

Zeta Functions of a Class of Artin–Schreier Curves with Many Automorphisms

Irene Bouw, Wei Ho, Beth Malmskog, Renate Scheidler,
Padmavathi Srinivasan, and Christelle Vincent

Abstract This paper describes a class of Artin–Schreier curves, generalizing results of Van der Geer and Van der Vlugt to odd characteristic. The automorphism group of these curves contains a large extraspecial group as a subgroup. Precise knowledge of this subgroup makes it possible to compute the zeta function of the curves in this class over the field of definition of all automorphisms in the subgroup.

Keywords Zeta function • Artin-Schreier curves • Extraspecial groups • Maximal curves

2010 *Mathematics Subject Classification*. Primary: 14G10; Secondary: 11G20, 14H37

I. Bouw (✉)

Institute of Pure Mathematics, Ulm University, D-89069 Ulm, Germany
e-mail: irene.bouw@uni-ulm.de

W. Ho

Department of Mathematics, University of Michigan, 530 Church Street,
Ann Arbor, MI 48109, USA
e-mail: weiho@umich.edu

B. Malmskog

Department of Mathematics and Statistics, Villanova University, 800 Lancaster Avenue,
Villanova, PA 19085, USA
e-mail: beth.malmskog@villanova.edu

R. Scheidler

Department of Mathematics and Statistics, University of Calgary, 2500 University
Drive NW, Calgary, AB, Canada T2N 1N4
e-mail: rscheidl@ucalgary.ca

P. Srinivasan

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts
Avenue, Cambridge, MA 02139, USA
e-mail: padma_sk@math.mit.edu

C. Vincent

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Avenue,
Burlington, VT 05401, USA
e-mail: christelle.vincent@uvm.edu

1 Introduction

In [24], Van der Geer and Van der Vlugt introduced a class of Artin–Schreier curves over a finite field with a highly rich structure. For example, these curves have a very large automorphism group that contains a large extraspecial p -group as a subgroup. Results of Lehr–Matignon [15] show that the automorphism groups of these curves are “maximal” in a precise sense. (Lehr–Matignon call this a *big action*.) A further remarkable property is that all these curves are supersingular. This yields an easy way of producing large families of supersingular curves.

In [24], the authors explore these curves and their Jacobians over fields of characteristic 2. In this case, there is an intriguing connection between the curves in this class and the weight enumerator of Reed–Müller codes, which was their original motivation for investigating this family of curves. In Sect. 13 of [24], they sketched extensions of some of their results to odd characteristic, but few details are given. The present paper extends the main results and strategy of [24] to the corresponding class of curves in odd characteristic, providing full details and proofs.

The main difference between the two cases is that the aforementioned extraspecial group of automorphisms has exponent p in the case of odd characteristic p , whereas the exponent is 4 in characteristic 2. As a result, some of the arguments in the odd characteristic case are more involved than those of [24]. Moreover, we have streamlined the reasoning of [24] and combined it with ideas from [15] to describe the automorphism group of the curves under investigation.

Arguably the most important object associated to an algebraic curve is its zeta function since it encodes a large amount of information about the curve, including point counts. Our main result is Theorem 8.4 which computes the zeta function of the members of the family of curves under consideration over a sufficiently large field. This not only generalizes the corresponding result in [24] for characteristic 2, but we also note that the authors of [24] do not offer an odd-characteristic analogue in their paper.

The most prominent member of the family of curves considered in this paper is the Hermite curve H_p (Example 9.5), which is well known to be a maximal curve over fields of square cardinality. We discuss other members of the family that are maximal in Sect. 9. More examples along the same lines have also been found by Çakçak and Özbudak in [3].

We now describe the contents of this paper in more detail. Let p be an odd prime and $R(X) \in \mathbb{F}_p[X]$ be an additive polynomial of degree p^h , i.e., for indeterminates X and Y we have $R(X + Y) = R(X) + R(Y)$. We denote by C_R the smooth projective curve given by the Artin–Schreier equation

$$Y^p - Y = XR(X).$$

The key to the structure of the curve C_R is the bilinear form $\text{Tr}(XR(Y) + YR(X))$, introduced in Sect. 2, whose kernel W is characterized in Proposition 2.1, Part 2. We obtain an expression for the number of points of C_R over a finite field in terms of W . Over a sufficiently large field \mathbb{F}_q of square cardinality, we conclude that

the curve C_R is either maximal or minimal, i.e., either the upper or lower Hasse–Weil bound is attained (Theorem 2.5 and Part 2 of Remark 8.2). To determine which of these cases applies, we use the automorphisms of C_R .

In Sects. 3 and 4, we show that W also determines a large p -subgroup P of the group of automorphisms (Theorem 4.3). With few exceptions, P is the Sylow p -subgroup of $\text{Aut}(C_R)$ (Theorem 4.4). It is an extraspecial group of exponent p and order p^{2h+1} , where $\deg(R) = p^h$ (Theorem 5.3).

In general, the size of the automorphism group restricts the possibilities for the number of rational points of a curve. In our situation, there is a concrete relationship, since both the automorphisms and the rational points of C_R may be described in terms of the space W . We establish a point-counting result that applies to the smallest field \mathbb{F}_q over which all automorphisms in P are defined.

The determination of the zeta function of C_R over \mathbb{F}_q (Theorem 8.4) relies on a decomposition result for the Jacobian $J(C_R)$ of C_R (Proposition 6.3) that is an application of a result of Kani–Rosen [12]. More precisely, we show that $J(C_R)$ is isogenous over \mathbb{F}_q to the product of Jacobians of quotients of C_R by suitable subgroups of P over \mathbb{F}_q (Proposition 6.3). These quotient curves are twists of the curve C_{R_0} with $R_0(X) = X$ (Theorem 7.4) for which we may determine the zeta function by explicit point counting. Putting everything together yields a precise expression for the zeta function of C_R .

Our results also yield explicit examples of maximal curves (Sect. 9). The main technical difficulty here is determining the field \mathbb{F}_q over which all automorphisms in P are defined.

1.1 Notation

Let p denote an odd prime, \mathbb{F}_p be the finite field of order p , and $k = \overline{\mathbb{F}_p}$ be the algebraic closure of \mathbb{F}_p . All curves under consideration are assumed to be smooth, projective, and absolutely irreducible. Consider the curve C_R defined by the affine equation

$$Y^p - Y = XR(X), \tag{1}$$

where

$$R(X) = \sum_{i=0}^h a_i X^{p^i} \in \mathbb{F}_{p^r}[X]$$

is a fixed additive polynomial of degree p^h with $h \geq 0$ and whose coefficient field is denoted \mathbb{F}_{p^r} . Note that R is additive, i.e., $R(X + Y) = R(X) + R(Y)$ in $\mathbb{F}_{p^r}[X]$. Thus, C_R is defined over \mathbb{F}_{p^r} and has genus

$$g(C_R) = \frac{p^h(p-1)}{2}.$$

Of interest will be the polynomial $E(X)$ derived from $R(X)$ via

$$E(X) = (R(X))^{p^h} + \sum_{i=0}^h (a_i X)^{p^{h-i}} \in \mathbb{F}_{p^r}[X] \quad (2)$$

with zero locus

$$W = \{c \in k : E(c) = 0\}. \quad (3)$$

Note that the formal derivative of $E(X)$ with respect to X is the constant nonzero polynomial a_h , so $E(X)$ is a separable additive polynomial of degree p^{2h} with coefficients in \mathbb{F}_{p^r} . It follows that W is an \mathbb{F}_p -vector space of dimension $2h$. When $h = 0$, i.e., $R(X) = a_0 X$, we have $W = \{0\}$.

We denote by \mathbb{F}_q the splitting field of $E(X)$, so $W \subset \mathbb{F}_q$. In Sect. 4 of this paper we will define and investigate a subgroup P of the group of automorphisms of C_R , and the automorphisms contained in P will be defined over this field \mathbb{F}_q .

For convenience, we summarize the most frequently used notation in Table 1.

2 The Kernel of the Bilinear Form Associated to C_R

Let \mathbb{F}_{p^s} be any extension of \mathbb{F}_{p^r} . For each s a multiple of r , we associate to the curve C_R the s -ary quadratic form

$$x \mapsto \mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(x))$$

on \mathbb{F}_{p^s} , where $\mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p} : \mathbb{F}_{p^s} \rightarrow \mathbb{F}_p$ is the trace from the s -dimensional vector space \mathbb{F}_{p^s} down to \mathbb{F}_p . The associated symmetric bilinear form on $\mathbb{F}_{p^s} \times \mathbb{F}_{p^s}$ is

$$(x, y) \mapsto \frac{1}{2} \mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)), \quad (4)$$

with kernel

$$W(\mathbb{F}_{p^s}) = \{c \in \mathbb{F}_{p^s} : \mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(y) + yR(c)) = 0 \text{ for all } y \in \mathbb{F}_{p^s}\}. \quad (5)$$

Note that $W(\mathbb{F}_{p^s})$ is a vector space over \mathbb{F}_p . The following characterizations and properties of $W(\mathbb{F}_{p^s})$ will turn out to be useful:

Proposition 2.1. *Let $c \in \mathbb{F}_{p^s}$. Then the following hold:*

1. *If $c \in W(\mathbb{F}_{p^s})$, then $\mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(c)) = 0$.*
2. *We have $c \in W(\mathbb{F}_{p^s})$ if and only if there exists a polynomial $B(X) \in \mathbb{F}_{p^s}[X]$ with*

$$B(X)^p - B(X) = cR(X) + R(c)X. \quad (6)$$

Table 1 Frequently used notation

Symbol	Meaning and place of definition
p	An odd prime
\mathbb{F}_{p^r}	Field of definition of $R(X)$ and of C_R (Sect. 1.1)
\mathbb{F}_{p^s}	An arbitrary extension of \mathbb{F}_{p^r} (Sect. 2)
\mathbb{F}_q	$\mathbb{F}_q \supseteq \mathbb{F}_{p^r}$ splitting field of $E(X)$ (Sect. 1.1)
$k = \overline{\mathbb{F}}_p$	Algebraic closure of \mathbb{F}_p (Sect. 1.1)
C_R	The curve $C_R : Y^p - Y = XR(X)$ over \mathbb{F}_{p^r} (Eq. 1)
\overline{C}_A	Quotient curve C_R/A (Theorem 7.4)
$R(X)$	$R(X) = \sum_{i=0}^h a_i X^{p^i} \in \mathbb{F}_{p^r}[X]$ an additive polynomial (Eq. 1)
$E(X)$	$E(X) = (R(X))^{p^h} + \sum_{i=0}^h (a_i X)^{p^{h-i}} \in \mathbb{F}_{p^r}[X]$ (Eq. 2)
b, c	Elements in k with $b^p - b = cR(c)$ (Remark 3.3)
$B_c(X) = B(X)$	Polynomial s.t. $B(X)^p - B(X) = cR(X) + R(c)X$ (Eqs. 6 and 11)
$W(\mathbb{F}_{p^s})$	$W(\mathbb{F}_{p^s}) = \{c \in \mathbb{F}_{p^s} : \text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(y) + y(R(c))) = 0 \text{ for all } y \in \mathbb{F}_{p^s}\}$ (Eq. 5)
W	$W = W(\mathbb{F}_q)$, space of zeros of $E(X)$ (Eq. 3)
$S(f)$	$S(f) = \{(a, c, d) \in k^* \times k \times \mathbb{F}_p^* : \text{there is } g \in k[X] \text{ s. t. } f(aX + c) - df(X) = g(X)^p - g(X)\}$ (Eq. 10)
$\text{Aut}^0(C_R)$	Group of automorphisms of C_R that fix ∞ (Sect. 4)
$\sigma_{a,b,c,d}$	Automorphism in $\text{Aut}^0(C_R)$ (Eq. 15)
$\sigma_{b,c}$	$\sigma_{b,c} = \sigma_{1,b,c,1}$ (Sect. 5)
ρ	Artin–Schreier automorphism, $\rho = \sigma_{1,1,0,1}$ (following Eq. 15)
P	Sylow p -subgroup of $\text{Aut}^0(C_R)$ (Theorem 4.3)
H	$H = \text{Aut}^0(C_R)/P$ (Theorem 4.3)
$Z(G)$	Center of a group G
$E(p^3)$	Extraspecial group of order p^3 and exponent p (Corollary 5.4)
\mathcal{A}	A maximal abelian subgroup of P (Proposition 5.5)
J_R	$J_R = \text{Jac}(C_R)$, the Jacobian variety of C_R
$J \sim_{\mathbb{F}} J'$	The ab. var. J and J' are isogenous over the field \mathbb{F} (Sect. 6).
$L_{C,\mathbb{F}}(T)$	Numerator of the zeta function of the curve C over the field \mathbb{F} (Sect. 8)

Moreover, there is a unique solution $B_c(X) \in X\mathbb{F}_{p^s}[X]$ to Eq. (6), and

- a. The polynomial $B_c(X)$ is additive.
 - b. Every solution $B(X)$ of (6) is of the form $B(X) = B_c(X) + \beta$ for some $\beta \in \mathbb{F}_p$.
 - c. If $c_1, c_2 \in W(\mathbb{F}_{p^s})$, then $B_{c_1+c_2}(X) = B_{c_1}(X) + B_{c_2}(X)$.
3. We have $c \in W(\mathbb{F}_{p^s})$ if and only if $E(c) = 0$, where $E(X)$ is the polynomial of (2) with zero locus W as defined in (3). In other words, $W(\mathbb{F}_{p^s}) = W \cap \mathbb{F}_{p^s}$.

Proof.

1. Let $c \in W(\mathbb{F}_{p^s})$. Then substituting $y = c$ into (5) yields $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(2cR(c)) = 0$. Since $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(X)$ is \mathbb{F}_p -linear and p is odd, this forces $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(c)) = 0$.

2. The proof of Part 2 is analogous to that of Proposition 3.2 of [24]. Assume that $c \in W(\mathbb{F}_{p^s})$. We show the existence of a solution B of (6), and show that statements 2a–2c hold.

