Two-torsion in the Jacobian of hyperelliptic curves over finite fields

By

Gunther Cornelissen

Abstract. We determine the exact dimension of the $\mathbf{F}_2$-vector space of $\mathbf{F}_q$-rational 2-torsion points in the Jacobian of a hyperelliptic curve over $\mathbf{F}_q$ (q odd) in terms of the degrees of the rational factors of its discriminant, and relate this to genus theory for the corresponding function field. As a corollary, we prove the existence of a point of order > 2 in the Jacobian of certain real hyperelliptic curves.

Mathematics Subject Classification (2000): 11R29, 14H40

1. Introduction. Because of Cohen-Lenstra type heuristics in function fields (Friedman and Washington [4]), only the 2-primary part of the class group of hyperelliptic curves is expected *not* to behave randomly. Indeed, Artin (for "imaginary" fields), Zhang and Sémirat (in general) prove the following theorem by developing genus theory and counting ambiguous classes in hyperelliptic function fields:

(1.1) Theorem. (E. Artin [1], §11, X. Zhang [9], S. Sémirat [8]) *Let $D = eP_1 \cdots P_s$, where P_i are mutually distinct monic irreducible polynomials of degree d_i over $\mathbf{F}_q$ (q odd) with leading coefficient $e \in \mathbf{F}_q$, and let $k = \deg(D)$. Let $\mathrm{Pic}(\mathcal{O}_D)$ be the class group of the maximal order $\mathcal{O}_D$ of $\mathbf{F}_q(x, \sqrt{D(x)})$ containing $\mathbf{F}_q[x]$. Its 2-rank $r_2(D) = \dim_{\mathbf{Z}/2} \mathrm{Pic}(\mathcal{O}_D)[2]$ is*

(a) $r_2(D) = s - 2$ if k is even, $e \in \mathbf{F}_q^2$ and some d_i is odd;

(b) $r_2(D) = s - 1$ if [k is odd] or [$e \in \mathbf{F}_q^2$ and all d_i are even] or [k is even, $e \in \mathbf{F}_q - \mathbf{F}_q^2$ and some d_i is odd];

(c) $r_2(D) = s$ if $e \in \mathbf{F}_q - \mathbf{F}_q^2$ and all d_i are even. □

(1.2) Corollary. *The class number $h(D)$ of $\mathcal{O}_D$ is divisible by $2^{r_2(D)}$, where $r_2(D)$ is as in (1.1).* □

This theorem has a geometrical meaning. Notations being as above, let X_D be the associated hyperelliptic curve, whose affine equation is $y^2 = D(x)$. Let J_D be the Jacobian of X_D. Observe that $\mathcal{O}_D$ consists of functions on X_D which are holomorphic outside points above the place $\infty = \frac{1}{x}$ of $\mathbf{F}_q(x)$. The class group of $\mathcal{O}_D$ fits into the following exact sequence (Rosen, [6], 4.1):

$$0 \to R_D \to J_D(\mathbf{F}_q) \to \mathrm{Pic}(\mathcal{O}_D) \to \mathbf{Z}/\delta\mathbf{Z} \to 0, \tag{1.3}$$

where R_D is the group of degree zero divisor classes on X_D supported at the points at infinity, and δ is the greatest common divisor of the degrees of the points at infinity of X_D.

It is known (loc. cit.) that $\delta = 1$, unless e is not a square and k is even (in which case $\delta = 2$). Furthermore, R_D is trivial, unless D is *real* (viz., if e is a square and k is even). For such real D, R_D is generated by the divisor $\infty_1 - \infty_2$, where ∞_1 and ∞_2 are the points of X_D above ∞. Its order is the *regulator* of D (viz., $|R_D| = \log_q |\varepsilon_D|_{\infty_i}$, where ε_D is a fundamental unit of $\mathcal{O}_D$, for any $i = 1, 2$). If D is not real, it is called *imaginary*.

The geometry contained in theorem (1.1) is that it bounds the *2-rank of the Jacobian*

$$\hat{r}_2(D) := \dim_{\mathbf{Z}/2\mathbf{Z}} J_D[2](\mathbf{F}_q)$$

non-trivially (from above in the imaginary case and from below in the real case).

The aim of this paper is to show how to compute $\hat{r}_2(D)$ exactly, only from the data $\{d_i\}_{i=1}^s$, independently of the arithmetic theory used in proving theorem (1.1). More precisely:

(1.4) Theorem. *For the 2-rank of J_D the following holds:*
(a) $\hat{r}_2(D) = s - 2$ if k is even and some d_i is odd;
(b) $\hat{r}_2(D) = s - 1$ if [k is odd] or [$s = 1$ and $k = 2 \bmod 4$];
(c) $\hat{r}_2(D) = s$ if [$s > 1$ and all d_i are even] or [$s = 1$ and $k = 0 \bmod 4$].

