CURVES IN CHARACTERISTIC 2 WITH NON-TRIVIAL 2-TORSION

WOUTER CASTRYCK, MARCO STRENG, DAMIANO TESTA

Abstract. Cais, Ellenberg and Zureick-Brown recently observed that over finite fields of characteristic two, all sufficiently general smooth plane projective curves of a given odd degree admit a non-trivial rational 2-torsion point on their Jacobian. We extend their observation to curves given by Laurent polynomials with a fixed Newton polygon, provided that the polygon satisfies a certain combinatorial property. We also show that in each of these cases, the sufficiently general condition is implied by being ordinary. Our treatment includes many classical families, such as hyperelliptic curves of odd genus and $C_{a,b}$ curves. In the hyperelliptic case, we provide alternative proofs using an explicit description of the 2-torsion subgroup.

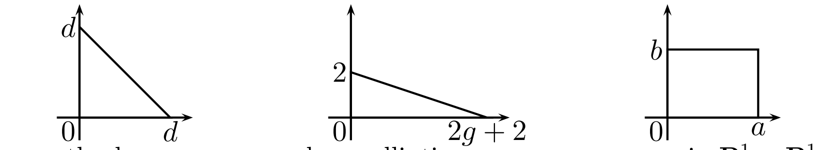
1. Introduction

The starting point of this article is a recent theorem by Cais, Ellenberg and Zureick-Brown [CEZB, Thm. 4.2], asserting that over a finite field k of characteristic 2, almost all smooth plane projective curves of a given odd degree $d \geq 3$ have a non-trivial k-rational 2-torsion point on their Jacobian. Here, 'almost all' means that the corresponding proportion converges to 1 as $\#k$ and/or d tend to infinity. The underlying observation is that such curves admit

- a 'geometric' k-rational half-canonical divisor Θ_{geom}: the canonical class of a smooth plane projective curve of degree d equals $(d-3)H$, where H is the class of hyperplane sections; if d is odd then $\frac{1}{2}(d-3)H$ is half-canonical,
- an 'arithmetic' k-rational half-canonical divisor Θ_{arith} (whose class is sometimes called the *canonical theta characteristic*), related to the fact that over a perfect field of characteristic 2, the derivative of a Laurent series is always a square [Mum, p. 191].

The difference $\Theta_{\text{geom}} - \Theta_{\text{arith}}$ maps to a k-rational 2-torsion point on the Jacobian. The proof of [CEZB, Thm. 4.2] then amounts to showing that, quite remarkably, this point is almost always non-trivial.

There exist many classical families of curves admitting such a geometric half-canonical divisor. Examples include hyperelliptic curves of odd genus g, whose canonical class is given by $(g-1)g^1_2$ (where g^1_2 denotes the hyperelliptic pencil), and smooth projective curves in $\mathbf{P}^1_k \times \mathbf{P}^1_k$ of even bidegree (a, b) (both a and b even, that is), where the canonical class reads $(a-2)R_1 + (b-2)R_2$ (here R_1, R_2 are the two rulings of $\mathbf{P}^1_k \times \mathbf{P}^1_k$). The families mentioned so far are parameterized by sufficiently generic polynomials that are supported on the polygons



smooth plane curves of degree d | hyperelliptic curves of genus g | curves in $\mathbf{P}^1_k \times \mathbf{P}^1_k$ of bidegree (a, b),

respectively. The following lemma, which is an easy consequence of the theory of toric surfaces (see Section 2), gives a purely combinatorial reason for the existence of a half-canonical divisor in these cases.

Lemma 1. *Let k be a perfect field and let Δ be a two-dimensional lattice polygon. For each edge $\tau \subset \Delta$, let $a_\tau X + b_\tau Y = c_\tau$ be its supporting line, where $\gcd(a_\tau, b_\tau) = 1$. Suppose that the system of congruences*

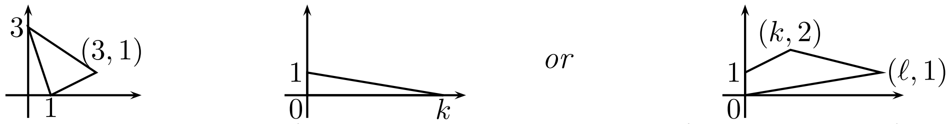
$$\{\ a_\tau X + b_\tau Y \equiv c_\tau + 1 \pmod 2\ \}_{\tau \text{ edge of } \Delta} \tag{1}$$

admits a solution in $\mathbf{Z}^2$. Then any sufficiently general Laurent polynomial $f \in k[x^{\pm 1}, y^{\pm 1}]$ that is supported on Δ defines a curve carrying a k-rational half-canonical divisor on its non-singular complete model.

In the proof of Lemma 1 below, where we describe this half-canonical divisor explicitly, we will be more precise on the meaning of 'sufficiently general'.

Here again, when specializing to characteristic 2, there is, in addition, an arithmetic k-rational half-canonical divisor. So it is natural to wonder whether the proof of [CEZB, Thm. 4.2] still applies in these cases. We will show that it usually does.

Theorem 2. *Let Δ be a two-dimensional lattice polygon satisfying the conditions of Lemma 1, where in addition we assume that Δ is not unimodularly equivalent to*



for some $k \geq 1$ | *for some $0 \leq k < \ell \geq 3$ with k even and ℓ odd.*

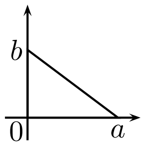
Then there exists a non-empty Zariski open subset $S_\Delta/\mathbf{F}_2$ of the space of Laurent polynomials that are supported on Δ having the following property. For every perfect field k of characteristic 2 and every $f \in S_\Delta(k)$, the Jacobian of the non-singular complete model of the curve defined by f has a non-trivial k-rational 2-torsion point.