We first recursively define numbers b_i using the following formulas:

$$b_0 = -ca_0 - R(c), \quad (7)$$

$$b_i = -ca_i + b_{i-1}^p \quad \text{for } 1 \leq i \leq h-1, \quad (8)$$

and set $B_c(X) = \sum_{i=0}^{h-1} b_i X^{p^i}$. Then $B_c(X) \in X\mathbb{F}_{p^s}[X]$, $B_c(X)$ is additive, and $B_{c_1+c_2}(X) = B_{c_1}(X) + B_{c_2}(X)$ for all $c_1, c_2 \in W(\mathbb{F}_{p^s})$. Furthermore, a simple calculation reveals that

$$B_c^p(X) - B_c(X) = cR(X) + R(c)X + \epsilon X^{p^h}$$

with $\epsilon = b_{h-1}^p - ca_h \in \mathbb{F}_{p^s}$. Note that $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(B_c(y)^p - B_c(y)) = 0$ for all $y \in \mathbb{F}_{p^s}$ by the additive version of Hilbert's Theorem 90.

If $c \in W(\mathbb{F}_{p^s})$, then $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(y) + yR(c)) = 0$ for all $y \in \mathbb{F}_{p^s}$, therefore $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(\epsilon y^{p^h}) = 0$, which forces $\epsilon = 0$. Hence $B_c(X)$ satisfies (6), and

$$b_{h-1}^p = ca_h. \quad (9)$$

Moreover, if $B(X)$ is any solution to (6), then $(B(X) - B_c(X))^p = B(X) - B_c(X)$, so $B(X) - B_c(X) \in \mathbb{F}_p$.

Conversely, if (6) has a solution $B(X) \in \mathbb{F}_{p^s}[X]$, then

$$0 = \text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(B(y)^p - B(y)) = \text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(cR(y) + R(c)y)$$

for all $y \in \mathbb{F}_{p^s}$, so $c \in W(\mathbb{F}_{p^s})$.

3. This result is stated for p odd in Proposition 13.1 and proved for $p = 2$ in Proposition 3.1 of [24]. It is also addressed in Remark 4.15 of the preprint [14] (the explicit statement is not included in [15], but can readily be deduced from the results therein).

□

Remark 2.2. The characteristic-2 analogue of Part 2 of Proposition 2.1 can be found in Sect. 3 of [24]. We also note that Part 1 of Proposition 2.1 does not hold in characteristic $p = 2$ in general (see Sect. 5 of [24]).

Part 3 of Proposition 2.1 immediately establishes the following corollary:

Corollary 2.3. $W(\mathbb{F}_{p^s}) \subseteq W$, with equality for any extension \mathbb{F}_{p^s} of the splitting field \mathbb{F}_q of E .

We conclude this section with a connection between the \mathbb{F}_p -dimension of the space $V_s = \mathbb{F}_{p^s}/W(\mathbb{F}_{p^s})$ and the number of \mathbb{F}_{p^s} -rational points on the curve C_R .

This is obtained by projecting the bilinear form (4) onto V_s . We write $\bar{x} = x + W(\mathbb{F}_{p^s})$ for the elements in V_s . Proposition 2.6 below is one of the key ingredients in the determination of the zeta function of C_R over \mathbb{F}_q (Theorem 8.4).

Proposition 2.4. *Define a map Q_s on $V_s \times V_s$ via*

$$Q_s(\bar{x}, \bar{y}) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)).$$

Then Q_s is a non-degenerate bilinear form on $V_s \times V_s$.

Proof. We begin by showing that Q_s is well-defined. Let $x_1, x_2 \in \mathbb{F}_{p^s}$. Then

$$\begin{aligned} \bar{x}_1 = \bar{x}_2 &\iff x_1 - x_2 \in W(\mathbb{F}_{p^s}) \\ &\iff \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}((x_1 - x_2)R(y) + yR(x_1 - x_2)) = 0 \text{ for all } y \in \mathbb{F}_{p^s} \\ &\iff \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(x_1R(y) + yR(x_1)) = \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(x_2R(y) + yR(x_2)) \text{ for all } y \in \mathbb{F}_{p^s} \\ &\iff Q_s(\bar{x}_1, \bar{y}) = Q_s(\bar{x}_2, \bar{y}) \text{ for all } \bar{y} \in V_s. \end{aligned}$$

Similarly, one obtains that $\bar{y}_1 = \bar{y}_2$ if and only if $Q_s(\bar{x}, \bar{y}_1) = Q_s(\bar{x}, \bar{y}_2)$ for all $\bar{x} \in V_s$. So if $(\bar{x}_1, \bar{y}_1) = (\bar{x}_2, \bar{y}_2)$, then $Q_s(\bar{x}_1, \bar{y}_1) = Q_s(\bar{x}_1, \bar{y}_2) = Q_s(\bar{x}_2, \bar{y}_2)$.

It is obvious that Q_s is bilinear. To establish non-degeneracy, let $\bar{x} \in V_s$ with $Q_s(\bar{x}, \bar{y}) = 0$ for all $\bar{y} \in V_s$. Then $\operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)) = 0$ for all $y \in \mathbb{F}_{p^s}$, so $x \in W(\mathbb{F}_{p^s})$, and hence $\bar{x} = \bar{0}$. \square

It follows that the quadratic form $\bar{x} \mapsto Q_s(\bar{x}, \bar{x})$ on V_s is non-degenerate. Therefore, its zero locus

$$\{\bar{x} \in V_s : \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(x)) = 0\}$$

defines a smooth quadric over \mathbb{F}_p .

In [11], Joly provides a formula for the cardinality of the zero locus of a non-degenerate quadratic form, which we reproduce here for the convenience of the reader. The case of n odd is treated in Chap. 6, Sect. 3, Proposition 2.7, and the case of n even is Proposition 2.9 of Chap. 6, Sect. 3. Note that in [11], the result is proved for forms over an arbitrary finite field, but we restrict to \mathbb{F}_p here which is sufficient for our purpose.

Theorem 2.5 (Joly [11]). *Let $a_1X_1^2 + \cdots + a_nX_n^2$ be a non-degenerate quadric in n variables with coefficients in \mathbb{F}_p , and N be the cardinality of its zero locus. Then*

$$N = \begin{cases} p^{n-1} & \text{if } n \text{ is odd,} \\ p^{n-1} + (p^{n/2} - p^{n/2-1}) & \text{if } n \text{ is even and } (-1)^{n/2}a_1 \cdots a_n \in (\mathbb{F}_p^*)^2, \\ p^{n-1} - (p^{n/2} - p^{n/2-1}) & \text{if } n \text{ is even and } (-1)^{n/2}a_1 \cdots a_n \notin (\mathbb{F}_p^*)^2. \end{cases}$$

Applying this result to the quadric $x \mapsto \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(x))$ on the space $\mathbb{F}_{p^s}/W(\mathbb{F}_{p^s})$, we obtain the following point count for the curve C_R . This result is already presented in [24], but we include it here to provide a proof.

Proposition 2.6 (Proposition 13.4 of [24]). *Let $w_s = \dim_{\mathbb{F}_p}(W(\mathbb{F}_{p^s}))$ and $n_s = s - w_s$. Then the number of \mathbb{F}_{p^s} -rational points on C_R is*

$$\#C_R(\mathbb{F}_{p^s}) = \begin{cases} p^s + 1 & \text{for } n_s \text{ odd,} \\ p^s + 1 \pm (p - 1)\sqrt{p^{s+w_s}} & \text{for } n_s \text{ even,} \end{cases}$$

with the sign depending on the coefficients of the quadratic form Q_s .

Proof. We have $V_s = \mathbb{F}_{p^s}/W(\mathbb{F}_{p^s}) \simeq \mathbb{F}_p^{n_s}$, where $n_s = s - w_s$. Therefore, for $\bar{x} \in V_s$, we may write $\bar{x} = (x_1, \dots, x_{n_s})$, with each $x_i \in \mathbb{F}_p$. In this way, $Q_s(\bar{x}, \bar{x})$ on the space V_s is a non-degenerate quadric in n_s variables with coefficients in \mathbb{F}_p . Furthermore, it is diagonalizable by Chap. 8, Theorem 3.1 of [5] since p is odd, and therefore can be written in the form $\sum_{i=1}^{n_s} a_i X_i^2$ with $a_i \in \mathbb{F}_p$ for $1 \leq i \leq n_s$. As a consequence we may apply Theorem 2.5 to obtain the cardinality of the set

$$\{\bar{x} \in V_s \simeq \mathbb{F}_p^{n_s} : Q_s(\bar{x}, \bar{x}) = 0\} = \{\bar{x} \in V_s : \text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(x)) = 0\}.$$

Each $\bar{x} \in V_s$ with $Q_s(\bar{x}, \bar{x}) = 0$ gives rise to p^{w_s} distinct values $x \in \mathbb{F}_{p^s}$ such that $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(x)) = 0$. For each of these $x \in \mathbb{F}_{p^s}$, we have p solutions y to the equation $y^p - y = xR(x)$. In addition to these points, C_R has one point at infinity which is defined over any extension of \mathbb{F}_{p^s} . Hence $\#C_R(\mathbb{F}_{p^s}) = p^{w_s+1}N + 1$ with N given as in Theorem 2.5 (with $n = n_s$). \square

Note that a more general version of Proposition 2.6 can be found in Theorem 4.1 of [4].

3 Connection to Automorphisms of C_R

In this section, we generalize the results of Proposition 2.1 to lay the groundwork for our investigation of the k -automorphisms of C_R that stabilize ∞ , the unique point at infinity on C_R . We follow Sect. 3 of [15], but our notation is slightly different. Similar results may also be found in [7].

We define for any polynomial $f(X) \in k[X]$ the set

$$S(f(X)) = \{(a, c, d) \in k^* \times k \times \mathbb{F}_p^* : \text{there exists } g(X) \in Xk[X] \text{ such that} \\ f(aX + c) - df(X) = g(X)^p - g(X)\}. \tag{10}$$

In our situation we take $f(X) = XR(X)$, where $R(X)$ is an additive polynomial of degree p^h . It is easy to verify that if $(a, c, d) \in S(XR(X))$ then the map $(x, y) \mapsto (ax + c, dy + g(x))$ is an automorphism of C_R that fixes ∞ . In fact, in Lemma 4.1 we will see that every automorphism of C_R that fixes ∞ is of this form. The elements in $S(XR(X))$, along with the polynomial $g(X)$, can be characterized explicitly as follows:

Proposition 3.1. *If $h = 0$, then $S(XR(X)) = \{(a, 0, a^2) : a^2 \in \mathbb{F}_p^*\}$.*

Proof. If $h = 0$, then $R(X) = a_0X$, so

$$(aX + c)R(aX + c) - dXR(X) = a_0((a^2 - d)X^2 + 2acX + c^2).$$

This polynomial is of the form $g(X)^p - g(X)$ if and only if $g(X)^p - g(X) = 0$, or equivalently, $a^2 = d$, $c = 0$ and $g(X) \in \mathbb{F}_p$. \square

Proposition 3.2.

1. *Assume that $h \geq 1$ and let $a \in k^*$, $c \in k$ and $d \in \mathbb{F}_p^*$. Then $(a, c, d) \in S(XR(X))$ if and only if there exists $B(X) \in Xk[X]$ such that*

$$cR(X) + R(c)X = B(X)^p - B(X), \quad (11)$$

and

$$aR(aX) = dR(X). \quad (12)$$

2. *If the equivalent conditions of Part 1 are fulfilled, then c and $B(X)$ satisfy the following conditions:*

- a. *We have that $c \in W$.*
- b. *The polynomial $B(X) = B_c(X)$ only depends on c and is uniquely determined by (11) and the condition that $B_c(X) \in Xk[X]$. It is an additive polynomial with coefficients in $\mathbb{F}_{p^r}(c) \subseteq \mathbb{F}_q$.*
- c. *The polynomial $B_c(X)$ is identically zero if and only if $c = 0$, and has degree p^{h-1} otherwise.*

3. *For a triple $(a, c, d) \in S(XR(X))$, all polynomials $g(X)$ as given in (10) are of the form*

$$g(X) = B_c(aX) + \frac{B_c(c)}{2} + i,$$

as i ranges over \mathbb{F}_p . In particular, each of these polynomials $g(X)$ has coefficients in $\mathbb{F}_q(a)$.

Proof.

1. Let $(a, c, d) \in k^* \times k \times \mathbb{F}_p^*$. Suppose first that there exists $B(X) \in Xk[X]$ satisfying (11), and that a and d satisfy (12). Then for any $b \in k$ such that $b^p - b = cR(c)$, we have

$$\begin{aligned} (aX + c)R(aX + c) - dXR(X) &= X(aR(aX) - dR(X)) + cR(aX) + aXR(c) + cR(c) \\ &= B(aX)^p - B(aX) + b^p - b, \end{aligned}$$

and so we may take $g(X) = B(aX) + b$ to show that $(a, c, d) \in S(XR(X))$.

Conversely, suppose that $(a, c, d) \in S(XR(X))$. Then there exists a polynomial $g(X) \in k[X]$ such that

$$X(aR(aX) - dR(X)) + cR(aX) + aR(c)X + cR(c) = g(X)^p - g(X).$$

Writing $g(X) = b + \widetilde{B}(X)$ with $\widetilde{B}(X) \in Xk[X]$, we see that this is equivalent to the existence of a polynomial $\widetilde{B}(X) \in Xk[X]$ such that

$$\widetilde{B}(X)^p - \widetilde{B}(X) = XF(X) + G(X) \quad (13)$$

where $F(X) = aR(aX) - dR(X)$ and $G(X) = cR(aX) + aR(c)X$ are both additive polynomials. We note for future reference during the proof of Part 3 that this also implies $b^p - b = cR(c)$.

Note that (12) holds if and only if $F(X) = 0$, in which case $B(X) = \widetilde{B}(X/a) \in Xk[X]$ satisfies (11). Thus, it suffices to show that $(a, c, d) \in S(XR(X))$ implies $F(X) = 0$ to complete the proof of Part 1.

To this end, we note that all the monomials in $XF(X)$ and $G(X)$ are of the form X^{p^i+1} and X^{p^i} for $0 \leq i \leq h$. If $\widetilde{B}(X) = 0$, then this immediately forces $F(X) = G(X) = 0$, so assume that $\widetilde{B}(X) \neq 0$.