In particular, the following supplements the divisibility result in (1.2) (which would only give divisibility by 2):

(1.5) Corollary. *For imaginary fields with D irreducible of degree divisible by 4, the class number $h(D)$ is divisible by 4.*

Combination of theorem (1.1) and (1.4) via the sequence (1.3) leads to the following information:

(1.6) Corollary. *The following only happens when $s = 1$ and k is divisible by 4, or D has only factors of even degree:*
(a) For an imaginary discriminant D of even degree, all two-torsion classes in $\mathrm{Pic}(\mathcal{O}_D)$ have even degree;
(b) Let ρ be the prime-to-2 part of $|R_D|$. For a real discriminant D, the divisor $\rho(\infty_1 - \infty_2)$ is not further divisible in $J_D(\mathbf{F}_q)[2^\infty]$.

Here, $G[2^\infty]$ denotes the 2-primary part of a group G. The imaginary case of (1.6) is not so interesting, but for the real case, we get the following result about the existence of higher order 2-power torsion:

(1.7) Corollary. *Let D be real, such that $|R_D|$ is even. If D has a factor of odd degree, or D is irreducible with $k = 2 \bmod 4$, then there exists a point of order > 2 in $J_D(\mathbf{F}_q)[2^\infty]$.*

The method of proof of theorem (1.4) (as for $s = 1$ in [2]) is to reduce the computation of $\hat{r}_2(D)$ to linear algebra by studying the action of $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ on $J_D[2]$. Thus, the proof has quite a different flavour from that of theorem

(1.1). Another explanation of the peculiar behaviour observed in corollary (1.5) was provided using class field theory in [3].

(1.8) R e m a r k. Although the higher 2-power torsion should also behave in some regular way, it is much more difficult to control its dependence on D. In particular, there is in general no criterion only depending on $\{d_i\}$ to decide whether $2^{\hat{r}_2(D)+1}$ divides $h(D)$ (cf. [2], theorem H(ii)).

(1.9) R e m a r k. In recent years, hyperelliptic curves over finite fields and their divisor class groups seem to have attracted some interest in coding theory and cryptography (cf. Koblitz [5], Scheidler et. al. [7]). The class number and the regulator are measures for the size of the key space of such systems.

2. The action of Galois on the 2-torsion. Let $\{t_1, \cdots, t_k\}$ be the roots of D. Let $J_D[M]$ denote the M-torsion of J_D for any integer M. Then $J_D[M] = (\mathbf{Z}/M\mathbf{Z})^{2g}$ for any M coprime to q, where g is the genus of X. We have that $2g = k - 2$ if k is even and $2g = k - 1$ if k is odd. We leave out the proofs of the next lemma, which is straightforward.

(2.1) Lemma. (a) *If k is odd, let ∞ be the unique point at infinity of X, and let $D_i = (t_i, 0) - \infty$ for $i = 1, ..., k$. Then $\{D_1, ..., D_k\}$ span $J[2]$ as an $\mathbf{F}_2$-vector space, subject to the single relation $\sum_{i=1}^{k} D_i = 0$. In particular, $\{D_1, ..., D_{k-1}\}$ is a basis of $J_D[2]$.*

(b) *If k is even, let $D_i = (t_i, 0) - (t_1, 0)$ for $i = 2, ..., k$. Then $\{D_2, ..., D_k\}$ span $J[2]$ as an $\mathbf{F}_2$-vector space, subject to the single relation $\sum_{i=2}^{k} D_i = 0$. In particular, $\{D_2, ..., D_{k-1}\}$ is a basis of $J_D[2]$.* □

Let G be the Galois group of D over $\mathbf{F}_q$, and

$$\sigma = (t_1 \dots t_{d_1})(t_{d_1+1} \dots t_{d_1+d_2}) \cdots (t_{d_1+\dots+d_{s-1}+1} \dots t_{d_1+\dots+d_s})$$

a generator of G, expressed as a permutation of the roots of D. We have that $J_D[2](\mathbf{F}_q) = J_D[2]^G$, where $J_D[2]^G$ is the set of G-invariant elements in $J_D[2]$. The equation

$$?x \in J_D[2] \ : \ \sigma x = x \tag{2.2}$$

defining a G-invariant 2-torsion point x becomes linear when expressed by matrices w.r.t. the bases from lemma (2.1).