(Right before the proof of Theorem 2 we will define the set S_Δ explicitly.) As a consequence, if k is a finite field of characteristic 2, then the proportion of Laurent polynomials that are supported on Δ, which define a curve whose Jacobian has a non-trivial k-rational 2-torsion point, tends to 1 as $\#k \to \infty$. See the end of Section 3, where we also discuss asymptotics for increasing dilations of Δ, i.e. the analogue of $d \to \infty$ in the smooth plane curve case. In Section 4 we give sufficient conditions that have a more arithmetic flavor, involving the rank of the Hasse-Witt matrix.

These observations seem new even for hyperelliptic curves of odd genus[1] (even though this is a well-known fact for the subfamily of hyperelliptic curves having a prescribed

[1] In view of the asymptotic consequences discussed in Section 3, this observation shows that [CFHS, Principle 3] can fail for $g > 2$.

k-rational Weierstrass point; see below). In this case we can give alternative proofs using an explicit description of the 2-torsion subgroup; see Section 5. Another interesting class of examples is given by the polygons



where a and b are not both even. The case $a = b$ corresponds to the smooth plane curves of odd degree considered in [CEZB]. The case $\gcd(a, b) = 1$ corresponds to so-called $C_{a,b}$ curves. The case $b = 2$, $a = 2g + 1$ (a subcase of the latter) corresponds to hyperelliptic curves having a prescribed k-rational Weierstrass point P. Note that in this case $g^1_2 \sim 2P$, so there is indeed always a k-rational half-canonical divisor, regardless of the parity of g.

Remark 3. This explains why Denef and Vercauteren had to allow a factor 2 while generating cryptographic hyperelliptic and $C_{a,b}$ curves in characteristic 2; see Sections 6 of [DV1, DV2].

Finally, the case $b = 3$, $a \geq 4$ corresponds to trigonal curves having maximal Maroni invariant (that is trigonal curves for which the series $(h^0(ng^1_3))_{n \in \mathbf{Z}_{\geq 0}}$ starts increasing by steps of 3 as late as the Riemann-Roch theorem allows it to do); if $a = 6$, these are exactly the genus-4 curves having a unique g^1_3.

We conclude by stressing that the results in this paper are unlikely to generalize to characteristic $p > 2$, by lack of an appropriate analogue of our arithmetic half-canonical divisor Θ_{arith}.

2. Half-canonical divisors from toric geometry

Let k be a perfect field, let $f = \sum_{(i,j) \in \mathbf{Z}^2} c_{i,j} x^i y^j \in k[x^{\pm 1}, y^{\pm 1}]$ be a Laurent polynomial, and let

$$\Delta(f) = \operatorname{conv}\left\{ (i,j) \in \mathbf{Z}^2 \,\middle|\, c_{i,j} \neq 0 \right\}$$

be the Newton polygon of f, which we assume to be two-dimensional. We say that f is *non-degenerate with respect to its Newton polygon* if for every face $\tau \subset \Delta(f)$ (vertex, edge, or $\Delta(f)$ itself) the system

$$f_\tau = \frac{\partial f_\tau}{\partial x} = \frac{\partial f_\tau}{\partial y} = 0 \qquad \text{with } f_\tau = \sum_{(i,j) \in \tau \cap \mathbf{Z}^2} c_{i,j} x^i y^j$$

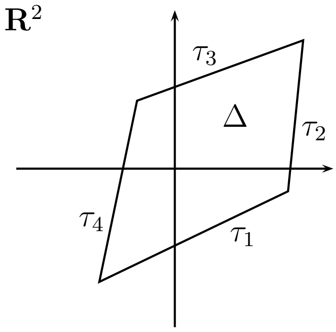
has no solutions[2] over an algebraic closure of k. For a given two-dimensional lattice polygon Δ, we say that f is Δ-*non-degenerate* if $\Delta(f) = \Delta$ and f is non-degenerate with respect to its Newton polygon. The condition of Δ-non-degeneracy is generically satisfied, in the sense that it is characterized by the non-vanishing of

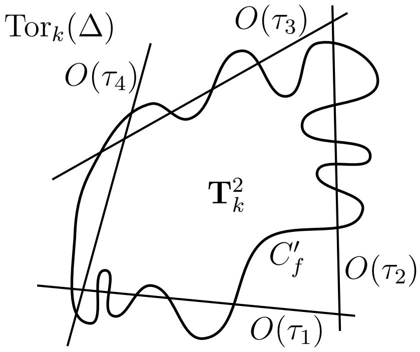
$$\rho_\Delta := \operatorname{Res}_\Delta\left(f, x\frac{\partial f}{\partial x}, y\frac{\partial f}{\partial y} \right) \in \mathbf{Z}[c_{i,j} | (i,j) \in \Delta \cap \mathbf{Z}^2]$$

(where $\operatorname{Res}_\Delta$ is the sparse resultant; ρ_Δ does not vanish identically in any characteristic [CV, §2]). Non-degenerate Laurent polynomials are always (absolutely) irreducible.

[2]Note that this is in fact automatically true if τ is a vertex.

To a two-dimensional lattice polygon Δ one can associate a toric surface $\text{Tor}_k(\Delta)$, which is a compactification of $\mathbf{T}_k^2 = \text{Spec}\, k[x^{\pm 1}, y^{\pm 1}]$ to which the natural self-action of the latter extends algebraically. This extended action decomposes $\text{Tor}_k(\Delta)$ in a finite number of orbits, which naturally correspond (in a dimension-preserving manner) to the faces of Δ; for each face τ, write $O(\tau)$ for the according orbit. Now if $f \in k[x^{\pm 1}, y^{\pm 1}]$ is a Δ-non-degenerate Laurent polynomial, the non-degeneracy condition with respect to Δ itself ensures that it cuts out a non-singular curve C_f in $\mathbf{T}_k^2 = O(\Delta)$. Similarly, one finds that its compactification C'_f in $\text{Tor}_k(\Delta)$ does not contain any of the zero-dimensional $O(\tau)$'s, and that it intersects the one-dimensional $O(\tau)$'s transversally.