Comparing degrees in (13) shows that $\deg(\widetilde{B}) \leq p^{h-1}$. Put

$$\widetilde{B}(X) = \sum_{j=1}^{p^{h-1}} \tilde{b}_j X^j, \quad \tilde{b}_j \in k \text{ for } 1 \leq j \leq p^{h-1},$$

and consider the polynomial $\widetilde{B}(X)^p - \widetilde{B}(X)$. In this polynomial, the coefficient of X^j for $1 \leq j \leq p^h$ is

$$\begin{cases} -\tilde{b}_j & \text{when } p \nmid j, \\ \tilde{b}_{j/p}^p - \tilde{b}_j & \text{when } p \mid j \text{ and } j \leq p^{h-1}, \\ \tilde{b}_{p^{h-1}}^p & \text{when } j = p^h. \end{cases}$$

All coefficients of X^j for $j \neq p^i, p^i + 1$ must vanish. We conclude that the coefficients \tilde{b}_j of $\widetilde{B}(X)$ are zero for all $j \neq p^i, p^i + 1$, so we may write $\widetilde{B}(X) = XU(X) + V(X)$ where $U(X), V(X) \in k[X]$ are additive polynomials. Then (13) yields

$$X^p U(X)^p + V(X)^p - XU(X) - V(X) = XF(X) + G(X).$$

Except for the monomials in $X^p U(X)^p$, this polynomial identity only contains monomials of the form X^{p^i} and X^{p^i+1} ; the monomials in $X^p U(X)^p$ all take the form X^{p+p^i+1} . This forces $U(X) = 0$. Thus, $XF(X) = V(X)^p - V(X) - G(X)$ is additive, which is only possible if $F(X) = 0$.

2. The proof of Part 2 is now straightforward. We remark that Eq. (11) is identical to Eq. (6). Therefore 2a follows from Part 2 of Proposition 2.1, and $B(X)$ is identical to the polynomial $B_c(X)$ defined in that proposition since $B(X) \in Xk[X]$. Thus, $B(X)$ only depends on c and is unique, and we write $B_c(X)$ for this polynomial from now on. The additivity of $B_c(X)$ was already established in the proof of Part 1, since $B_c(X) = \widetilde{B}(X/a)$, and $\widetilde{B}(X) = V(X)$ is additive; note that it also follows from Part 2a of Proposition 2.1. Moreover, the coefficients of B_c satisfy (7)–(9) and thus belong to $\mathbb{F}_{p^r}(c)$. Part 1 and Corollary 2.3 imply that $\mathbb{F}_{p^r}(c) \subseteq \mathbb{F}_q$. This proves 2b.

If $c = 0$, then $B_c(X) = 0$. If $c \neq 0$, the polynomial $B_c(X)$ is obviously nonzero and (9) shows that $B_c(X)$ has degree p^{h-1} . This proves 2c.

3. Writing $g(X) = b + \widetilde{B}(X)$ with $\widetilde{B}(X) \in Xk[X]$ as in the proof of Part 1, we have already seen that $B_c(X) = \widetilde{B}(X/a)$, and b is any solution to the equation $b^p - b = cR(c)$. Any two such solutions differ by addition of an element in \mathbb{F}_p . Furthermore, since $2 \in \mathbb{F}_p^*$, it follows from (11) that $b = B_c(c)/2$ satisfies $b^p - b = cR(c)$, and the first statement of Part 3 follows. The second statement of Part 3 follows from Part 2b.

□

Remark 3.3. We repeat here a remark made in the proof since we will use this throughout the paper. For a triple $(a, c, d) \in S(XR(X))$, all polynomials $g(X)$ as given in (10) can be written as

$$g(X) = B_c(aX) + b,$$

where $B_c(aX) \in \mathbb{F}_q(a)[x]$, and $b \in k$ is a solution of the equation

$$b^p - b = cR(c). \quad (14)$$

Part 3 of Proposition 3.2 implies that every solution b of this equation is of the form $b = B_c(c)/2 + i$ with $i \in \mathbb{F}_p$.

4 Automorphism Group of C_R

In this section we apply the results of the previous section to study the group $\text{Aut}(C_R)$ of k -automorphisms of the curve C_R , and more particularly the subgroup $\text{Aut}^0(C_R)$ of automorphisms of C_R that fix the unique point at infinity, i.e., the unique point of C_R which does not belong to the affine curve defined by (1). The main result is Theorem 4.3, which describes $\text{Aut}^0(C_R)$.

Recall from Sect. 3 that to a triple $(a, c, d) \in S(XR(X))$ we associate the k -automorphism

$$\begin{aligned} \sigma_{a,b,c,d}: C_R &\rightarrow C_R \\ (x, y) &\mapsto (ax + c, dy + b + B_c(ax)) \end{aligned} \quad (15)$$

of C_R . Here b is a solution of the equation $b^p - b = cR(c)$ (see Remark 3.3) and B_c is as in Proposition 3.2. Note that $\sigma_{a,b,c,d}$ fixes the point ∞ . In the rest of the paper, we denote by

$$\rho(x, y) = \sigma_{1,1,0,1}(x, y) = (x, y + 1)$$

the Artin–Schreier automorphism of the curve C_R .

The following lemma summarizes some properties of the automorphisms $\sigma_{a,b,c,d}$:

Lemma 4.1. *With the above notation and assumptions, we have*

1. *Every element of the stabilizer $\text{Aut}^0(C_R)$ of the point ∞ is of the form $\sigma_{a,b,c,d}$ as in (15).*
2. *The automorphisms $\sigma_{1,b,c,1}$ with $(b, c) \neq (0, 0)$ have order p . For $(a, d) \neq (1, 1)$ the order of $\sigma_{a,b,c,d}$ is not a p -power.*

Proof. The lemma follows from Corollaries 3.4 and 3.5 in [15]. We recall the proof.

1. Part 1 follows from Proposition 3.3 of [15] in the case that $g(C_R) \geq 2$. (Since p is odd in our set-up and the genus of C_R is $p^h(p - 1)/2$, this only excludes the case that $h = 0$ and $p = 3$. This case is treated in the proof of Corollary 3.4 of [15].) Namely, let $\varphi \in \text{Aut}^0(C_R)$ be an automorphism of C_R fixing ∞ . Then the proof of Proposition 3.3 of [15] shows that there exists an isomorphism $\tilde{\varphi}: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ together with a commutative diagram

$$\begin{array}{ccc} C_R & \xrightarrow{\varphi} & C_R \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{\tilde{\varphi}} & \mathbb{P}^1, \end{array}$$

where the vertical maps are $(x, y) \mapsto x$.

The morphism $\tilde{\varphi}$ fixes $\infty \in \mathbb{P}^1$, hence it is an affine linear transformation and we may write it as $\tilde{\varphi}(x) = ax + c$ with $a \in k^*$ and $c \in k$. The commutative diagram above implies that $\varphi(x, y) = (ax + c, dy + g(x))$ for some $g(X) \in k[X]$ and $d \in k^*$. The assumption that φ fixes the point ∞ implies that $g(X) \in k[X]$ is a polynomial. The statement that $\varphi = \sigma_{a,b,c,d}$ follows since φ is assumed to be an automorphism of C_R .

2. To prove Part 2 we first remark that if $\sigma_{a,b,c,d}$ has p -power order, then $a = d = 1$, since 1 is the only p th root of unity in k . We show that every nontrivial automorphism $\sigma_{1,b,c,1}$ has order p .

We compute that

$$\sigma_{1,b,c,1}^p(x, y) = (x + pc, y + pb + B_c(x) + B_c(x + c) + \dots + B_c(x + (p - 1)c)).$$

Recall from Proposition 3.2 that B_c is an additive polynomial; in particular, its constant term vanishes. Hence

$$B_c(X) + B_c(X + c) + \cdots + B_c(X + (p - 1)c) = \sum_{i=0}^{p-1} B_c(ic) = \sum_{i=0}^{p-1} iB_c(c) = 0.$$

This implies that $\sigma_{1,b,c,1}^p = 1$.

□

Remark 4.2. Part 2 of Lemma 4.1 does not hold for $p = 2$. In [24], Theorem 4.1 it is shown that $\text{Aut}^0(C_R)$ always contains automorphisms of order 4 for $h \geq 1$ and $p = 2$. See also [15], Sect. 7.2 for a concrete example. In Remark 7.3 we give a few more details on the differences between the cases $p = 2$ and p odd.

The following result is Theorem 13.3 of [24], and describes the group $\text{Aut}^0(C_R)$. The structure of the Sylow p -subgroup P of $\text{Aut}^0(C_R)$ will be described in more detail in Sect. 5 below. Again, we include this result here to provide a proof.

Theorem 4.3 (Theorem 13.3 of [24]).

1. The group $\text{Aut}^0(C_R)$ has a unique Sylow p -subgroup, which we denote by P . It is the subgroup consisting of all automorphisms $\sigma_{1,b,c,1}$ and has cardinality p^{2h+1} .
2. The automorphisms $\sigma_{a,0,0,d}$ form a cyclic subgroup $H \subset \text{Aut}^0(C_R)$ of order

$$\frac{e(p - 1)}{2} \gcd_{\substack{i \geq 0 \\ a_i \neq 0}}(p^i + 1),$$

where $e = 2$ if all of the indices i such that $a_i \neq 0$ have the same parity, and $e = 1$ otherwise.

3. The group $\text{Aut}^0(C_R)$ is the semi-direct product of the normal subgroup P and the subgroup H .

Proof.

1. To prove Part 1, one easily checks that $\{\sigma_{1,b,c,1} : \sigma_{1,b,c,1} \in \text{Aut}^0(C_R)\}$ is a subgroup of $\text{Aut}^0(C_R)$. (This is similar to the proof of Lemma 5.2 below.) The statements on the order of $\sigma_{a,b,c,d}$ in Part 2 of Lemma 4.1 imply that P is the unique Sylow p -subgroup of $\text{Aut}^0(C_R)$, which implies that P is a normal subgroup.

Parts 2a and 3 of Proposition 3.2 imply that the cardinality of P is equal to $p\#W$. The last statement of Part 1 therefore follows from Part 3 of Proposition 2.1, since E is a separable polynomial of degree p^{2h} .

2. To prove Part 2, we consider all elements $(a, 0, d) \in S(XR(X))$. Part 2c of Proposition 3.2 implies that the polynomial B_0 corresponding to this tuple is zero. Part 2 of Proposition 3.2 therefore implies that $(a, 0, d) \in S(XR(X))$ if and only

if $aR(aX) = dR(X)$. This condition is equivalent to $d = a^{p^i+1}$ for all $0 \leq i \leq h$ with $a_i \neq 0$, as can be readily seen by comparing coefficients in $aR(aX)$ and $dR(X)$. Part 2 now follows immediately.

3. Note that the order of H is prime to p . In particular, we have $H \cap P = \{1\}$. Part 3 follows since $\text{Aut}^0(C_R)$ is generated by H and P .

□

For completeness we state the following theorem, which follows from [19], Satz 6 and Satz 7. (See also Theorem 3.1 of [15].) Since we study the automorphism group of C_R over the algebraically closed field k here, it is no restriction to assume that $R(X)$ is monic.

Theorem 4.4. *Let R be monic.*

1. Assume that $R(X) \notin \{X, X^p\}$. Then $\text{Aut}(C_R) = \text{Aut}^0(C_R)$.
2. If $R(X) = X^p$, then $\text{Aut}(C_R) \cong \text{PGU}_3(p)$.
3. If $R(X) = X$, then $\text{Aut}(C_R) \simeq \text{SL}_2(p)$.

For future reference we note the following result on the higher ramification groups of the point $\infty \in C_R$ in the cover $C_R \rightarrow C_R/\text{Aut}^0(C_R)$. For the definition of the higher ramification groups and their basic properties we refer to [18], Chap. 4 or [20], Chap. 3.

Lemma 4.5. *Let R be an additive polynomial of degree $h \geq 1$, and C_R as given in (1).*

1. The filtration of higher ramification groups in the lower numbering of $\text{Aut}^0(C_R)$ is

$$G = G_0 = \text{Aut}^0(C_R) \supsetneq P = G_1 \supsetneq G_2 = \cdots = G_{1+p^h} = \langle \rho \rangle \supsetneq \{1\}.$$

2. Let $H \subset \text{Aut}(C_R)$ be any subgroup which contains ρ . Then $g(C_R/H) = 0$.

Proof. To prove Part 1, write v_∞ for the valuation at the unique point ∞ at infinity and choose a uniformizing parameter t at ∞ . One easily computes that

$$v_\infty \left(\frac{\sigma(t) - t}{t} \right) = \begin{cases} 1 + p^h & \text{if } \sigma \in \langle \rho \rangle \setminus \{1\}, \\ 1 & \text{if } \sigma \in P \setminus \langle \rho \rangle. \end{cases}$$

This may also be deduced from the fact that the quotient of C_R by the subgroup generated by the Artin–Schreier automorphism $\rho(x, y) = (x, y + 1)$ has genus 0 ([16], Lemma 2.4).

Part 2 follows immediately from the fact that the function field of the curve $C_R/\langle \rho \rangle$ is $k(X)$. This can also be deduced from Part 1. □

5 Extraspecial Groups and the Structure of P

We now focus again on the subgroup P described in Part 1 of Theorem 4.3. Part 2 of Lemma 4.1 implies that the Sylow p -subgroup P of $\text{Aut}^0(C_R)$ consists precisely of the automorphisms $\sigma_{1,b,c,1}(x, y) = (x + c, y + b + B_c(x))$. For brevity, we simplify their notation to

$$\sigma_{b,c} = \sigma_{1,b,c,1}.$$

The main result of the section, Theorem 5.3, states that P is an extraspecial group. For more details on extraspecial groups we refer the reader to Chap. III.13 of [9] and [22]. Recall that we assume that p is an odd prime. The classification of extraspecial 2-groups is different from that for odd primes.

Definition 5.1. A noncommutative p -group G is *extraspecial* if its center $Z(G)$ has order p and the quotient $G/Z(G)$ is elementary abelian.

We denote by $E(p^3)$ the unique nonabelian group of cardinality p^3 and exponent p . It can be given by generators and relations as follows:

$$E(p^3) = \langle x, y \mid x^p = y^p = [x, y]^p = 1, [x, y] \in Z(E(p^3)) \rangle.$$

This group obviously is an extraspecial group.

The following lemma describes the commutation relation in P . The lemma contains the key steps to prove that P is an extraspecial group.

Lemma 5.2. *Assume that $h \geq 1$.*

1. *We have $[\sigma_{b_1,c_1}, \sigma_{b_2,c_2}] = \rho^{-\epsilon(c_1,c_2)}$, where*

$$\epsilon(c_1, c_2) = B_{c_1}(c_2) - B_{c_2}(c_1).$$

2. *We have $Z(P) = [P, P] = \langle \rho \rangle$. The quotient group $P/Z(P)$ is isomorphic to the space W defined in equation (3), where the isomorphism is induced by $\sigma_{b,c} \mapsto c$.*

3. *Any two non-commuting elements σ, σ' of P generate a normal subgroup $E_{\sigma,\sigma'} := \langle \sigma, \sigma' \rangle$ of P which is isomorphic to $E(p^3)$.*

Proof.