(2.3) N o t a t i o n. Let P_n denote the permutation matrix of an

n-cycle, viz.,

$$P_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}_{n \times n} .$$

Also, if m is a given matrix, let $m[r]$ (respectively $m[c]$) denote the matrix m in which the first row (respectively, the last column) has been replaced by a complete row (column) of 1's. If we write $m[r][c]$, we mean that both operations $[r]$ and $[c]$ have been applied to m, *and* the top right corner element of m has been set to zero.

(2.4) Lemma. *With respect to a suitable basis for $J_D[2]$, the action of $\sigma \neq 1$ is as follows:*

(a) *If k is odd, $\sigma = \mathrm{diag}(P_{d_1}, \cdots, P_{d_i}, \cdots, P_{d_s-1})[c]$.*

(b) *If k is even and $s > 1$, then*

$$\sigma = \mathrm{diag}(P_{d_1-1}, P_{d_2}, \cdots, P_{d_i}, \cdots, P_{d_s-1})[r][c].$$

(c) *If k is even and $s = 1$, then $\sigma_1 = P_{k-2}[r][c]$.*

P r o o f. If k is odd, we can assume that $t_{k-1}^{\sigma} = t_k$ since σ is not trivial. One immediately sees that the expression for σ w.r.t. the basis from (2.1)(a) is as indicated.

If k is odd, we can assume that $t_1^{\sigma} = t_2$. If t_{k-2} is not stable by σ, then it acts via the given matrix on the basis from (2.1)(b). On the other hand, if $t_{k-2}^{\sigma} = t_{k-2}$, then the matrix of σ w.r.t. the basis from (2.1)(b) is $\sigma = \mathrm{diag}(P_{d_1-1}, P_{d_2}, \cdots, P_{d_i}, \cdots, P_{d_s-1})[r]$, but adding all rows to the last one, we find the given expression (using that $k - 2 = 0$ in $\mathbf{F}_2$ if k is even). □

From this, one computes immediately the solution space of the equation (2.3).

(2.5) N o t a t i o n. For a sequence α and an integer n, let $\alpha^{[n]}$ denote the sequence α, n times repeated.

(2.6) Lemma. *The solution space $\mathbf{V}$ of the equation (2.2) w.r.t. the basis of lemma (2.1) has the following following form:*

(a) *If k is odd,*

$$\mathbf{V} = \{(\alpha_1^{[d_1]}, \cdots, \alpha_{s-1}^{[d_{s-1}]}, 0^{[d_s-1]}) \ : \ \alpha_i \in \mathbf{F}_2\}$$

(b) *If k is even and D has a factor of odd degree,*

$$\mathbf{V} = \{(\alpha_1^{[d_1-1]}, \cdots, \alpha_{s-1}^{[d_{s-1}]}, 0^{[d_s-1]}) \ : \ \alpha_i \in \mathbf{F}_2\},$$

subject to the condition that

$$d_1\alpha_1 + \cdots + d_{s-1}\alpha_{s-1} = 0. \tag{2.6.1}$$

(*c*) *If k is even and all factors of D are of even degree, then*

$$\begin{aligned}\mathbf{V} \;=\; \{&((\alpha_1, \alpha_1+\alpha_s)^{[\frac{d_1-2}{2}]}, \alpha_1, (\alpha_2, \alpha_2+\alpha_s)^{[\frac{d_2}{2}]}, \dots \\ &\dots, (\alpha_{s-1}, \alpha_{s-1}+\alpha_s)^{[\frac{d_{s-1}}{2}]}, (\alpha_s, 0)^{[\frac{d_s-2}{2}]}, \alpha_s)\ \alpha_i \in \mathbf{F}_2\};\end{aligned}$$

subject to the condition that

$$\frac{k-4}{2} \cdot \alpha_s = 0. \tag{2.6.2}$$

P r o o f. The result for odd k is immediate. Assume k is even. The last $d_s - 1$ rows of the equation (2.2) imply that the last $d_s - 1$ coordinates of a solution x are of the form $(\alpha_s, 0, \alpha_s, \dots)$.

Furthermore, if $s > 1$, the d_{s-1} (respectively $d_{s-2}, \dots$) preceding rows form a kind of permutation equations, and imply that the d_{s-1} (respectively, $d_{s-2}, \dots$) preceding coordinates of x are of the form $(\alpha_{d_{s-1}}, \alpha_{d_{s-1}} + \alpha_s, \dots, \alpha_{d_{s-1}} + \alpha_s)$ (respectively ...), with $\alpha_s = 0$ if d_{s-1} is odd (respectively, $d_{s-2}, \dots$). Finally, the first row of σ leads to an extra condition of the form (2.6.1) if some d_i is odd; and

$$\alpha_1 + \alpha_s(\frac{d_1-2}{2} + \frac{d_2}{2} + \ldots + \frac{d_{s-1}}{2} + \frac{d_s-2}{2}) = \alpha_1,$$

if all d_i are even — which is (2.6.2). □

P r o o f o f t h e o r e m (1.4). One only has to count the dimension of the solution spaces in lemma (2.6). Condition (2.6.1) imposes an extra relation since not all d_i are even, and condition (2.6.2) only imposes an extra relation if $s = 1$ and $k = 2 \bmod 4$. □