In particular, since $\text{Tor}_k(\Delta)$ is normal, the non-degeneracy of f implies that C'_f is a non-singular complete model of C_f. See [CC, §3-4] and [CDV, §2] for more details.

Example 4. Assume that $\Delta = \text{conv}\{(0,0),(d,0),(0,d)\}$. In this case $\text{Tor}_k(\Delta)$ is just the projective plane, and the toric orbits are

- $\mathbf{T}_k^2 = O(\Delta)$,
- the three coordinate points $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$, which are the orbits of the form $O(\text{vertex})$,
- the three coordinate axes from which the coordinate points are removed: these are the orbits of the form $O(\text{edge})$.

Thus C'_f is a non-singular projective plane curve that is non-tangent to any of the coordinate axes, and that does not contain any of the coordinate points. This is essentially an if-and-only-if: an absolutely irreducible Laurent polynomial $f \in k[x^{\pm 1}, y^{\pm 1}]$, for which $\Delta(f) \subset \Delta$, is Δ-non-degenerate if and only if its zero locus in $\mathbf{T}_k^2$ compactifies to a non-singular degree d curve in $\mathbf{P}_k^2$ that is non-tangent to the coordinate axes, and that does not contain the coordinate points.

Example 5. Let $g \geq 2$ be an integer, and consider $f = y^2 + h_1(x)y + h_0(x)$, where $\deg h_1 \leq g{+}1$, $\deg h_0 = 2g{+}2$, and $h_0(0) \neq 0$. Then $\Delta(f) = \text{conv}\{(0,0),(2g{+}2,0),(0,2)\}$, and $\text{Tor}_k(\Delta(f))$ is the weighted projective plane $\mathbf{P}_k(1:g+1:1)$. Here again, if f is non-degenerate with respect to its Newton polygon then C'_f is a non-singular curve that is non-tangent to the coordinate axes and that does not contain any coordinate points. In this case C'_f is a hyperelliptic curve of genus g (cf. Remark 8).

Now for each edge $\tau \subset \Delta$ let $\nu_\tau \in \mathbf{Z}^2$ be the inward pointing primitive normal vector to τ, let p_τ be any element of $\tau \cap \mathbf{Z}^2$, and let D_τ be the k-rational divisor on C'_f cut out by $O(\tau)$. Using the Δ-non-degeneracy of f one can prove

$$\text{div} \frac{dx}{xy\frac{\partial f}{\partial y}} = \sum_{\tau \text{ edge}} (-\langle \nu_\tau, p_\tau \rangle - 1) D_\tau. \tag{2}$$

Here $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbf{R}^2$. See [CDV, Cor. 2.7] for an elementary but elaborate proof of (2). It is possible to give a more conceptual proof using adjunction theory, along the lines of [CLS, Prop. 10.5.8].

Remark 6. From the theory of sparse resultants it follows that $\partial f / \partial y$ does not vanish identically, so that the left-hand side of (2) makes sense. Note also that $0 = df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy$, so we could as well have written

$$\text{div} \frac{dy}{xy\frac{\partial f}{\partial x}}. \tag{3}$$

Proof of Lemma 1. Assume that f is Δ-non-degenerate (which, as mentioned above, is a non-empty Zariski open condition). Let $(i_0, j_0) \in \mathbf{Z}^2$ be a solution to the given system of congruences. We claim that the translated polygon $(-i_0, -j_0) + \Delta$ is such that all corresponding $\langle \nu_\tau, p_\tau \rangle$'s are odd. To see this, note that in this case $(0,0)$ is a solution to the according system of congruences (1). This implies that all c_τ's are odd. Together with $\langle \nu_\tau, p_\tau \rangle = \pm c_\tau$ this yields the claim. So by applying the above to $x^{-i_0} y^{-j_0} f$, we find that

$$\Theta_{\text{geom}} = \sum_{\tau \text{ edge}} \frac{-\langle \nu_\tau, p_\tau \rangle - 1}{2} D_\tau$$

is a k-rational half-canonical divisor on $C'_{x^{-i_0} y^{-j_0} f} = C'_f$. $\square$

Example 4 (continued). Assume that d is odd, so that the conditions from Lemma 1 are satisfied. Applying the above proof with $(i_0, j_0) = (1, 1)$ yields

$$\Theta_{\text{geom}} = \frac{d-3}{2} D_\infty$$

where D_∞ is the divisor cut out by the line at infinity. So we recover the divisor class mentioned in the introduction.

Remark 7. Still assume that $\Delta = \text{conv}\{(0,0), (d,0), (0,d)\}$ with d odd. We already noted that the condition of non-degeneracy restricts our attention to smooth plane curves of degree d that do not contain the coordinate points and that intersect the coordinate axes transversally. But of course *any* smooth plane curve of degree d carries a k-rational half-canonical divisor. This shows that the non-degeneracy condition, even though it is generically satisfied, is sometimes a bit stronger than needed.[3] For a general two-dimensional lattice polygon Δ, the according weaker condition reads that f is Δ-*toric*, meaning that $\Delta(f) \subset \Delta$, that $\Delta(f)^{(1)} = \Delta^{(1)}$, and that C_f compactifies to a non-singular

[3] The reader might want to note that there always exists an automorphism of $\mathbf{P}^2_k$ that puts our smooth plane curve in a non-degenerate position (at least if $\#k$ is sufficiently large). But for more general instances of Δ, the automorphism group of $\text{Tor}_k(\Delta)$ may be much smaller (e.g. the only automorphisms may be the ones coming from the $\mathbf{T}^2_k$-action), in which case it might be impossible to resolve tangency to the one-dimensional toric orbits.

curve C'_f in $\mathrm{Tor}_k(\Delta)$. Here $\Delta^{(1)}$ denotes the lattice polygon obtained by taking the convex hull of the $\mathbf{Z}^2$-points that lie in the interior of Δ, and similarly for $\Delta(f)^{(1)}$. See [CC, §4] for more background on this notion. Now we have to revisit Remark 6, however: there do exist instances of Δ-toric Laurent polynomials $f \in k[x^{\pm 1}, y^{\pm 1}]$ for which $\partial f / \partial y$ *does* vanish identically (example: take $f = 1 + x^2y^2 + x^3y^2$ and $\Delta = \Delta(f)$). For these instances the left-hand side of (2) does not make sense. But in that case $\partial f / \partial x$ does not vanish identically (otherwise C_f would have singularities), and one can prove that (2) holds with the left-hand side replaced by (3).