1. To prove Part 1, we compute that

$$\sigma_{b,c}^{-1}(x, y) = (x - c, y - b - B_c(x - c)).$$

We therefore have

$$\begin{aligned} \sigma_{b_1,c_1} \sigma_{b_2,c_2} \sigma_{b_1,c_1}^{-1} \sigma_{b_2,c_2}^{-1}(x, y) &= \sigma_{b_1,c_1} \sigma_{b_2,c_2} \sigma_{b_1,c_1}^{-1}(x - c_2, y - b_2 - B_{c_2}(x - c_2)) \\ &= \sigma_{b_1,c_1} \sigma_{b_2,c_2}(x - c_2 - c_1, y - b_2 - B_{c_2}(x - c_2) - b_1 - B_{c_1}(x - c_2 - c_1)) \\ &= \sigma_{b_1,c_1}(x - c_1, y - B_{c_2}(x - c_2) - b_1 - B_{c_1}(x - c_2 - c_1) + B_{c_2}(x - c_2 - c_1)) \end{aligned}$$

$$\begin{aligned}
 &= \sigma_{b_1,c_1}(x - c_1, y - b_1 - B_{c_1}(x - c_2 - c_1) - B_{c_2}(c_1)) \\
 &= (x, y - B_{c_1}(x - c_2 - c_1) - B_{c_2}(c_1) + B_{c_1}(x - c_1)) \\
 &= (x, y + B_{c_2}(c_1) - B_{c_1}(c_2)).
 \end{aligned}$$

Since $\sigma_{b_1,c_1}\sigma_{b_2,c_2}\sigma_{b_1,c_1}^{-1}\sigma_{b_2,c_2}^{-1}$ certainly belongs to $\text{Aut}^0(C_R)$, Part 1 of Lemma 4.1 implies that $\sigma_{b_1,c_1}\sigma_{b_2,c_2}\sigma_{b_1,c_1}^{-1}\sigma_{b_2,c_2}^{-1} = \sigma_{a,b,c,d}$ for some a, b, c , and d . From our computation above, $a = d = 1$ and $c = 0$. Since $c = 0$, by Part 2c of Proposition 3.2, $B_c(X) = 0$, which implies that $b = B_{c_2}(c_1) - B_{c_1}(c_2) \in \mathbb{F}_p$.

2. Part 1 shows that $[P, P] \subset \langle \rho \rangle$. Since P is noncommutative, we have equality. Because $\rho = \sigma_{1,0}$ and $B_0(X) = 0$ by Part 2c of Proposition 3.2, we have that for any $\sigma_{b,c}$,

$$\sigma_{b,c}\rho\sigma_{b,c}^{-1}\rho^{-1} = \rho^{B_c(0)} = 1,$$

since $B_c(X)$ is an additive polynomial and therefore has no constant term. Thus ρ commutes with every element of P , and $[P, P] = \langle \rho \rangle \subseteq Z(P)$.

To finish the proof of the first statement of Part 2, we now show that if $c_1 \neq 0$, then for each automorphism σ_{b_1,c_1} there exists an automorphism σ_{b_2,c_2} such that σ_{b_1,c_1} and σ_{b_2,c_2} do not commute. This shows that in fact $\langle \rho \rangle = Z(P)$.

Let $c_1 \in W \setminus \{0\}$. By Part 2 of Proposition 2.1 and Part 1 of Proposition 3.2, $(1, c_1, 1) \in S(XR(X))$ and by Part 2c of Proposition 3.2, $B_{c_1}(X)$ has degree p^{h-1} . Considering $c_2 =: C$ as a variable, the recursive formulas (7) and (8) for the coefficients b_i of B_C show that $\deg_C(b_i) \leq p^{h+i}$. We conclude that the degree of $\epsilon(c_1, C)$, when considered as polynomial in C , is at most p^{2h-1} . Since the cardinality of W is p^{2h} , it follows that there exists a $c_2 \in W$, and therefore $\sigma_{b_2,c_2} \in P$, such that $\epsilon(c_1, c_2) \neq 0$. We conclude that $Z(P) = \langle \rho \rangle$.

Since $\rho\sigma_{b,c} = \sigma_{b+1,c}$, it follows from Part 3 of Proposition 3.2 that the map

$$P \rightarrow W, \quad \sigma_{b,c} \mapsto c$$

is a surjective group homomorphism with kernel $\langle \rho \rangle$.

3. Let $\sigma := \sigma_{b_1,c_1}, \sigma' := \sigma_{b_2,c_2} \in P$ be two non-commuting elements, and write $\epsilon = \epsilon(c_1, c_2)$. Part 1 implies that $\sigma\sigma' = \rho^{-\epsilon}\sigma'\sigma$. Since σ, σ' , and ρ have order p (Part 2 of Lemma 4.1), it follows that σ and σ' generate a subgroup $E(\sigma, \sigma')$ of order p^3 of P , which contains $Z(P) = \langle \rho \rangle$. Since the exponent of this subgroup is p , it is isomorphic to $E(p^3)$.

For an arbitrary element $\sigma_{b,c} \in P$, Part 1 implies that $\sigma_{b,c}\sigma\sigma_{b,c}^{-1} \in \langle \rho, \sigma \rangle \subset E(\sigma, \sigma')$, and similarly for σ' replacing σ . Thus $E(\sigma, \sigma')$ is a normal subgroup, proving Part 3. □

Theorem 5.3. *Assume that $h \geq 1$. Then the group P is an extraspecial group of exponent p .*

Proof. Since $h \geq 1$, Part 2 of Lemma 5.2 shows that P is an extraspecial group. Part 2 of Lemma 4.1 yields that P has exponent p . □

We now show that P is a central product of h copies of $E(p^3)$, i.e., P is isomorphic to the quotient of the direct product of h copies of $E(p^3)$, where the centers of each copy have been identified. These subgroups of P of order p^3 have been described in Part 3 of Lemma 5.2.

Corollary 5.4. *Assume that $h \geq 1$. Then P is a central product of h copies of $E(p^3)$.*

Proof. Theorem III.13.7.(c) of [9] states that P is the central product of h extraspecial groups P_i of order p^3 . Since P has exponent p , it follows that the groups P_i have exponent p as well. Therefore $P_i \simeq E(p^3)$. \square

We describe the decomposition of P as a central product from Corollary 5.4 explicitly; this description is in fact the proof given in Theorem III.13.7.(c) of [9]. The proof of Part 2 of Lemma 5.2 shows that $\epsilon(c_1, c_2)$ defines a non-degenerate symplectic pairing

$$W \times W \rightarrow \mathbb{F}_p, \quad (c_1, c_2) \mapsto \epsilon(c_1, c_2).$$

We may choose a basis $(c_1, \dots, c_h, c'_1, \dots, c'_h)$ of W such that

$$\epsilon(c_i, c'_j) = \delta_{ij},$$

where δ_{ij} is the Kronecker function. In particular, it follows that $\langle c_1, \dots, c_h \rangle \subset W$ is a maximal isotropic subspace of the bilinear form ϵ .

For every i , choose elements $\sigma_i, \sigma'_i \in P$ which map to c_i, c'_i , respectively, under the quotient map from Part 2 of Lemma 5.2. This corresponds to choosing an element b_i as in Part 3 of Proposition 3.2 for each i . Part 1 of Lemma 5.2 implies that σ_i does not commute with σ'_i , but commutes with σ_j, σ'_j for every $j \neq i$. Therefore $E_i = \langle \sigma_i, \sigma'_i \rangle$ is isomorphic to $E(p^3)$ (Part 3 of Lemma 5.2). It follows that P is the central product of the subgroups E_i .

We finish this section with a description of the maximal abelian subgroups of P . This will be used in Sect. 6 to obtain a decomposition of the Jacobian of C_R .

Proposition 5.5. *Let $h \geq 1$.*

1. *Every maximal abelian subgroup \mathcal{A} of P is an elementary abelian group of order p^{h+1} , and is normal in P .*
2. *Let $\mathcal{A} \simeq (\mathbb{Z}/p\mathbb{Z})^{h+1}$ be a maximal abelian subgroup of P . For any subgroup $A = A_p \simeq (\mathbb{Z}/p\mathbb{Z})^h \subset \mathcal{A}$ with $A_p \cap Z(P) = \{1\}$ there exist subgroups A_1, \dots, A_{p-1} of \mathcal{A} such that*

$$\mathcal{A} = Z(P) \cup A_1 \cup \dots \cup A_p,$$

$$A_i \simeq (\mathbb{Z}/p\mathbb{Z})^h, \quad A_i \cap Z(P) = \{1\}, \quad A_i \cap A_j = \{1\} \text{ if } i \neq j.$$

3. *Any two subgroups A of \mathcal{A} of order p^h which trivially intersect the center of P are conjugate inside P .*

Proof.

1. The statement that the maximal abelian subgroups \mathcal{A} of P have order p^{h+1} is Theorem III.13.7.(e) of [9].
2. A maximal abelian subgroup \mathcal{A} is the inverse image of a maximal isotropic subspace of W . Since P has exponent p , we conclude that $\mathcal{A} \simeq (\mathbb{Z}/p\mathbb{Z})^{h+1}$ is elementary abelian. Part 1 of Lemma 5.2 and the fact that \mathcal{A} is the inverse image of a maximal isotropic subspace of W imply that \mathcal{A} is a normal subgroup of P . This proves Part 1.

Let $\mathcal{A} \subset P$ be a maximal abelian subgroup. Without loss of generality, we may assume that \mathcal{A} corresponds to the maximal isotropic subspace generated by the basis elements c_1, \dots, c_h of W as described above. In this case we have $\mathcal{A} = \langle \rho, \sigma_1, \dots, \sigma_h \rangle$ where σ_i maps to c_i under the map from Part 2 of Lemma 5.2. Define

$$A_p := \langle \sigma_1, \dots, \sigma_h \rangle.$$

This is a subgroup of \mathcal{A} of order p^h such that $A_p \cap Z(P) = \{1\}$.

We define $\tau = \sigma_{b \cdot c'_1 + \dots + c'_h}$, where b is some solution of the equation

$$b^p - b = (c'_1 + \dots + c'_h)R(c'_1 + \dots + c'_h)$$

as specified in Remark 3.3. Let

$$A_i = \tau^i A_p \tau^{-i}, \quad i = 1, \dots, p-1.$$

By Part 2a of Proposition 2.1, $B_c(X)$ is additive in c . This implies that

$$B_{c'_1 + \dots + c'_h}(X) = \sum_{i=1}^h B_{c'_i}(X).$$

The choice of the basis c_i, c'_i of W , together with Part 1 of Lemma 5.2 implies therefore that

$$\tau \sigma_i \tau^{-1} = \rho^{-\epsilon(c'_i, c_i)} \sigma_i = \rho^{\epsilon(c_i, c'_i)} \sigma_i = \rho \sigma_i.$$

It follows that $A_i \cap Z(P) = \{1\}$ and $A_i \cap A_j = \{1\}$ if $i \neq j$. By counting, we see that each non-identity element of \mathcal{A} is contained in exactly one A_i .

3. Let A, A' be two subgroups of \mathcal{A} as in the statement of Part 3. Without loss of generality, we may assume that $A = A_p = \langle \sigma_1, \dots, \sigma_h \rangle$, as in the proof of Part 2. Then $A' = \langle \rho^{j_1} \sigma_1, \dots, \rho^{j_h} \sigma_h \rangle$ for suitable $j_i \in \mathbb{F}_p$. Define $c = \sum_{i=1}^h j_i c_i \in W$ and choose b with $b^p - b = B_c(c)/2$. As in the proof of Part 2 it follows that $\tau := \sigma_{b \cdot c}$ satisfies $\tau A \tau^{-1} = A'$.

□

6 Decomposition of the Jacobian of C_R

In this section we decompose the Jacobian of C_R over the splitting field \mathbb{F}_q of the polynomial E . This decomposition allows us to reduce the calculation of the zeta function of C_R over \mathbb{F}_q to that of a certain quotient curve. This quotient curve is computed in Sect. 7, and Sect. 8 combines these results to compute the zeta function of C_R over \mathbb{F}_q .

The decomposition result (Proposition 6.3) we prove below is based on the following general result of Kani–Rosen, Theorem B of [12]:

Theorem 6.1 (Kani–Rosen [12]). *Let C be a smooth projective curve defined over an algebraically closed field k , and G a (finite) subgroup of $\text{Aut}_k(C)$ such that $G = H_1 \cup H_2 \cup \dots \cup H_t$, where the subgroups $H_i \leq G$ satisfy $H_i \cap H_j = \{1\}$ for $i \neq j$. Then we have the isogeny relation*

$$\text{Jac}(C)^{t-1} \times \text{Jac}(C/G)^g \sim \text{Jac}(C/H_1)^{h_1} \times \dots \times \text{Jac}(C/H_t)^{h_t},$$

where $g = \#G$, $h_i = \#H_i$, and $\text{Jac}^n = \text{Jac} \times \dots \times \text{Jac}$ (n times).

We apply Theorem 6.1 to a maximal abelian subgroup $\mathcal{A} \subset P$. Recall from Part 1 of Proposition 5.5 that \mathcal{A} is an elementary abelian p -group of order p^{h+1} which contains the center $Z(P) = \langle \rho \rangle$ of P . Part 3 of Proposition 3.2 implies that all automorphisms in \mathcal{A} are defined over \mathbb{F}_q .

Recall from Part 2 of Proposition 5.5 the existence of a decomposition

$$\mathcal{A} = A_0 \cup A_1 \cup \dots \cup A_p, \tag{16}$$

where $A_0 = \langle \rho \rangle$ is the center of P and for $i \neq 0$ the A_i are elementary abelian p -groups of order p^h .

