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, Sabancı University, 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 α, α^3, α^{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*

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

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*

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

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