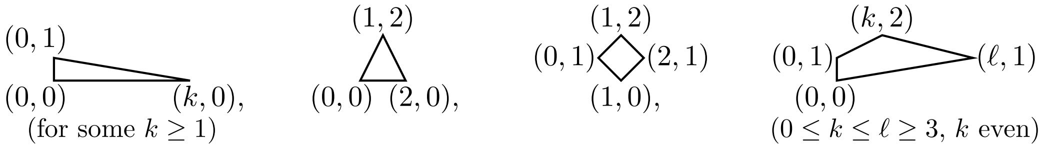
Remark 8. We mention two other well-known features of Δ-non-degenerate (or Δ-toric) Laurent polynomials, that can be seen as consequences to (2); see for instance [CC, CV] and the references therein:

- the genus of C'_f equals $\#\left(\Delta^{(1)} \cap \mathbf{Z}^2\right)$,
- if $\#\left(\Delta^{(1)} \cap \mathbf{Z}^2\right) \geq 2$, then C'_f is hyperelliptic if and only if $\Delta^{(1)} \cap \mathbf{Z}^2$ is contained in a line.

3. Proof of the main result

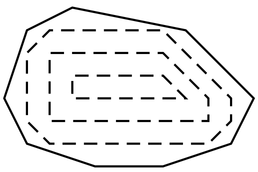
Lemma 9. *Let Δ be a two-dimensional lattice polygon and suppose as in Lemma 1 that* (1) *admits a solution in $\mathbf{Z}^2$. If Δ is not among the polygons excluded in the hypothesis of Theorem 2, then there is a solution of* (1) *contained in $\Delta \cap \mathbf{Z}^2$.*

Proof. Let us first classify all two-dimensional lattice polygons Δ for which the reduction-modulo-2 map $\pi_\Delta \colon \Delta \cap \mathbf{Z}^2 \to (\mathbf{Z}/(2))^2$ is not surjective. If the interior lattice points of Δ lie on a line, then surjectivity fails if and only if Δ is among



(a) (b) (c) (d)

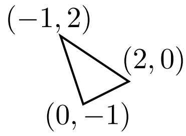
(up to unimodular equivalence). This assertion follows from Koelman's classification; see [Koe, Ch. 4] or [Cas, Thm. 10]. Now any two-dimensional lattice polygon Δ can be peeled into 'onion skins', by subsequently taking the convex hull of the interior lattice points, until one ends up with a lattice polygon whose interior lattice points are contained in a line.



If π_Δ is not surjective, then clearly π_Ω is not surjective for each onion skin Ω. In particular, the last onion skin must necessarily be among (a-d).

But for a lattice polygon to arise as an onion skin of a strictly larger lattice polygon Δ is a stringent condition. Using the criterion from [HS, Lem. 9-11] one sees that the only polygons among (a-d) of this type are the polygons (a) with $k = 1$ or $k = 2$, the polygon

(b) and the polygon (c). The same criterion shows that the only instance of such a larger Δ for which π_Δ is not surjective is



(e)

(up to unimodular equivalence). The latter, again by [HS, Lem. 9-11], is not an onion skin of a strictly bigger lattice polygon itself. This ends the classification: up to unimodular equivalence, the instances of Δ for which π_Δ is not surjective are (a)-(e).

Now let Δ be a two-dimensional lattice polygon and suppose that (1) admits a solution in $\mathbf{Z}^2$. If π_Δ is surjective, then it clearly also admits a solution in $\Delta \cap \mathbf{Z}^2$. So we may assume that Δ is among (a-e). Then the lemma follows by noting that cases (b), (c) and (d) with ℓ even admit the solution $(1,1) \in \Delta \cap \mathbf{Z}^2$, and that cases (a), (e) and (d) with ℓ odd were excluded in the énoncé. $\square$

Remark 10. Because of Remark 8, the excluded polygons correspond to certain classes of smooth plane quartics, rational curves, and hyperelliptic curves, respectively.

We can now define the variety S_Δ mentioned in the statement of Theorem 2. Namely, we will prove the existence of a non-trivial k-rational 2-torsion point under the assumption that

- f is Δ-non-degenerate (i.e. the genericity assumption from Lemma 1), and
- for at least one solution $(i_0, j_0) \in \Delta \cap \mathbf{Z}^2$ to the system of congruences (1), the corresponding coefficient c_{i_0,j_0} is non-zero.

So we can let S_Δ be defined by $c_{i_0,j_0}\rho_\Delta \neq 0$.

Remark 11. Here again, one can weaken the condition of being Δ-non-degenerate to being Δ-toric, as described in Remark 7. When that stronger version is applied to $\Delta = \mathrm{conv}\{(0,0),(d,0),(0,d)\}$ with d odd, one exactly recovers [CEZB, Thm. 4.2].