Each group A_i defines a quotient curve $\overline{C}_{A_i} := C_R/A_i$. Since all automorphisms in A_i are defined over \mathbb{F}_q , it follows that the quotient curve \overline{C}_{A_i} together with the natural map $\pi_{A_i}: C_R \rightarrow \overline{C}_{A_i}$ may also be defined over \mathbb{F}_q . The following lemma implies that all curves \overline{C}_{A_i} are isomorphic over \mathbb{F}_q :

Lemma 6.2. *Let \mathcal{A} be a maximal abelian subgroup of P , and let A and A' be two subgroups of \mathcal{A} of order p^h which have trivial intersection with the center of P . Then the curves C_R/A and C_R/A' are isomorphic over \mathbb{F}_q .*

Proof. Part 3 of Proposition 5.5 states that the subgroups A and A' are conjugate inside P . Namely, we have $A' = \tau A \tau^{-1}$ for an explicit element $\tau \in P$. The automorphism τ of C_R induces an isomorphism

$$\tau: C_R/A \rightarrow C_R/A'.$$

Since τ is defined over \mathbb{F}_q , this isomorphism is defined over \mathbb{F}_q as well. \square

We write $J_R := \text{Jac}(C_R)$ for the Jacobian variety of C_R . Since C_R is defined over \mathbb{F}_q and has an \mathbb{F}_q -rational point, the Jacobian variety J_R is also defined over \mathbb{F}_q . The map π_{A_i} induces \mathbb{F}_q -rational isogenies

$$\pi_{A_i,*}: J_R \rightarrow \text{Jac}(\overline{C}_{A_i}), \quad \pi_{A_i}^*: \text{Jac}(\overline{C}_{A_i}) \rightarrow J_R. \tag{17}$$

The element

$$\varepsilon_{A_i} = \frac{1}{p^h} \pi_{A_i}^* \circ \pi_{A_i,*} \in \text{End}^0(J_R) := \text{End}(J_R) \otimes \mathbb{Q}$$

is an idempotent (Sect. 2 of [12]) and satisfies the property that $\varepsilon_{A_i}(J_R)$ is isogenous to $\text{Jac}(\overline{C}_{A_i})$. Note that p^h is the degree of the map π_{A_i} .

In the following result we use these idempotents to decompose J_R . The same strategy was also used in Sect. 10 of [24] in the case that $p = 2$. In that source, Van der Geer and Van der Vlugt give a direct proof in their situation of the result of Kani–Rosen (Theorem 6.1) that we apply here.

Proposition 6.3. *There exists an \mathbb{F}_q -isogeny*

$$J_R \sim_{\mathbb{F}_q} \text{Jac}(\overline{C}_{A_p})^{p^h}.$$

Proof. We apply Theorem 6.1 to the decomposition (16) of a maximal abelian subgroup \mathcal{A} of P . This result shows the existence of a k -isogeny

$$J_R^p \times \text{Jac}(C_R/\mathcal{A})^{p^{h+1}} \sim_k \text{Jac}(\overline{C}_{A_0})^p \times \prod_{i=1}^p \text{Jac}(\overline{C}_{A_i})^{p^h}. \tag{18}$$

The groups \mathcal{A} and A_0 contain the Artin–Schreier element ρ ; hence the curves C_R/\mathcal{A} and \overline{C}_{A_0} have genus zero (Part 2 of Lemma 4.5). Therefore the Jacobians of these curves are trivial and may be omitted from (18).

As before, let $\varepsilon_{A_i} \in \text{End}(J_R)$ denote the idempotent corresponding to A_i . Theorem 2 of [12] states that the isogeny relation from (18) is equivalent to the relation

$$p \text{ Id} \sim p^h \left(\sum_{i=1}^p \varepsilon_{A_i} \right) \in \text{End}^0(J_R).$$

Here, as defined on p. 312 of [12], the notation $a \sim b$ means that $\chi(a) = \chi(b)$ for all virtual characters of $\text{End}^0(J_R)$. Since $\text{End}^0(J_R)$ is a \mathbb{Q} -algebra, we may divide by p on both sides of this relation. Applying Theorem 2 of [12] once more yields the isogeny relation

$$J_R \sim_k \prod_{i=1}^p \text{Jac}(\overline{C}_{A_i})^{p^{h-1}}. \tag{19}$$

We have already seen that the isogenies $\pi_{A_i}^*$ and $\pi_{A_i,*}$ are defined over \mathbb{F}_q . It follows that the isogeny (19) is defined over \mathbb{F}_q as well (see also Remark 6 in Sect. 3 of [12]). Since the curves \overline{C}_{A_i} , and hence also their Jacobians, are isomorphic (Lemma 6.2), the statement of the proposition follows. \square

7 Quotients of C_R by Elementary Abelian p -Groups

We consider again a maximal abelian subgroup $\mathcal{A} \simeq (\mathbb{Z}/p\mathbb{Z})^{h+1}$ of P and choose $A \subset \mathcal{A}$ with $A \simeq (\mathbb{Z}/p\mathbb{Z})^h$ and $A \cap Z(P) = \{1\}$. In this section we compute an \mathbb{F}_q -model of the quotient curve $\overline{C}_A = C_R/A$. Lemma 6.2 implies that the \mathbb{F}_q -isomorphism class of the quotient curve does not depend on the choice of the subgroup A .

Since $A \cap Z(P) = \{1\}$, Part 1 of Lemma 4.5 implies that the filtration of higher ramification groups in the lower numbering of A is

$$A = G_0 = G_1 \supsetneq G_2 = \{1\},$$

so the Riemann–Hurwitz formula yields

$$2g(C_R) - 2 = p^h(p - 1) - 2 = (2g(\overline{C}_A) - 2)p^h + 2(p^h - 1).$$

We conclude that $g(\overline{C}_A) = (p - 1)/2$.

Proposition 5.5 implies that the elements of A commute with ρ , since $\rho \in Z(P)$. It follows that \overline{C}_A is an Artin–Schreier cover of the projective line branched at one point. Artin–Schreier theory implies therefore that \overline{C}_A may be given by an Artin–Schreier equation

$$Y^p - Y = f_A(X),$$

where $f_A(X)$ is a polynomial of degree 2. Theorem 7.4 below implies that this polynomial $f_A(X)$ is in fact of the form $f_A(X) = a_A X^2$ for an explicit constant a_A . These curves are all isomorphic over the algebraically closed field k , but not over \mathbb{F}_q . The following lemma describes the different \mathbb{F}_q -models of the curves $Y^p - Y = eX^2$ for $e \in \mathbb{F}_q$.

Lemma 7.1. *For $e \in \mathbb{F}_q$, define the curve D_e by the affine equation*

$$Y^p - Y = eX^2. \tag{20}$$

Two curves D_{e_1} and D_{e_2} as in (20) are isomorphic over \mathbb{F}_q if and only if e_1/e_2 is the product of a square in \mathbb{F}_q^ with an element of \mathbb{F}_p^* . In particular, over $\overline{\mathbb{F}_q}$, any two of these curves are isomorphic.*

Proof. Let D_{e_1} and D_{e_2} be curves of the form (20). Suppose there exists an \mathbb{F}_q -isomorphism $\varphi: D_{e_1} \rightarrow D_{e_2}$. We claim that there exists an \mathbb{F}_q -isomorphism which sends $\infty \in D_{e_1}$ to $\infty \in D_{e_2}$.

We first consider the case that $p > 3$, i.e., $g(D_{e_i}) \geq 2$. In this case, Proposition 3.3 of [15] states that there exists an automorphism σ of D_{e_1} over $\overline{\mathbb{F}}_q$ such that $\varphi \circ \sigma$ sends the point $\infty \in D_{e_1}$ to the point $\infty \in D_{e_2}$. To prove the claim it suffices to show that σ may be defined over \mathbb{F}_q .

To prove this, we follow the proof of Proposition 3.3 of [15] and use the fact that φ maps every point of D_{e_1} to a point of D_{e_2} with the same polar semigroup. Theorem 3.1.(a) of [15] implies that the only points of D_{e_1} with the same polar semigroup as ∞ are the points $Q_i := (0, i)$ with $i \in \mathbb{F}_p$. It follows that $\varphi^{-1}(\infty)$ is either ∞ or Q_i for some $i \in \mathbb{F}_p$. In the former case, there is nothing to show. If $\varphi^{-1}(\infty) = Q_i$, we may choose

$$\sigma(x, y) = \left(\frac{x}{y^{(p+1)/2}}, \frac{iy - 1}{y} \right).$$

Note that this is an automorphism of D_{e_1} which maps ∞ to Q_i . Moreover, σ is defined over the field of definition of D_{e_1} , and we are done.

We now prove the claim in the case that $p = 3$. In this case the curves D_{e_i} are elliptic curves. The inverse $\varphi^{-1}: D_{e_2} \rightarrow D_{e_1}$ of φ is also defined over \mathbb{F}_q . It follows that $Q := \varphi^{-1}(\infty) \in D_{e_1}(\mathbb{F}_q)$ is \mathbb{F}_q -rational. Then the translation $\tau_{Q-\infty}: P \mapsto P + Q - \infty$ is defined over \mathbb{F}_q and sends the unique point $\infty \in D_{e_1}$ to Q . Precomposing φ with $\tau_{Q-\infty}$ gives an \mathbb{F}_q -isomorphism which sends $\infty \in D_{e_1}$ to $\infty \in D_{e_2}$.

Therefore, without loss of generality we let $\varphi: D_{e_1} \rightarrow D_{e_2}$ be an \mathbb{F}_q -isomorphism which sends the unique point of D_{e_1} at ∞ to the unique point of D_{e_2} at ∞ . Any such automorphism can be written as $\varphi(x, y) = (v_0x + v_1, v_2y + v_3)$ with $v_i \in \mathbb{F}_q$ and $v_2v_0 \neq 0$. The condition that φ maps D_{e_1} to D_{e_2} is equivalent to

$$v_2^p = v_2, \quad v_2e_1 = e_2v_0^2, \tag{21}$$

$$0 = 2e_2v_0v_1, \quad v_3^p - v_3 = e_2v_1^2. \tag{22}$$

It follows that $v_1 = 0$ and $v_2, v_3 \in \mathbb{F}_p$. The coefficient e_2 is given by

$$e_2 = \frac{v_2e_1}{v_0^2}.$$

This proves the first assertion of the lemma. The second assertion is clear since any element of $\overline{\mathbb{F}}_q^*$ is a square in $\overline{\mathbb{F}}_q^*$. \square

We now compute an \mathbb{F}_q -model of the curve C_R/A for $A \subset P$ an elementary abelian subgroup of cardinality p^h with $A \cap Z(P) = \{1\}$. We prove this by induction on h , following Sect. 13 of [24]. The following proposition is the key step in the inductive argument. It is a corrected version of Proposition 13.5 of [24], which extends to odd p Proposition 9.1 of [24] and is presented without proof. Indeed,

the formula for the coordinate V of the quotient curve given in Proposition 13.5 of [24] contains an error that has been corrected here. We recall that $R(X)$ is an additive polynomial of degree p^h with leading coefficient $a_h \in \mathbb{F}_{p^r} \subseteq \mathbb{F}_q$.

Proposition 7.2. *Assume that $h \geq 1$, and let*

$$\sigma(x, y) := \sigma_{b,c}(x, y) = (x + c, y + b + B_c(x))$$

be an automorphism of C_R with $c \neq 0$ and $b = B_c(c)/2$. Then the quotient curve $C_R/\langle\sigma\rangle$ is isomorphic over \mathbb{F}_q to the smooth projective curve given by an affine equation

$$V^p - V = \tilde{f}(U) = U\tilde{R}(U), \quad (23)$$

where $\tilde{R}(U) \in \mathbb{F}_q[U]$ is an additive polynomial of degree p^{h-1} with leading coefficient

$$\tilde{a} = \begin{cases} \frac{a_h}{c^{p-1}} & \text{if } h \neq 1, \\ \frac{a_h}{2c^{p-1}} & \text{if } h = 1. \end{cases}$$

Proof. In the proof c is fixed, therefore we write $B(X)$ for $B_c(X)$. We define new coordinates

$$U = X^p - c^{p-1}X, \quad V = -Y + \Psi(X) = -Y + \gamma X^2 + \frac{X}{c}B(X), \quad (24)$$

where γ is defined by

$$\gamma = -\frac{B(c)}{2c^2}.$$

One easily checks that U and V are invariant under σ . The invariance of V under σ is equivalent to the property

$$\Psi(X + c) - \Psi(X) = B(X) + b.$$

Here we use the definition of b as $b = B(c)/2$. Since U and V generate a degree- p subfield of the function field of C_R and the automorphism σ has order p , U and V generate the function field of the quotient curve $C_R/\langle\sigma\rangle$.

From the definition of U and V above, one can see that the Artin–Schreier automorphism ρ induces an automorphism $\tilde{\rho}(U, V) = (U, V - 1)$ on the quotient curve $C_R/\langle\sigma\rangle$. It follows that the quotient curve is also given by an Artin–Schreier equation, which we may write as

$$V^p - V = -Y^p + Y + \Psi^p(X) - \Psi(X) = -XR(X) + \Psi^p(X) - \Psi(X). \quad (25)$$

It is clear that the right-hand side of (25) can be written as a polynomial $\tilde{f}(U)$ in U , since it is invariant under σ by construction. Since the constant term of Ψ is zero, the right-hand side has a zero at $X = 0$, so $\tilde{f}(U) \in U\mathbb{F}_q[U]$.

Recall that Part 1 of Proposition 3.2 established

$$B(X)^p - B(X) = cR(X) + XR(c). \quad (26)$$

This implies

$$XR(X) = \frac{X(B(X)^p - B(X))}{c} - \frac{X^2R(c)}{c}.$$

It follows that

$$-XR(X) + \Psi^p(X) - \Psi(X) = \frac{B(X)^p}{c^p}U + \gamma^p X^{2p} + X^2 \left(\frac{R(c)}{c} - \gamma \right). \quad (27)$$

Using (26) one computes

$$\gamma^p X^{2p} + X^2 \left(\frac{R(c)}{c} - \gamma \right) = \gamma^p U^2 - \frac{B(c)^p}{c^{p+1}} XU.$$

Define

$$\Theta(X) = \frac{B(X)^p}{c^p} - \frac{B(c)^p}{c^{p+1}} X.$$

Since Θ is invariant under σ , we may write $\Theta(X) = \theta(U)$ as a polynomial in U . Note that $\theta(0) = 0$ since $\Theta(0) = 0$. The additivity of the polynomials B and U in the variable X implies that the polynomial θ is additive in the variable U . It follows that we may write $\theta(U) = \sum_{i=0}^{h-1} \mu_i U^i$. From (9), we deduce that the leading coefficient of θ is

$$\mu_{h-1} = \frac{b_{h-1}^p}{c^p} = \frac{a_h}{c^{p-1}}.$$

Altogether, we find

$$V^p - V = \tilde{f}(U) = U(\theta(U) + \gamma^p U).$$

Setting $\tilde{R}(U) := \theta(U) + \gamma^p U$, we see that $\tilde{R}(U)$ is an additive polynomial in U . The statement about the leading coefficient of $\tilde{R}(U)$ follows from the definitions of θ and γ . \square

Remark 7.3. We discuss a crucial difference between even and odd characteristic: Proposition 7.2 is a statement about the automorphisms $\sigma_{b,c}$ of order p which

are not contained in the center of P . For p odd all elements of $P \setminus Z(P)$ have order p . This is not true for $p = 2$, as we already noted in Remark 4.2. Indeed all extraspecial 2-groups contain elements of order 4. The precise structure of the extraspecial group P in the case that $p = 2$ can be found in Theorem 4.1 of [24]. The automorphisms $\sigma_{b,c} \in P \setminus Z(P)$ of order 2 are easily recognized: they satisfy $c \neq 0$ but $B_c(c) = 0$. This observation considerably simplifies the computation in the proof of Proposition 7.2.

