*

$$C_j := \{(\mathrm{Tr}_j(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}))_{x\in\mathbb{F}^*_{q^j}} : \lambda_1, \ldots, \lambda_s \in \mathbb{F}_q\}. \tag{6.1}$$

Assume the following divisibility conditions on C_j:

$2^{\frac{ju}{2}}$ *divides all the weights in C_j for j even,*

$2^{\frac{ju-1}{2}}$ *divides all the weights in C_j for j odd.*

Assume that the family $\mathcal{F}$ consists of curves with maximal genus 3 (i.e. $i_s \leq 7$ in (3.1)). Then all curves in $\mathcal{F}$ are supersingular.

Proof. By (3.3), the assumptions imply the following about the S_j for members in a family of Artin–Schreier type curves of the form (3.1):

$$2^{\frac{ju}{2}+1} \text{ divides } S_j \text{ for } j \text{ even,}$$
$$2^{\frac{ju+1}{2}} \text{ divides } S_j \text{ for } j \text{ odd.}$$

We will show via (2.2) that the divisibility conditions on the coefficients of the L-polynomials (Lemma 2.1) for the members of $\mathcal{F}$ are satisfied. The first four equations are

$$a_0 = 1$$
$$S_1 = a_1$$
$$S_2 + a_1S_1 = 2a_2$$
$$S_2 + a_1S_2 + a_2S_1 = 3a_3.$$

Clearly $2^{(u+1)/2}$ divides a_1, which implies that 2^u divides a_2. In the final equation, each term on the left is divisible $2^{(3u+1)/2}$, which implies the same thing for a_3. □

Hence, equivalence of the weight divisibility conditions in Theorem 3.1 (for the special case $q = 2^u$ and u odd) and the supersingularity of the related curve family $\mathcal{F}$ is established for families with genus $g = 2$ and $g = 3$. In other words, the converse is true in those cases. However, for families which contain curves of higher genera, the divisibility conditions on codes in Theorem 3.1 are not strong enough to yield supersingularity of the related curve families. Hence the converse is still an open problem in general.

Remark 6.2. We point out why the proof breaks down with curves of genus 4. The next recursion is

$$S_4 + a_1S_3 + a_2S_2 + a_3S_1 = 4a_4. \tag{6.2}$$

The assumptions and proof of Theorem 6.1 lead to the conclusion that 2^{2u+1} divides all terms on the left hand side of (6.2). This implies that 2^{2u-1} divides a_4, whereas we require 2^{2u} dividing a_4 for supersingularity.

We know that genus 4 hyperelliptic curves (5.8) are supersingular if and only if $\alpha = 0$. Therefore the condition $\alpha = 0$ is somehow equivalent to the condition 2^{2u} dividing a_4. This equivalence is proved in [9].

Remark 6.3. Since the converse is true for genus 3 (with $q = 2^u$ and odd u), Theorem 3.1 is equivalent to supersingularity of the related family of curves. Oort's result says that there are no genus 3 supersingular hyperelliptic curves, so therefore we can conclude that the related code sequence does not have the divisibilities stated in Theorem 3.1. The curves in this case are the family

$$y^2 + y = \lambda_1x + \lambda_2x^3 + \lambda_3x^5 + \alpha x^7$$

which are hyperelliptic, and have 2-rank 0, but are not supersingular if $\alpha \neq 0$. The 2-rank is the dimension of the 2-torsion subgroup in the Jacobian, and supersingularity implies that the 2-rank is 0 but the converse is not true for genus $\geq$3.

Acknowledgments

The first author was partially supported by TÜBİTAK project 111T234. The second author's research was supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

References

[1] G. McGuire, An alternative proof of a result on the weight divisibility of a cyclic code using supersingular curves, Finite Fields Appl. 18 (2) (2012) 434–436.

[2] X. Zeng, J. Shan, L. Hu, A triple-error-correcting cyclic code from the Gold and Kasami–Welch APN power functions, Finite Fields Appl. 18 (1) (2012) 70–92.

[3] G. van der Geer, M. van der Vlugt, Reed–Muller codes and supersingular curves I, Compos. Math. 84 (3) (1992) 333–367.

[4] R. Schoof, Families of curves and weight distribution of codes, Bull. Amer. Math. Soc. 32 (2) (1995) 171–183.

[5] J. Wolfmann, New bounds on cyclic codes from algebraic curves, in: Lecture Notes in Computer Science, vol. 388, Springer-Verlag, New York, 1989, pp. 47–62.

[6] H. Stichtenoth, Algebraic Function Fields and Codes, in: GTM, vol. 254, Springer-Verlag, Berlin, 2009.

[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, in: North-Holland Mathematical Library, vol. 16, 1977.

[8] J. Scholten, H.J. Zhu, Slope estimates of Artin–Schreier curves, Compos. Math. 137 (3) (2003) 275–292.

[9] J. Scholten, H.J. Zhu, Hyperelliptic curves in characteristic 2, Int. Math. Res. Not. 17 (2002) 905–917.

[10] K.-Z. Li, F. Oort, Moduli of Supersingular Abelian Varieties, in: Lecture Notes Math., vol. 1680, Springer-Verlag, 1998.

[11] J. Scholten, H.J. Zhu, Families of supersingular curves in characteristic 2, Math. Res. Lett. 9 (2002) 639–650.

[12] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Trans. Inform. Theory 47 (2001) 2751–2760.

[13] C. Güneri, F. Özbudak, A relation between quasi-cyclic codes and 2-D cyclic codes, Finite Fields Appl. 18 (1) (2012) 123–132.

[14] G. McGuire, A. Zaytsev, The number of rational points on hyperelliptic supersingular curves of genus 4 in characteristic 2, Finite Fields and their Applications 18 (2012) 886–893.

[15] R. Lidl, H. Niederreiter, Finite Fields, in: Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, MA, 1983.

[16] O. Moreno, C. 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 (6) (1994) 1894–1907.