Proof of Theorem 2. By replacing f with $x^{-i_0}y^{-j_0}f$ if needed, we assume that $(0,0) \in \Delta$ is a solution to the system of congruences (1) and that the constant term of f is non-zero. As explained in [Mum, p. 191], C'_f comes equipped with a k-rational divisor Θ_{arith} such that $2\Theta_{\mathrm{arith}} = \mathrm{div}\, dx$. (Recall that the derivative of a Laurent series over k is always a square, so the order of dx at a point of C'_f is indeed even.) On the other hand, Lemma 1 and its proof provide us with a k-rational divisor Θ_{geom} such that

$$2\Theta_{\mathrm{geom}} = \mathrm{div}\, \frac{dx}{xy\frac{\partial f}{\partial y}}.$$

In order to prove that $\Theta_{\mathrm{geom}} \not\sim \Theta_{\mathrm{arith}}$ (and hence that $\mathrm{Jac}(C'_f)$ has a non-trivial k-rational 2-torsion point), we need to show that

$$xy\frac{\partial f}{\partial y}$$

is a non-square when considered as an element of the function field $k(C_f)$. If it were a square, then there would exist Laurent polynomials α, G, H such that

$$H^2 xy \frac{\partial f}{\partial y} + \alpha f = G^2 \qquad \text{in } k[x^{\pm 1}, y^{\pm 1}], \tag{4}$$

where $f \nmid H$. Taking derivatives with respect to y yields

$$(\alpha + H^2 x) \frac{\partial f}{\partial y} = \frac{\partial \alpha}{\partial y} f,$$

which together with (4) results in

$$\left((\alpha + H^2 x)\alpha + H^2 xy \frac{\partial \alpha}{\partial y} \right) f = (\alpha + H^2 x) G^2.$$

Since f is irreducible, it follows that $f \mid (\alpha + H^2 x)$ or $f \mid G^2$. Using (4) and $f \nmid H$, the latter implies that $f \mid \frac{\partial f}{\partial y}$, which is a contradiction (by the theory of sparse resultants, see Remark 6; one can alternatively repeat the argument using (3) if wanted). So we know that $f \mid (\alpha + H^2 x)$. Along with (4) we conclude that there exists a Laurent polynomial $\beta \in k[x^{\pm 1}, y^{\pm 1}]$ such that

$$H^2 x \left(y \frac{\partial f}{\partial y} + f \right) + \beta f^2 = G^2.$$

Taking derivatives with respect to x yields

$$H^2 \left(f + x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y} + xy \frac{\partial^2 f}{\partial x \partial y} \right) + \frac{\partial \beta}{\partial x} f^2 = 0.$$

Since f has a non-zero constant term, the large factor between brackets is non-zero. On the other hand, since $f \nmid H$, it must be a multiple of f^2. Note that $\Delta(f^2) = 2\Delta(f)$, while $\Delta(f + \cdots + xy\partial^2 f/(\partial x \partial y)) \subset \Delta(f)$. This is a contradiction. $\square$

We end this section by discussing some asymptotic consequences to Theorem 2.

Growing field size. Let Δ be a two-dimensional lattice polygon satisfying the conditions of Theorem 2. Let k be a finite field of characteristic 2. Because non-degeneracy is characterized by the non-vanishing of ρ_Δ, the proportion of Δ-non-degenerate Laurent polynomials $f \in k[x^{\pm 1}, y^{\pm 1}]$ (amongst all Laurent polynomials that are supported on Δ) converges to 1 as $\#k \to \infty$. Then Theorem 2 implies:

$$\lim_{\#k \to \infty} \text{Prob} \left(\text{Jac}(C'_f)(k)[2] \neq 0 \;\middle|\; f \in k[x^{\pm 1}, y^{\pm 1}] \text{ is } \Delta\text{-non-degenerate} \right) = 1.$$

As soon as $\#(\Delta^{(1)} \cap \mathbf{Z}^2) \geq 2$ this is deviating statistical behavior: in view of Katz-Sarnak-Chebotarev-type density theorems [KS, Theorem 9.7.13], for a general smooth proper family of genus g curves, one expects that the probability of having a non-trivial rational 2-torsion point on the Jacobian approaches the chance that a random matrix in $\text{GL}_g(\mathbf{F}_2)$ satisfies $\det(M - \text{Id}) = 0$, which is

$$-\sum_{r=1}^{g} \prod_{j=1}^{r} \frac{1}{1 - 2^j}$$

by [CFHS, Thm. 6]. For $g = 1, 2, 3, 4, \ldots$, these probabilities are $1, \frac{2}{3}, \frac{5}{7}, \frac{32}{45}, \ldots$ (converging to about 0.71121).

In the table below we denote by $\square_i$ the square $[0, i]^2$ (for $i = 2, 3, 4$), by H_g the hyperelliptic polygon $\text{conv}\{(0,0), (2g+2, 0), (0, 2)\}$ (for $g = 7, 8$), and by E the exceptional polygon $\text{conv}\{(1,0), (3,1), (0,3)\}$ from the statement of Theorem 2. Each entry corresponds to a sample of 10^4 uniformly randomly chosen Laurent polynomials $f \in k[x^{\pm 1}, y^{\pm 1}]$ that are supported on $\square_2, \square_3, \ldots$ The table presents the proportion of f's for which $\text{Jac}(C'_f)$ has a non-trivial k-rational 2-torsion point, among those f's that are non-degenerate with respect to their Newton polygon $\Delta(f) = \square_2, \square_3, \ldots$ The count was carried out using Magma [BCP], either by using the intrinsic function for computing the Hasse-Weil zeta function, or by spelling out the Hasse-Witt matrix [SV, Thm. 1.1] and applying Manin's theorem [Man].

k	$\square_2$ $(g=1)$	$\square_3$ $(g=4)$	$\square_4$ $(g=9)$	H_7 $(g=7)$	H_8 $(g=8)$	E $(g=3)$
$\mathbf{F}_2$	0/0	0.370	0.958	0.995	0.670	0.143
$\mathbf{F}_4$	0.750	0.621	1.000	1.000	0.795	0.449
$\mathbf{F}_8$	0.884	0.654	1.000	1.000	0.852	0.591
$\mathbf{F}_{16}$	0.940	0.697	1.000	1.000	0.872	0.661
$\mathbf{F}_{32}$	0.968	0.704	1.000	1.000	0.877	0.696
$\mathbf{F}_{64}$	0.986	0.716	1.000	1.000	0.880	0.694
$\mathbf{F}_{128}$	0.992	0.703	1.000	1.000	0.889	0.708
$\mathbf{F}_{256}$	0.996	0.709	1.000	1.000	0.888	0.707
asymptotic prediction	1	$\frac{32}{45} \approx 0.711$	1	1	$\frac{8}{9} \approx 0.889$	$\frac{5}{7} \approx 0.714$