3. Special 2-torsion classes. We will now prove the corollaries. First of all, (1.5) needs no further explanation.

(3.1) The first claim of corollary (1.6) follows immediately from (1.1), (1.3) and (1.4). However, we will prove it independently. Assume that D is imaginary of even degree. If D has a factor P of odd degree, then there is a 2-torsion class of odd degree, namely the class of the ideal above P in $\mathcal{O}_D$ (which is not principal). If all d_i are even, then all ambiguous ideals (viz., ideals I such that $I = I^{-1}$) have even degree, but there is the unique ambiguous class (viz., an ideal class $[I]$ such that $[I] = [I]^{-1}$ in $\mathrm{Pic}(\mathcal{O}_D)$)

which is not the class of any ambiguous ideal (cf. Artin, loc. cit.). It is the class of the ideal $(C, B + \sqrt{D})$ if we write $D = eC^2 + B^2$ for some C of degree $\frac{k}{2}$ and $\deg(B) < \deg(C)$. The parity of its degree is well-defined and equal to $\deg(C) = \frac{k}{2} \bmod 2$. If $s > 1$ and all d_i are even, then k is divisible by 4; in particular, the degree of the ambiguous class is even. On the other hand, if $s = 1$, then the ambiguous class has even degree exactly when k is divisible by 4. This is what we wanted to prove. □

(3.2) I know of no independent proof of the second fact of corollary (1.6). It follows from (1.1) and (1.4) in the following way. The divisor $\rho(\infty_1 - \infty_2)$ has order $|R_D|/\rho$ in $J_D[2^\infty]$. If it is not further divisible, then we can write

$$J_D[2^\infty] = \mathbf{Z}/2^{a_1} \times \cdots \times \mathbf{Z}/2^{a_r},$$

where $2^{a_1} = |R_D|/\rho$ and $r = \hat{r}_2(D)$ is the geometric rank. Since the whole group of order 2^{a_1} coincides with $R_D[2^\infty]$, it is killed by the map $J_D[2^\infty] \to \mathrm{Pic}(\mathcal{O}_D)[2^\infty]$, so the 2-rank of the latter group would satisfy $r_2(D) = \hat{r}_2(D) - 1$. Looking at theorem (1.1) and (1.4), this only happens in the real case if $s = 1$ and k is divisible by 4, or all d_i are even. □

(3.3) The claim of corollary (1.7) can be proved as follows: by (1.6), $\rho(\infty_1 - \infty_2)$ is further divisible in $J_D[2^\infty]$, say $= 2\mathcal{D}$, where $\mathcal{D}$ is of order > 2 ($2\mathcal{D} = \rho(\infty_1 - \infty_2) \neq 0$ since $|R_D|$ is even). □

A c k n o w l e d g m e n t. The author is post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO - Vlaanderen). This work was done while visiting the MPIM.

References

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen, I, II. Math. Z. **19** (1924), 153–246, = Collected Papers, pp. 1–94.

[2] G. Cornelissen, Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields, Math. Ann. **314** (1999), 175–196.

[3] G. Cornelissen, The 2-primary class group of certain hyperelliptic curves, Max-Planck-Institut für Mathematik Preprint 1999-96.

[4] E. Friedman and L.C. Washington, On the distribution of divisor class groups of curves over a finite field, Théorie des nombres (Quebec, PQ, 1987), 227–239, de Gruyter, Berlin, 1989.

[5] N. Koblitz, Hyperelliptic cryptosystems, J. of Cryptology **1** (1988), 139–150.

[6] M. Rosen, The Hilbert class field in function fields, Expos. Math. **5** (1987), 365–378.

[7] R. Scheidler, A. Stein and H.C. Williams, Key-exchange in real quadratic congruence function fields, Des. Codes Cryptogr. **7** (1996), 153–174.

[8] S. Sémirat, Genus theory for quadratic function fields and applications, Inst. de Math. de Jussieu, Prépublication 1998-192.

[9] X. Zhang, Ambiguous classes and 2-rank of class group of quadratic function field, J. of China Univ. of Science and Technology **17** (1987), 425–430.

Gunther Cornelissen
Max-Planck-Institut für Mathematik
Vivatsgasse 7
D-53111 Bonn

University of Gent
Department of Pure Mathematics
Galglaan 2
B-9000 Gent

e-mail gc@cage.rug.ac.be