The distinction between elements of order 2 and 4 in $P \setminus Z(G)$ in characteristic 2 yields a decomposition of the polynomial E (Theorem 3.4 of [24]). There is no analogous result in odd characteristic.

Recall from Sect. 5 that every maximal abelian subgroup \mathcal{A} of P is the inverse image of a maximal isotropic subspace \bar{A} of W . For any such \mathcal{A} , let $\{c_1, \dots, c_h\}$ be a basis of \bar{A} as described prior to Proposition 5.5. Then every subgroup of \mathcal{A} of order p^h that intersects $Z(P)$ trivially is generated by automorphisms of the form $\{\sigma_{b_1,c_1}, \dots, \sigma_{b_h,c_h}\}$ where $b_i^p - b_i = c_i R(c_i)$ for $1 \leq i \leq h$. In fact, there is a one-to-one correspondence between such subgroups of \mathcal{A} and sets of elements $\{b_1, \dots, b_h\}$ satisfying $b_i^p - b_i = c_i R(c_i)$. By Remark 3.3 the elements in all these sets are of the form $b_i = B_{c_i}(c_i)/2 + i$ with $i \in \mathbb{F}_p$.

Theorem 7.4. *Assume $h \geq 0$. Let \mathcal{A} be a maximal abelian subgroup of P . Any subgroup $A \subset \mathcal{A}$ of order p^h that intersects the center $Z(P)$ of P trivially gives rise to an \mathbb{F}_q -isomorphism of the quotient curve \bar{C}_A onto the smooth projective curve given by the affine equation*

$$Y^p - Y = a_{\mathcal{A}} X^2.$$

Here

$$a_{\mathcal{A}} = \frac{a_h}{2} \prod_{c \in \bar{A} \setminus \{0\}} c,$$

for $h \geq 1$, where we recall that a_h is the leading coefficient of R and \bar{A} is the maximal isotropic subspace of W that is the image of \mathcal{A} under the quotient map $P \rightarrow W$. For $h = 0$, we let

$$a_{\mathcal{A}} = a_0.$$

Proof. We prove by induction on h that there exists a subgroup $A \subset \mathcal{A}$ with $A \simeq (\mathbb{Z}/p\mathbb{Z})^h$ and $Z(P) \cap A = \{1\}$ such that the quotient curve $\bar{C}_A = C_R/A$ is given over \mathbb{F}_q by the equation stated in the theorem. The statement of the theorem follows from this using Lemma 6.2.

For $h = 0$ the statement is true by definition.

Assume that $h \geq 1$ and that the statement of the theorem holds for all additive polynomials $R(X)$ of degree p^{h-1} . Fix a basis $\{c_1, c_2, \dots, c_h\}$ for the image of

\mathcal{A} in W . We may choose $b_h = B_{c_h}(c_h)/2$. As in Sect. 5, we write $\sigma_h(x, y) = \sigma_{b_h, c_h}(x, y) = (x + c_h, y + b_h + B_{c_h}(x))$. Proposition 7.2 implies that the quotient curve $C_{h-1} := C_R/\langle\sigma_h\rangle$ is given by an Artin–Schreier equation

$$Y_{h-1}^p - Y_{h-1} = X_{h-1}R_{h-1}(X_{h-1}),$$

where R_{h-1} is an additive polynomial of degree p^{h-1} .

Since \mathcal{A} is an abelian group, it follows that $\mathcal{A}_{h-1} := \mathcal{A}/\langle\sigma_h\rangle \simeq (\mathbb{Z}/p\mathbb{Z})^h$ is a maximal abelian subgroup of the Sylow p -subgroup P_{h-1} of $\text{Aut}^0(C_{h-1})$. The definition of the coordinate X_{h-1} as $X^p - c_h^{p-1}X$ in the proof of Proposition 7.2 implies that \mathcal{A}_{h-1} corresponds to the maximal isotropic subspace $\langle\bar{c}_1, \dots, \bar{c}_{h-1}\rangle$ of $W_{h-1} := W/\langle c_h, c'_h\rangle$, where $\bar{c}_i = c_i^p - c_h^{p-1}c_i$ and $c'_h \in W$ is an element with $\epsilon(c_i, c'_h) = \delta_{i,h}$ as in Sect. 5.

The induction hypothesis implies that there exists a subgroup $A_{h-1} \subset \mathcal{A}_{h-1}$ with $A_{h-1} \simeq (\mathbb{Z}/p\mathbb{Z})^{h-1}$ and $A_{h-1} \cap Z(P_{h-1}) = \{1\}$ such that the quotient C_{h-1}/A_{h-1} is given by

$$Y_0^p - Y_0 = a_{\mathcal{A}_{h-1}}X_0^2.$$

We may choose b_i satisfying $b_i^p - b_i = c_iR(c_i)$ for $i = 1, \dots, h-1$ such that the images of $\sigma_{b_1, c_1}, \dots, \sigma_{b_{h-1}, c_{h-1}}$ in \mathcal{A}_{h-1} generate A_{h-1} (Remark 3.3). Put $\sigma_i = \sigma_{b_i, c_i}$ for $i = 1, \dots, h-1$. Then $A := \langle\sigma_1, \dots, \sigma_h\rangle$ satisfies

$$C_R/A \simeq_{\mathbb{F}_q} C_{h-1}/A_{h-1}.$$

This concludes the induction proof.

The statement about $a_{\mathcal{A}}$ follows immediately from the formula for the leading coefficient of the quotient curve given in Proposition 7.2. □

8 The Zeta Function of the Curve C_R

In this section, we describe the zeta function of the curve C_R over the splitting field \mathbb{F}_q of the polynomial $E(X)$ defined in (2).

Let C be a curve defined over a finite field \mathbb{F}_{p^s} , and write $N_n = \#C(\mathbb{F}_{p^{sn}})$ for the number of points on C over any extension $\mathbb{F}_{p^{sn}}$ of \mathbb{F}_{p^s} . Recall that the *zeta function* of C , defined as

$$Z_C(T) = \exp\left(\sum_{n \geq 1} \frac{N_n T^n}{n}\right),$$

is a rational function with the following properties:

1. The zeta function may be written as

$$Z_C(T) = \frac{L_{C, \mathbb{F}_{p^s}}(T)}{(1-T)(1-p^s T)},$$

where $L_{C, \mathbb{F}_{p^s}}(T) \in \mathbb{Z}[T]$ is a polynomial of degree $2g(C)$ with constant term 1.

2. Write $L_{C, \mathbb{F}_{p^s}}(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$ with $\alpha_i \in \mathbb{C}$. After suitably ordering the α_i , we have

$$\alpha_{2g-i} = \frac{p^s}{\alpha_i}, \quad |\alpha_i| = p^{s/2}.$$

3. For each n , we have

$$N_n = \#C(\mathbb{F}_{p^{sn}}) = 1 + p^{sn} - \sum_{i=1}^{2g} \alpha_i^n.$$

4. If

$$L_{C, \mathbb{F}_{p^s}}(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$$

as above, then for any $r \geq 0$, we have

$$L_{C, \mathbb{F}_{p^{rs}}}(T) = \prod_{i=1}^{2g} (1 - \alpha_i^r T).$$

The numerator $L_{C, \mathbb{F}_{p^s}}(T)$ of the zeta function $Z_C(T)$ over \mathbb{F}_{p^s} is called the *L-polynomial* of C/\mathbb{F}_{p^s} . If the field is clear from the context, we sometimes omit it from the notation and simply write $L_C(T)$.

Recall that the Hasse–Weil bound asserts that

$$|\#C(\mathbb{F}_{p^s}) - (p^s + 1)| \leq 2p^{s/2}g(C).$$

A curve C/\mathbb{F}_{p^s} is called *maximal* if $\#C(\mathbb{F}_{p^s}) = p^s + 1 + 2p^{s/2}g(C)$ and *minimal* if $\#C(\mathbb{F}_{p^s}) = p^s + 1 - 2p^{s/2}g(C)$. Since the number of points on a curve must be an integer, if C is a maximal curve, then s must be even. Furthermore, using properties 2 and 3 above, it is clear that C is maximal if $\alpha_j = -p^{s/2}$ for each $1 \leq j \leq 2g(C)$, and C is minimal if $\alpha_j = p^{s/2}$ for each $1 \leq j \leq 2g(C)$.

Assume that s is even and that \mathbb{F}_{p^s} is an extension of \mathbb{F}_q . In the notation of Proposition 2.6, we have $w_s = \dim_{\mathbb{F}_p} W = 2h$ (Corollary 2.3). Since the curve C_R has genus $p^h(p-1)/2$, Proposition 2.6 implies that C_R is either maximal or minimal in this case. Moreover, one easily sees that if either s is odd or \mathbb{F}_{p^s} does

not contain \mathbb{F}_q , then C_R is neither maximal nor minimal. The following proposition asserts that this almost determines the zeta function of C_R over \mathbb{F}_q . The statement is an extension to odd characteristic of Theorems 10.1 and 10.2 of [24]. Note that the statement for odd characteristic is simpler than that for characteristic 2.

Proposition 8.1. *Let \mathbb{F}_{p^s} be an extension of \mathbb{F}_q , the splitting field of $E(X)$. Write $g = p^h(p - 1)/2$ for the genus of C_R .*

1. *If s is even, the L -polynomial of C_R is*

$$L_{C_R}(T) = (1 \pm p^{s/2}T)^{2g}.$$

2. *If s is odd, the L -polynomial of C_R is*

$$L_{C_R}(T) = (1 \pm p^s T^2)^g.$$

Proof.

1. Let $\alpha_1, \dots, \alpha_{2g}$ be the reciprocal zeros of the L -polynomial of C over \mathbb{F}_{p^s} , where we order the α_i such that $\alpha_i \alpha_{2g-i} = p^s$.

We first assume that s is even. Since \mathbb{F}_{p^s} is an extension of \mathbb{F}_q , we have

$$N_1 = \#C_R(\mathbb{F}_{p^s}) = 1 + p^s \pm 2gp^{s/2} = 1 + p^s - \sum_{i=1}^{2g} \alpha_i.$$

Since $|\alpha_i| = p^{s/2}$ we conclude that

$$\alpha_1 = \dots = \alpha_{2g} = \pm p^{s/2}.$$

This proves Part 1.

2. We now assume that s is odd. Proposition 2.6 implies that

$$N_1 = \#C_R(\mathbb{F}_{p^s}) = 1 + p^s = 1 + p^s - \sum_{i=1}^{2g} \alpha_i. \tag{28}$$

Since the reciprocal roots of the L -polynomial of C over $\mathbb{F}_{p^{2s}}$ are α_j^2 , we conclude from Part 1 that either $\alpha_j^2 = p^s$ or $\alpha_j^2 = -p^s$ for all j .

If $\alpha_j^2 = -p^s$ for all j , then $\alpha_j = \pm i p^{s/2}$, where i is a primitive 4th root of unity. It follows that $\alpha_{2g-j} = p^s/\alpha_j = -\alpha_j$. Hence

$$(1 - \alpha_j T)(1 - \alpha_{2g-j} T) = 1 + p^s T^2.$$

Assume now that $\alpha_j^2 = p^s$ for all j . In this case we have $\alpha_j = \pm p^{s/2}$ and $\alpha_{2g-j} = p^s/\alpha_j = \alpha_j$. Let $m = \#\{1 \leq j \leq g : \alpha_j = p^{s/2}\}$. It follows from (28) that

$$0 = \#C_R(\mathbb{F}_{p^s}) - (p^s + 1) = p^{s/2}(-2m + 2(g - m)).$$

We conclude that $2g = 4m$, i.e., $m = g/2$ (in particular, g is even). For the L -polynomial of C_R over \mathbb{F}_{p^s} we find

$$L_{C_R}(T) = (1 - p^s T^2)^g,$$

as claimed in Part 2. □

Remark 8.2.

1. The proof of Part 2 of Proposition 8.1 shows that the case $L_{C_R}(T) = (1 - p^s T^2)^g$ can only occur when g is even, i.e., if $p \equiv 1 \pmod{4}$.
2. Assume that s is even. Then $\alpha_j = p^{s/2}$ or $\alpha_j = -p^{s/2}$ for all $1 \leq j \leq 2g$, and therefore C_R is either minimal or maximal. If C_R is minimal over \mathbb{F}_{p^s} , each $\alpha_j = p^{s/2}$. The curve C_R therefore remains minimal over each extension field $\mathbb{F}_{p^{sf}}$. If C_R is maximal over \mathbb{F}_{p^s} , each $\alpha_j = -p^{s/2}$. The reciprocal roots of the L -polynomial over $\mathbb{F}_{p^{sf}}$ are $\alpha_j^f = (-1)^f p^{sf/2}$. We conclude that C_R is maximal over $\mathbb{F}_{p^{sf}}$ if f is odd and minimal if f is even.

To determine the zeta function of C_R , it remains to decide when the different cases occur. The following result, which is an immediate corollary of Proposition 6.3, reduces this problem to the case $h = 0$.