Note that the conditions of Theorem 2 are satisfied for $\square_2$, $\square_4$ and H_7. So here we proved that the proportion converges to 1. In the case of H_8, by the material in Section 5 (see Corollary 27) we know that the proportion converges to $\frac{8}{9}$. In the other two cases $\square_4$ and E we have no clue, so our best guess is that these follow the $\text{GL}_g(\mathbf{F}_2)$-model.

Growing polygon. Let k be a finite field of characteristic 2. If Δ is a two-dimensional lattice polygon satisfying the conditions of Lemma 1, then the same holds for each odd Minkowski multiple $(2n+1)\Delta$. It seems reasonable to assume that the proportion of $(2n+1)\Delta$-non-degenerate Laurent polynomials $f \in k[x^{\pm 1}, y^{\pm 1}]$, amongst all Laurent polynomials that are supported on $(2n+1)\Delta$, converges to a certain strictly positive constant.

This is certainly true for the larger proportion of $(2n+1)\Delta$-*toric* Laurent polynomials. Namely, using [Poo2, Thm. 1.2] one can show that this proportion converges to

$$Z_{\text{Tor}_k(\Delta)\setminus S}((\#k)^{-3})^{-1} \cdot Z_S((\#k)^{-1})^{-1}$$

as $n \to \infty$; here S denotes the (finite) set of singular points of $\text{Tor}_k(\Delta)$, and Z stands for the Hasse-Weil Zeta function. It should be possible to prove a similar statement for non-degenerate Laurent polynomials by redoing the closed point sieve in the proof of [Poo2, Thm. 1.2], but we did not work out the details of this.

On the other hand, the number of solutions to (1) inside $(2n+1)\Delta \cap \mathbf{Z}^2$ tends to infinity. So the assumption would allow one to conclude:

$$\lim_{n\to\infty} \text{Prob}\left(\text{Jac}(C'_f)(k)[2] \neq 0 \;\middle|\; f \in k[x^{\pm 1}, y^{\pm 1}] \text{ is } (2n+1)\Delta\text{-non-degenerate} \right) = 1.$$

This is again deviating statistical behavior: in view of Cohen-Lenstra type heuristics, one naively expects a probability of about

$$1 - \prod_{j=1}^{\infty} (1 - 2^{-j}) \approx 0.71121;$$

see [CEZB] for some additional comments.

When applied to $(2n+1)\Sigma$-toric Laurent polynomials, where Σ is the standard simplex, one recovers the claim made before [CEZB, Thm. 4.2].

4. Connections with the rank of the Hasse-Witt matrix

Let us revisit the proof of Theorem 2 from the previous section. Our sufficient condition that

$$c_{i_0,j_0} \neq 0 \quad \text{for at least one solution } (i_0, j_0) \in \Delta \cap \mathbf{Z}^2 \text{ to the system (1)} \tag{5}$$

(see right before Remark 11) seems rather equation-specific. However, it is easy to show that automorphisms of $\text{Tor}_k(\Delta)$ cannot alter whether (5) is satisfied or not. For instance, in the case of smooth plane projective curves of odd degree $d \geq 3$, one verifies that if

$$F(X, Y, Z) = \sum_{i+j \leq d} c_{i,j} X^i Y^j Z^{d-i-j} \in k[X, Y, Z]$$

is such that $c_{i,j} = 0$ as soon as both i and j are odd, then applying a linear change of variables does not affect this. This suggests that something more fundamental is going on. In Conjecture 15 below we will formulate a guess for a geometric interpretation of condition (5), involving the rank of the Hasse-Witt matrix (or of the Cartier-Manin operator, if one prefers). We will prove this guess in a number of special cases. Our main references on the Hasse-Witt matrix are [Man, Ser, SV].

Here is a first fact:

Lemma 12. *Let k be a perfect field of characteristic 2, let Δ be a two-dimensional lattice polygon satisfying the conditions of Lemma 1, and let $f = \sum_{(i,j) \in \mathbf{Z}^2} c_{i,j} x^i y^j \in k[x^{\pm 1}, y^{\pm 1}]$ be a Δ-non-degenerate (or Δ-toric) Laurent polynomial. Let*

- *g be the genus of C'_f, i.e. $g = \#(\Delta^{(1)} \cap \mathbf{Z}^2)$, and*
- *ρ be the number of solutions $(i_0, j_0) \in \Delta \cap \mathbf{Z}^2$ to the system of congruences (1).*

If $c_{i_0,j_0} = 0$ for every such solution, then the rank of the Hasse-Witt matrix of C'_f is at most $g - \rho$.

Proof. By [CDV, Cor. 2.6 and 2.7] we find that

$$\left\{ x^i y^j \frac{dx}{xy \frac{\partial f}{\partial y}} \right\}_{(i,j) \in \Delta^{(1)} \cap \mathbf{Z}^2} \tag{6}$$

is a basis for the space of regular differentials on C'_f. (If in the Δ-toric case the denominator happens to vanish identically, one can replace $dx/(\partial f/\partial y)$ by $dy/(\partial f/\partial x)$ as explained in Remark 7.) Assume that $c_{i_0,j_0} = 0$ for each of the ρ solutions $(i_0, j_0) \in \Delta \cap \mathbf{Z}^2$ to the system (1). Remark that these solutions are all contained in $\Delta^{(1)}$. One then verifies that the ρ corresponding differentials $z_{i_0,j_0} dx$, where

$$z_{i_0,j_0} = \frac{x^{i_0} y^{j_0}}{xy \frac{\partial f}{\partial y}},$$

satisfy $\partial z_{i_0,j_0}/\partial x = 0$. Following the construction from [SV, §1] we conclude that at least ρ rows of the Hasse-Witt matrix with respect to the basis (6) are zero. □

As an interesting corollary we obtain:

Corollary 13. *Let k and Δ be as before and let f be a Δ-non-degenerate (or Δ-toric) Laurent polynomial over k. Assume moreover that Δ is not among the polygons excluded in the statement of Theorem 2. If C'_f is ordinary then it has a non-trivial k-rational 2-torsion point on its Jacobian.*

Proof. In view of Lemma 9, the fact that Δ is not among the excluded polygons ensures that $\rho > 0$. A result by Serre [Ser, Prop. 10] says that C'_f is ordinary if and only if its Hasse-Witt matrix has rank g. So the previous lemma implies that if C'_f is ordinary, then (5) is satisfied. The claim now follows from Theorem 2. □

Remark 14. The following alternative proof of Corollary 13 was suggested to us by Christophe Ritzenthaler. A result by Stöhr and Voloch [SV, Cor. 3.2] states that the Hasse-Witt matrix has rank $g - h^0(C'_f, \Theta_{\text{arith}})$. So if C'_f is ordinary then $h^0(C'_f, \Theta_{\text{arith}}) = 0$, and in particular Θ_{arith} cannot be linearly equivalent to an effective divisor. Now if Δ is not among the excluded polygons, then by Lemma 9 there is at least one solution $(i_0, j_0) \in \Delta \cap \mathbf{Z}^2$ to the system (1). Fix such a solution and consider the corresponding translated polygon $(-i_0, -j_0) + \Delta$, as in the proof of Lemma 1. We again find that all $\langle \nu_\tau, p_\tau \rangle$'s are odd, but now because $(0,0) \in (-i_0, -j_0) + \Delta$ we also find that they are strictly negative. In other words the resulting half-canonical divisor Θ_{geom} is effective. Hence Θ_{geom} and Θ_{arith} are non-equivalent. Their difference then yields a non-trivial k-rational 2-torsion point on $\text{Jac}(C'_f)$.

Our guess is that Lemma 12 admits the following converse. This would give the desired geometric interpretation of condition (5).

Conjecture 15. *Let k be a perfect field of characteristic 2, let Δ be a two-dimensional lattice polygon satisfying the conditions from Lemma 1, and let f be a Δ-non-degenerate (or Δ-toric) Laurent polynomial. Then the rank of the Hasse-Witt matrix of C'_f is at least $g - \rho$, and the bound is attained if and only if $c_{i_0,j_0} = 0$ for every solution $(i_0, j_0) \in \Delta \cap \mathbf{Z}^2$ to the system of congruences (1).*

We can prove this conjecture in a number of special cases. Because the statements seem interesting in their own right, we will each time reformulate (and sometimes refine) Conjecture 15 accordingly.

Theorem 16 (Conjecture 15 for smooth plane curves of odd degree). *Let k be a perfect field of characteristic 2, let $d \geq 3$ be an odd integer and let $f = \sum_{i+j \leq d} c_{i,j} x^i y^j \in k[x, y]$ define a smooth plane projective curve C/k of degree d and genus $g = (d-1)(d-2)/2$. Then the rank of the Hasse-Witt matrix of C is bounded from below by*

$$g - \frac{d^2 - 1}{8} = \frac{3}{8}(d-1)(d-3)$$

Furthermore equality holds if and only if $c_{i,j} = 0$ as soon as i and j are odd.

Proof. Recall from Remark 14 that Stöhr and Voloch [SV, Cor. 3.2] proved that the rank of the Hasse-Witt matrix is $g - h^0(C, \Theta_{\mathrm{arith}})$. By the Brill-Noether theory of smooth plane curves [Har, Thm. 2.1] we have

$$h^0(C, D) \leq \frac{\frac{d-1}{2}\frac{d+1}{2}}{2} = (d^2 - 1)/8 \tag{7}$$

for any divisor D on C of degree $g - 1$. In particular this also holds for $D = \Theta_{\mathrm{arith}}$, from which the lower bound follows. As for the last statement, by [Har, part 2b of Thm. 2.1] the bound in (7) is attained if and only if D is in the class of $\frac{d-3}{2}H$, i.e. if and only if $D \sim \Theta_{\mathrm{geom}}$. But the proof of Theorem 2 (or of [CEZB, Thm. 4.2]) is precisely about showing that if $c_{i,j} \neq 0$ for some i and j that are both odd, then $\Theta_{\mathrm{arith}} \not\sim \Theta_{\mathrm{geom}}$. This yields the 'only if' part, while the 'if' part follows from Lemma 12. □

Theorem 17 (Conjecture 15 for hyperelliptic curves of odd genus). *Let k be a perfect field of characteristic 2. Let C be a hyperelliptic curve of odd genus $g \geq 3$, given in weighted projective form by*

$$C\colon \quad Y^2 + H_1(X, Z)Y = H_0(X, Z), \tag{8}$$

where H_1 and H_0 in $k[X, Z]$ are homogeneous of degrees $g + 1$ and $2g + 2$ respectively. Then the rank of the Hasse-Witt matrix of C equals

$$g - \frac{1}{2} \deg \gcd \left(H_1, Z^{-1} \frac{\partial}{\partial X} H_1 \right).$$

In particular, it is bounded from below by

$$g - \frac{g+1}{2} = \frac{g-1}{2},$$

where equality holds if and only if $\frac{\partial}{\partial X} H_1 = 0$.