Corollary 8.3. *Let $A \simeq (\mathbb{Z}/p\mathbb{Z})^h \subset P$ be a subgroup with $A \cap Z(P) = \{0\}$. Write $\overline{C}_A = C_R/A$. Then*

$$L_{C_R, \mathbb{F}_q}(T) = L_{\overline{C}_A, \mathbb{F}_q}(T)^{p^h}.$$

Proof. This is an immediate consequence of Proposition 6.3, since abelian varieties which are isogenous over \mathbb{F}_q have the same zeta function over \mathbb{F}_q . This follows, for example, from the cohomological description of the zeta function in Sect. 1 of [13]. □

Recall from Theorem 7.4 that the curve \overline{C}_A from Corollary 8.3 is a curve of genus $(p - 1)/2$ given by an affine equation of the form

$$Y^p - Y = aX^2,$$

for some $a \in \mathbb{F}_q^*$. This corresponds to the case $h = 0$. All curves of this form are isomorphic over $\overline{\mathbb{F}}_q$, and the different \mathbb{F}_q -models are described in Lemma 7.1. The next result determines the L -polynomials of the curves \overline{C}_A . In the literature one finds many papers discussing the zeta function of similar curves using Gauss sums (for example, [6, 13, 27].) We give a self-contained treatment here based on the results of Sect. 2.

Theorem 8.4. *Consider the curve C_R over some extension of \mathbb{F}_q and put $g = g(C_R)$. For $h \geq 0$ we put $a = a_{\mathcal{A}}$ with $a_{\mathcal{A}}$ as given in Theorem 7.4 for some choice of \mathcal{A} .*

1. If $p \equiv 1 \pmod{4}$, then the L -polynomial of C_R over \mathbb{F}_{p^s} is given by

$$L_{C_R, \mathbb{F}_{p^s}}(T) = \begin{cases} (1 - p^s T^2)^g & \text{if } s \text{ is odd,} \\ (1 - p^{s/2} T)^{2g} & \text{if } s \text{ is even and } a \text{ is a square in } \mathbb{F}_{p^s}^*, \\ (1 + p^{s/2} T)^{2g} & \text{if } s \text{ is even and } a \text{ is a nonsquare in } \mathbb{F}_{p^s}^*. \end{cases}$$

2. If $p \equiv 3 \pmod{4}$, then the L -polynomial of C_R over \mathbb{F}_{p^s} is given by

$$L_{C_R, \mathbb{F}_{p^s}}(T) = \begin{cases} (1 + p^s T^2)^g & \text{if } s \text{ is odd,} \\ (1 - p^{s/2} T)^{2g} & \text{if } s \equiv 0 \pmod{4} \text{ and } a \text{ is a square in } \mathbb{F}_{p^s}^*, \\ (1 + p^{s/2} T)^{2g} & \text{if } s \equiv 0 \pmod{4} \text{ and } a \text{ is a nonsquare in } \mathbb{F}_{p^s}^*, \\ (1 + p^{s/2} T)^{2g} & \text{if } s \equiv 2 \pmod{4} \text{ and } a \text{ is a square in } \mathbb{F}_{p^s}^*, \\ (1 - p^{s/2} T)^{2g} & \text{if } s \equiv 2 \pmod{4} \text{ and } a \text{ is a nonsquare in } \mathbb{F}_{p^s}^*. \end{cases}$$

Proof. Corollary 8.3 implies that it suffices to consider the case $h = 0$. To prove the theorem we may therefore assume that $R(X) = aX$. We label the corresponding curve D_a as we do in Lemma 7.1.

Case 1: The element a is a square in $\mathbb{F}_{p^s}^*$.

Then Lemma 7.1 implies that D_a is isomorphic over \mathbb{F}_q to the curve D_1 given by the affine equation $Y^p - Y = X^2$. Since D_1 is defined over \mathbb{F}_p , we compute its L -polynomial over \mathbb{F}_p . The argument that we use here proceeds in the same manner as in the proof of Proposition 2.6. However, since both the polynomial $R(X)$ and the field are very simple, we do not need to consider the quadric Q considered in that proof explicitly.

As in the proof of Proposition 8.1, it suffices to determine the number N_2 of \mathbb{F}_{p^2} -rational points of the curve D_1 . We have $p + 1$ points with $x \in \{0, \infty\}$. As in the proof of Proposition 2.6, the \mathbb{F}_{p^2} -points with $x \neq 0, \infty$ correspond to squares $z = x^2$ with $\text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(z) = 0$. Every such element z yields exactly $2p$ rational points. Since $\text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(z) = z + z^p$, the nonzero elements of trace zero are exactly the elements with $z^{p-1} = -1$. Choosing an element $\zeta \in \mathbb{F}_{p^2}^*$ of order $2(p - 1)$, we conclude that the nonzero elements with trace zero are

$$\ker(\text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}) \setminus \{0\} = \{\zeta^{2j+1} : j = 0, \dots, p - 2\}.$$

First suppose that $p \equiv 3 \pmod{4}$. Then all the elements of $\ker(\text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p})$ are squares in \mathbb{F}_{p^2} , so

$$\#D_1(\mathbb{F}_{p^2}) = 1 + p + (p - 1)2p = 1 + p^2 + (p - 1)p.$$

As in the proof of Proposition 8.1 it follows that $\alpha_j = \pm i p^{1/2} = -\alpha_{2g-j}$ for $1 \leq j \leq g$ after suitable relabeling. If s is even, then $\alpha_j^s = \alpha_{2g-j}^s = i^s p^{s/2}$ and

$$(1 - \alpha_j^s T)(1 - \alpha_{2g-j}^s T) = 1 - 2i^s p^{s/2} T + p^s T^2 = \begin{cases} (1 - p^{s/2} T)^2 & \text{if } s \equiv 0 \pmod{4}, \\ (1 + p^{s/2} T)^2 & \text{if } s \equiv 2 \pmod{4}. \end{cases}$$

If s is odd, then $\alpha_j^s = \pm i^s p^{s/2} = -\alpha_{2g-j}^s$, and therefore

$$(1 - \alpha_j^s T)(1 - \alpha_{2g-j}^s T) = 1 + p^s T^2.$$

Now assume that $p \equiv 1 \pmod{4}$. Then none of the elements of $\ker(\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p})$ are squares in \mathbb{F}_{p^2} , and we conclude that

$$\#D_1(\mathbb{F}_{p^2}) = 1 + p = 1 + p^2 - (p-1)p.$$

Again as in the proof of Proposition 8.1 it follows that, up to relabeling, $\alpha_j = p^{s/2} = \alpha_{2g-j}$ for $1 \leq j \leq g/2$, and $\alpha_j = -p^{s/2} = \alpha_{2g-j}$ for $g/2 + 1 \leq j \leq g$. (Note that g is even since $p \equiv 1 \pmod{4}$.) We may therefore relabel again to ensure that $\alpha_j = p^{s/2} = -\alpha_{2g-j}$, for $1 \leq j \leq g$. With this new labeling, if s is even, then $\alpha_j^s = \alpha_{2g-j}^s = p^{s/2}$, and

$$(1 - \alpha_j^s T)(1 - \alpha_{j+g/2}^s T) = (1 - p^{s/2} T)^2,$$

and if s is odd, then $\alpha_j^s = p^{s/2} = -\alpha_{2g-j}$ and

$$(1 - \alpha_j^s T)(1 - \alpha_{j+g/2}^s T) = (1 - p^{s/2} T)(1 + p^{s/2} T) = (1 - p^s T^2).$$

This concludes Case 1.

Case 2: The element a is a nonsquare in $\mathbb{F}_{p^s}^*$ and s is odd.

Then the set $\{a\beta^2 : \beta \in \mathbb{F}_{p^s}^*\}$ contains $(p^s - 1)/2$ distinct elements, all of which are nonsquares. As a consequence, this set contains all nonsquares of \mathbb{F}_{p^s} . For s odd, the nonsquares in $\mathbb{F}_{p^s}^*$ are also nonsquares in \mathbb{F}_p^* , and therefore the set $\{a\beta^2 : \beta \in \mathbb{F}_{p^s}^*\}$ contains an element in \mathbb{F}_p^* . (In fact, this set contains all the nonsquares in \mathbb{F}_{p^s} .) Lemma 7.1 now implies that the curve D_a is isomorphic over \mathbb{F}_q to the curve D_1 , and the desired result follows therefore from Case 1.

Case 3: The element a is a nonsquare in $\mathbb{F}_{p^s}^*$ and s is even.

Here, we consider $M := \ker(\mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}) = \{z \in \mathbb{F}_{p^s} : \mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(z) = 0\}$. Since the trace is surjective and \mathbb{F}_p -linear, the cardinality of M is p^{s-1} . We may write M as a disjoint union

$$M = \{0\} \cup M^{\mathrm{sq}} \cup M^{\mathrm{nsq}},$$

where M^{sq} (resp. M^{nsq}) are the elements of $M \setminus \{0\}$ which are squares (resp. nonsquares) in $\mathbb{F}_{p^s}^*$.

As in the proof of Case 1 we have

$$\#D_1(\mathbb{F}_{p^s}) = 1 + p + 2p\#M^{\text{sq}},$$

and a similar argument gives

$$\#D_a(\mathbb{F}_{p^s}) = 1 + p + 2p\#M^{\text{nsq}}.$$

From the expression for $\#D_1(\mathbb{F}_{p^s})$ computed in Case 1, it follows that

$$\#M^{\text{sq}} = \begin{cases} \frac{p^{s-1}-1}{2} + \frac{(p-1)}{2}p^{(s-2)/2} & \text{if } p \equiv 3 \pmod{4} \text{ and } s \equiv 2 \pmod{4}, \\ \frac{p^{s-1}-1}{2} - \frac{(p-1)}{2}p^{(s-2)/2} & \text{if } p \equiv 1 \pmod{4} \text{ or } s \equiv 0 \pmod{4}. \end{cases}$$

Since $\#M^{\text{nsq}} = \#M - 1 - \#M^{\text{sq}} = p^{s-1} - 1 - \#M^{\text{sq}}$, we conclude that

$$\#D_a(\mathbb{F}_{p^s}) = \begin{cases} 1 + p^s - (p-1)p^{s/2} & \text{if } p \equiv 3 \pmod{4} \text{ and } s \equiv 2 \pmod{4}, \\ 1 + p^s + (p-1)p^{s/2} & \text{if } p \equiv 1 \pmod{4} \text{ or } s \equiv 0 \pmod{4}. \end{cases}$$

The expressions for the L -polynomial now follow as in the previous cases. □

We finish this section by proving that all curves C_R are supersingular. This result is not new. Our proof just adds some details to Theorem 13.7 in [24]. An alternative proof is given by Blache, Corollary 3.7(ii) of [2].

Proposition 8.5. *The curve C_R is supersingular, i.e., its Jacobian is isogenous over $k = \mathbb{F}_q$ to a product of supersingular elliptic curves.*

Proof. The curve C_R is supersingular if and only if all the slopes of the Newton polygon of the L -polynomial are $1/2$. (This follows, for example, from Theorem 2 of [23].) The statement of the proposition follows therefore from Theorem 8.4. □

The reasoning of Van der Geer and Van der Vlugt for Theorem 13.7 of [24] is slightly different, since they do not compute the L -polynomial of C_R over \mathbb{F}_q . They argue that the Jacobian variety J_R of C_R is isogenous over k to p^h copies of the Jacobian of the curve D_1 with equation $Y^p - Y = X^2$. (This is a weaker version of Proposition 6.3.) They then use the fact that the curve D_1 is supersingular.

9 Examples

By work of Ihara [10], Stichtenoth and Xing [21], and Fuhrmann and Torres [8], we know that for q a power of a prime, a curve C which is maximal over \mathbb{F}_{q^2} satisfies

$$g(C) \in \left[0, \frac{(q-1)^2}{4} \right] \cup \left\{ \frac{q(q-1)}{2} \right\}.$$

Moreover, the Hermite curves are the only maximal curves of genus $(q(q - 1))/2$ [17].

Recall from Sect. 8 that a curve C is maximal over $\mathbb{F}_{p^{2s}}$ if and only if its L -polynomial satisfies $L_{C, \mathbb{F}_{p^{2s}}} = (1 + p^{2s}T)^{2g(C)}$. In our setting, Theorem 8.4 shows that for a curve C_R of the type considered in this paper and a defined as in Theorem 8.4, if \mathbb{F}_{p^s} contains the splitting field \mathbb{F}_q of $E(X)$, then C_R is maximal over \mathbb{F}_{p^s} if and only if one of the following holds:

- s is even, a is a nonsquare in \mathbb{F}_q^* , and $p \equiv 1 \pmod{4}$,
- $s \equiv 0 \pmod{4}$, a is a nonsquare in \mathbb{F}_q^* , and $p \equiv 3 \pmod{4}$, or
- $s \equiv 2 \pmod{4}$, a is a square in \mathbb{F}_q^* , and $p \equiv 3 \pmod{4}$.

In each case the negation of the condition on a guarantees that C_R is a minimal curve over \mathbb{F}_{p^s} .

In light of these facts, the only difficulty in generating examples of maximal and minimal curves lies in computing suitable elements a . In this section we present certain cases in which such a can be computed. We start with a discussion of the case $h = 0$, and then turn our attention to $R(X) = X^{p^h}$. For more results along the same lines we refer to [1, 3]. In [4] it is shown that all curves C_R that are maximal over the field $\mathbb{F}_{p^{2n}}$ are quotients of the Hermite curve H_{p^n} with affine equation $yp^n - y = x^{p^n+1}$.

At the end of this section we briefly investigate isomorphisms between certain curves C_R and curves with defining equations

$$Y^p + Y = X^{p^h+1}.$$

Throughout this section, we let H_p denote the Hermite curve which is defined by the affine equation

$$Y^p + Y = X^{p+1}. \tag{29}$$

As mentioned above, this is a maximal curve over \mathbb{F}_{p^2} . The curve $Y^p + Y = X^2$ is a quotient of the Hermite curve H_p , and therefore this curve is maximal over \mathbb{F}_{p^2} . The following lemma determines when the twists

$$Y^p - Y = aX^2$$

of this curve are maximal. A similar result can also be found in Lemma 4.1 of [3].

Lemma 9.1. *Let $R(X) = aX \in \mathbb{F}_{p^{2s}}[X]$. Then C_R is maximal over $\mathbb{F}_{p^{2s}}$ if and only if one of the following conditions holds:*

1. $p \equiv 1 \pmod{4}$ and $a \in \mathbb{F}_{p^{2s}}^*$ is a nonsquare,
2. $p \equiv 3 \pmod{4}$, s is even, and $a \in \mathbb{F}_{p^{2s}}^*$ is a nonsquare, or
3. $p \equiv 3 \pmod{4}$, s is odd, and $a \in \mathbb{F}_{p^{2s}}^*$ is a square.

Proof. In this case we have $E(X) = 2aX$, hence $\mathbb{F}_{p^{2s}}$ automatically contains the splitting field of E . The lemma therefore follows from Theorem 8.4. □

Remark 9.2. The database manYPoints [26] compiles records of curves with many points. The following two maximal curves fall in the range of genus and cardinality covered in the database, and have now been included in manYPoints. Previously, the database did not state any lower bound for the maximum number of points of a curve of genus 5 over \mathbb{F}_{11^4} and a curve of genus 9 over \mathbb{F}_{19^4} .

1. In the case where $h = 0$, $p = 11$, and $s = 4$, let $a \in \mathbb{F}_{11^4}^*$ be a nonsquare. Then the curve

$$Y^{11} - Y = aX^2$$

is maximal over \mathbb{F}_{11^4} and of genus 5.

2. In the case where $h = 0$, $p = 19$, and $s = 4$, let $a \in \mathbb{F}_{19^4}$ be a nonsquare. Then the curve

$$Y^{19} - Y = aX^2$$

is maximal over \mathbb{F}_{19^4} and of genus 9.

The following proposition gives an example of a class of maximal curves with small genus compared to the size of their field of definition, in contrast to the Hermite curves which have large genus. A similar result for $p = 2$ can be found in Theorem 7.4 of [24]. A similar result with p replaced by an arbitrary prime power can be found in Proposition 4.6 of [3].

Proposition 9.3. *Let $h \geq 1$.*

1. *Let $R(X) = X^{p^h}$. Then $E(X) = X^{p^{2h}} + X$, which has splitting field $\mathbb{F}_q = \mathbb{F}_{p^{4h}}$. The curve C_R is minimal over \mathbb{F}_q .*
2. *Let $a_h \in \mathbb{F}_{p^{2h}}^*$ be an element with $a_h^{p^h - 1} = -1$ and define $R(X) = a_h X^{p^h}$. Then $E(X) = a_h^{p^h} (X^{p^{2h}} - X)$, which has splitting field $\mathbb{F}_q = \mathbb{F}_{p^{2h}}$. The curve C_R is maximal over \mathbb{F}_q .*

Proof. We first prove the statement about the splitting field of $E(X)$ for both cases. Consider the additive polynomial $R(X) = a_h X^{p^h} \in \mathbb{F}_{p^s}[X]$ with $h \geq 1$. Then (2) shows that

$$E(X) = a_h^{p^h} X^{p^{2h}} + a_h X.$$

If $a_h = 1$, then E has splitting field $\mathbb{F}_q = \mathbb{F}_{p^{4h}}$. If $a_h \in \mathbb{F}_{p^{2h}}^*$ satisfies $a_h^{p^h - 1} = -1$, then $E(X) = a_h^{p^h} (X^{p^{2h}} - X)$, which has splitting field $\mathbb{F}_q = \mathbb{F}_{p^{2h}}$. In both cases, we conclude from the explicit expression of E that

$$W = \{c \in \overline{\mathbb{F}}_p : c^{p^{2h}} = -a_h^{1-p^h} c\}.$$

For every $c \in W$, the formulas (7) and (8) imply that

$$B_c(X) = - \sum_{i=0}^{h-1} a_h^{p^i} c^{p^{h+i}} X^{p^i}.$$

We first consider the case where $a_h = 1$. Choose an element $c \in W \setminus \{0\}$, i.e., $c^{p^{2h}} = -c$, and define

$$\bar{A} = \{c\zeta : \zeta \in \mathbb{F}_{p^h}\} \subset W.$$

For any two ζ_j, ζ_k in \mathbb{F}_{p^h} , we have

$$B_{c\zeta_j}(c\zeta_k) = - \sum_{i=0}^{h-1} \zeta_j^{p^{h+i}} c^{p^{h+i+p^i}} \zeta_k^{p^i} = - \sum_{i=0}^{h-1} \zeta_j^{p^i} c^{p^{h+i+p^i}} \zeta_k^{p^{h+i}} = B_{c\zeta_k}(c\zeta_j),$$

since $\zeta^{p^h} = \zeta$ for any $\zeta \in \mathbb{F}_{p^h}$. Therefore the pairing from Part 1 of Lemma 5.2 satisfies

$$\epsilon(c\zeta_j, c\zeta_k) = B_{c\zeta_j}(c\zeta_k) - B_{c\zeta_k}(c\zeta_j) = 0 \quad \text{for any pair } (c\zeta_j, c\zeta_k) \in \bar{A}^2.$$

We conclude that $\bar{A} \subset W$ is a maximal isotropic subspace. Write $\mathcal{A} \subset P$ for the corresponding maximal abelian subgroup of P . Recall the constant from Theorem 7.4,

$$a_{\mathcal{A}} = \frac{a_h}{2} \prod_{\gamma \in \bar{A} \setminus \{0\}} \gamma,$$

when $h \geq 1$. Here the leading coefficient a_h of $R(X)$ is 1. The definition of \bar{A} implies that

$$\prod_{\gamma \in \bar{A} \setminus \{0\}} \gamma = c^{p^h-1} \prod_{\zeta \in \mathbb{F}_{p^h}^*} \zeta = -c^{p^h-1}.$$

We conclude that $a_{\mathcal{A}} = -c^{p^h-1}/2$ is a square in \mathbb{F}_q^* , since $-1/2$ is a square in $\mathbb{F}_{p^2}^* \subset \mathbb{F}_q^*$. Theorem 8.4 now yields

$$L_{C_R, \mathbb{F}_q}(T) = (1 - \sqrt{q}T)^{2g}.$$

It follows that C_R is minimal over \mathbb{F}_q .

We now assume that $a_h \in \mathbb{F}_{p^{2h}}^*$ satisfies $a_h^{p^h} = -a_h$. In this case the splitting field of $E(X)$ is $\mathbb{F}_q = \mathbb{F}_{p^{2h}}$ as shown earlier. Choose a primitive $(p^{2h} - 1)$ -st root of

unity ζ . Then we may write $a_h = \zeta^{(2j+1)(p^h+1)/2}$ for some j . It follows that $a_h \in \mathbb{F}_q^*$ is a square if and only if $(p^h + 1)/2$ is even. This is equivalent to $p \equiv 3 \pmod{4}$ and h odd.

We choose $\bar{A} = \mathbb{F}_{p^h} \subset W = \mathbb{F}_{p^{2h}}$. For every $c, c' \in \bar{A}$, we have

$$B_c(c') = - \sum_{i=0}^{h-1} (a_h c c')^{p^i} = B_{c'}(c).$$

As in the proof of Part 1, we conclude that \bar{A} is a maximal isotropic subspace for the pairing ϵ from Part 1 of Lemma 5.2. Since

$$\prod_{c \in \bar{A} \setminus \{0\}} c = -1,$$

we conclude that $a_{\mathcal{A}}$ is equivalent to a_h modulo squares in \mathbb{F}_q^* . (The argument is similar to that in the proof of Part 1.) We conclude that $a_{\mathcal{A}}$ is a square in \mathbb{F}_q^* if and only if $p \equiv 3 \pmod{4}$ and h is odd. Theorem 8.4 implies that C_R is a maximal curve over \mathbb{F}_q in each of these cases. This proves Part 2. \square

Remark 9.4. In their follow-up paper [25] to [24], Van der Geer and Van der Vlugt constructed further examples of maximal curves as a fiber product of the curves C_R . We have not considered this construction in the case of odd characteristic. We leave this as a subject for future research.

Example 9.5.

1. We consider the Hermite curve H_p given in (29), and the curve C_R given by

$$Y^p - Y = X^{p+1}.$$

We claim that the curves H_p and C_R are not isomorphic over \mathbb{F}_{p^2} . To see this, we show that $\#C_R(\mathbb{F}_{p^2}) = 1 + p \neq 1 + p^3 = \#H_p(\mathbb{F}_{p^2})$. This clearly implies that the two curves are not isomorphic over \mathbb{F}_{p^2} .

We note that

$$\psi: \mathbb{F}_{p^2}^* \rightarrow \mathbb{F}_{p^2}^*, \quad x \mapsto x^{1+p}$$

is the restriction of the norm on $\mathbb{F}_{p^2}/\mathbb{F}_p$, so the image of ψ is \mathbb{F}_p^* . It follows that

$$\text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x^{1+p}) = 2x^{1+p} \neq 0 \quad \text{for all } x \in \mathbb{F}_{p^2}^*.$$

We conclude that the \mathbb{F}_{p^2} -rational points of C_R are the p points with $x = 0$ together with the unique point ∞ . This proves the claim. (Exercise 6.7 in [20] asks to prove that H_p and C_R are isomorphic over \mathbb{F}_{p^2} if $p \equiv 1 \pmod{4}$). The above calculation shows that this does not hold.)

However, the Hermite curve H_p is isomorphic over \mathbb{F}_{p^2} to the curve given by

$$C_{R'} : Y^p - Y = a_1 X^{p+1},$$

where $a_1 \in \mathbb{F}_{p^2}$ satisfies $a_1^{p-1} = -1$. The isomorphism is given by $\psi: C_{R'} \rightarrow H_p, (x, y) \mapsto (x, a_1^p y)$. This conforms with Part 2 of Proposition 9.3.

- Let $a_h \in \mathbb{F}_{p^{2h}}^*$ be an element with $a_h^{p^h} = -a_h$ as in Part 2 of Proposition 9.3. Write $R(X) = a_h X^{p^h}$. Then $\psi: (x, y) \mapsto (x, a_h^{2h-1} y)$ defines an isomorphism between C_R and the curve given by

$$Y^p + Y = X^{p^h+1}.$$

Part 2 of Proposition 9.3 therefore implies that this curve is maximal over $\mathbb{F}_{p^{2h}}$. This can also be shown directly, for example, using Proposition 6.4.1 of [20].

Acknowledgements This research began at the Women in Numbers 3 workshop that took place April 20–25, 2014, at the Banff International Research Station (BIRS) in Banff, Alberta (Canada). We thank the organizers of this workshop as well as the hospitality of BIRS. We also thank Mike Zieve for pointing out some references to us.

IB is partially supported by DFG priority program SPP 1489, WH is partially supported by NSF grant DMS-1406066, and RS is supported by NSERC of Canada.

References

- Anbar, N., Meidl, W.: Quadratic functions and maximal Artin–Schreier curves. *Finite Fields Appl.* **30**, 49–71 (2014)
- Blache, R.: Valuation of exponential sums and the generic first slope for Artin–Schreier curves. *J. Number Theory* **132**(10), 2336–2352 (2012)
- Çakçak, E., Özbudak, F.: Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places. *J. Pure Appl. Algebra* **210**(1), 113–135 (2007)
- Çakçak, E., Özbudak, F.: Curves related to Coulter’s maximal curves. *Finite Fields Appl.* **14**(1), 209–220 (2008)
- Cassels, J.W.S.: *Rational Quadratic Forms*. London Mathematical Society Monographs, vol. 13. Academic/[Harcourt Brace Jovanovich], London/New York (1978)
- Coulter, R.S.: The number of rational points of a class of Artin–Schreier curves. *Finite Fields Appl.* **8**(4), 397–413 (2002)
- Elkies, N.D.: Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups. In: *Applications of Curves Over Finite Fields* (Seattle, WA, 1997). Contemporary Mathematics, vol. 245, pp. 77–107. American Mathematical Society, Providence, RI (1999)
- Fuhrmann, R., Torres, F.: The genus of curves over finite fields with many rational points. *Manuscripta Math.* **89**(1), 103–106 (1996)
- Huppert, B.: *Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften*, vol. 134. Springer, Berlin/New York (1967)
- Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**(3), 721–724 (1981)

11. Joly, J.R.: Équations et variétés algébriques sur un corps fini. *Enseignement Math.* (2) **19**, 1–117 (1973)
12. Kani, E., Rosen, M.: Idempotent relations and factors of Jacobians. *Math. Ann.* **284**(2), 307–327 (1989)
13. Katz, N.M.: Crystalline cohomology, Dieudonné modules, and Jacobi sums. In: *Automorphic forms, representation theory and arithmetic* (Bombay, 1979). Tata Institute of Fundamental Research Studies in Mathematics, vol. 10, pp. 165–246. Tata Institute of Fundamental Research, Bombay (1981)
14. Lehr, C., Matignon, M.: Automorphism groups for p -cyclic covers of the affine line. Preprint version of [15]. arXiv.math/0307031
15. Lehr, C., Matignon, M.: Automorphism groups for p -cyclic covers of the affine line. *Compositio Math.* **141**(5), 1213–1237 (2005)
16. Matignon, M., Rocher, M.: Smooth curves having a large automorphism p -group in characteristic $p > 0$. *Algebra Number Theory* **2**(8), 887–926 (2008)
17. Rück, H.G., Stichtenoth, H.: A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.* **457**, 185–188 (1994)
18. Serre, J.P.: *Corps locaux*, deuxième edn. No. VIII in *Publications de l'Université de Nancago*. Hermann, Paris (1968)
19. Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern. *Arch. Math. (Basel)* **24**, 615–631 (1973)
20. Stichtenoth, H.: *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics, vol. 254, 2nd edn. Springer, Berlin (2009)
21. Stichtenoth, H., Xing, C.P.: The genus of maximal function fields over finite fields. *Manuscripta Math.* **86**(2), 217–224 (1995)
22. Suzuki, M.: *Group Theory II*. Grundlehren der Mathematischen Wissenschaften, vol. 248. Springer, New York (1986)
23. Tate, J.: Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2**, 134–144 (1966)
24. van der Geer, G., van der Vlugt, M.: Reed–Müller codes and supersingular curves I. *Compositio Math.* **84**, 333–367 (1992)
25. van der Geer, G., van der Vlugt, M.: How to construct curves over finite fields with many points. In: *Catanese, F. (ed.) Arithmetic Geometry* (Cortona 1994). *Symposia Mathematica*, pp. 169–189. Cambridge University Press, Cambridge (1997)
26. van der Geer, G., Howe, E., Lauter, K., Ritzenthaler, C.: Table of curves with many points. <http://www.manypoints.org> (2015)
27. Yui, N.: On the Jacobian variety of the Fermat curve. *J. Algebra* **65**(1), 1–35 (1980)