Proof. Write $H_1 = \sum_{i=0}^{g+1} c_i X^i Z^{g+1-i}$ and define

$$P(X, Z) = \sum_{i=0}^{(g+1)/2} c_{2i} X^i Z^{(g+1)/2-i} \qquad \text{and} \qquad Q(X, Z) = \sum_{i=0}^{(g-1)/2} c_{2i+1} X^i Z^{(g-1)/2-i}.$$

Note that $H_1 = P^2 + XZQ^2$ and $\frac{\partial}{\partial X} H_1 = ZQ^2$. Now the polynomial $f = y^2 + H_1(x, 1)y + H_0(x, 1)$ is Δ-toric, where $\Delta = \mathrm{conv}\{(0, 0), (2g + 2, 0), (0, 2)\}$; here C'_f is nothing else but C. An explicit computation shows that the Hasse-Witt matrix with respect to the basis

(6) equals, up to a reordering of the rows, the Sylvester matrix of P and Q. It is well-known that the corank of the Sylvester matrix of two polynomials equals the degree of their greatest common divisor, which in our case equals

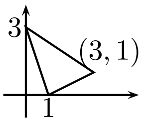
$$\deg\gcd(P,Q) = \frac{1}{2}\deg\gcd(P^2,Q^2) = \frac{1}{2}\deg\gcd\left(H_1, Z^{-1}\frac{\partial}{\partial X}H_1\right).$$

The remaining claims follow immediately. $\square$

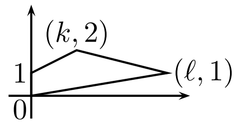
Remark 18. This indeed implies Conjecture 15 for hyperelliptic curves of odd genus because $\frac{\partial}{\partial X}H_1 = 0$ if and only if all terms $c_{i,j}x^iy^j$ in $f = y^2 + H_1(x,1)y + H_0(x,1)$ with i and j odd are 0.

Remark 19. The lower bound $(g-1)/2$ holds for arbitrary curves C of genus g (not necessarily odd) over fields of characteristic 2, and it can be attained by hyperelliptic curves only. This follows from Clifford's theorem, as explained in [SV, Cor. 3.2].

Theorem 20 (Conjecture 15 for the exceptional polygons)**.** *Let k be a perfect field of characteristic* 2*, let Δ be one of the polygons*



or



for some $0 \leq k < \ell \geq 3$ with k even and ℓ odd

that were excluded in the statement of Theorem 2, and let $f \in k[x^{\pm 1}, y^{\pm 1}]$ be Δ-non-degenerate (or Δ-toric). Then the rank of the Hasse-Witt matrix of C'_f is equal to $g = \#(\Delta^{(1)} \cap \mathbf{Z}^2)$. In particular C'_f is ordinary.

Proof. The polygon on the left corresponds to smooth plane quartics of the form

$$c_{1,0}XZ^3 + c_{1,1}XYZ^2 + c_{2,1}X^2YZ + c_{3,1}X^3Y + c_{1,2}XY^2Z + c_{0,3}Y^3Z.$$

The Hasse-Witt matrices of smooth plane quartics are explicitly described at the end of [SV, §3]. In our case this gives

$$\begin{pmatrix} c_{1,1} & c_{3,1} & 0 \\ 0 & c_{2,1} & c_{0,3} \\ c_{1,0} & 0 & c_{1,2} \end{pmatrix}$$

with determinant $c_{1,1}c_{2,1}c_{1,2} + c_{1,0}c_{3,1}c_{0,3}$. With the aid of a computer algebra package one can verify that this determinant is non-zero (using that the curve is smooth).

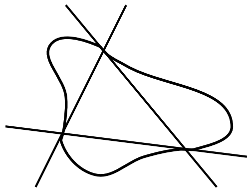
As for the polygons on the right, we have that $f = cx^ky^2 + h_1(x)y + c'$ for non-zero $c, c' \in k$ and a degree $\ell = g+1$ polynomial $h_1(x) \in k[x]$. Substituting $y \leftarrow yx^{-k}$ and multiplying the equation by $c^{-1}x^k$ puts our curve in the Weierstrass form

$$y^2 + c^{-1}h_1(x)y + c^{-1}c'x^k.$$

Using that k is even one sees that $h_1(x)$ is square-free (otherwise there would be an affine singularity). The result then follows from the previous theorem. $\square$

A fun corollary is the following geometric sufficient condition for ordinarity. Remark that similar conditions have been described before (such as the existence of 7 bitangent lines, which is actually sufficient and necessary; see [SV, §3]).

Corollary 21. *Let C be a smooth plane quartic curve over a field k of characteristic 2 admitting three non-colinear inflection points, such that the corresponding tangent lines are precisely the lines through two of these points.*



Then C is ordinary.

Proof. A projective transformation positions the three inflection points at $(0:0:1)$, $(0:1:0)$ and $(1:0:0)$. One verifies that the dehomogenization of the corresponding defining polynomial is Δ-non-degenerate, where Δ is the left-most polygon in the statement of the previous corollary. □

Remark 22. Theorems 16, 17 and 20 provide several characteristic 2 examples of families of curves whose Hasse-Witt matrices have constant rank. This (partly) addresses Question 2 of [FP, §3.7].

5. Hyperelliptic curves

Let C be a hyperelliptic curve of genus $g \geq 2$ over a perfect field k. Then C has a smooth weighted projective plane model of the form (8). The Newton polygon of (the defining polynomial of) the corresponding affine model $y^2 + H_1(x,1)y - H_0(x,1) = 0$ is contained in a triangle with vertices $(0,0)$, $(2g+2,0)$ and $(0,2)$, and is generically equal to this triangle. In particular, Theorem 2 implies that if the characteristic of k is 2 and C is sufficiently general of odd genus, then its Jacobian has a non-trivial k-rational 2-torsion point. By Corollary 13 we can replace 'sufficiently general' by 'ordinary'.

The purpose of this stand-alone section is to give alternative proofs of these facts (Corollaries 25 and 27), using an explicit description of the 2-torsion subgroup of $\mathrm{Jac}(C)$.

Theorem 23. *Let C/k be a hyperelliptic curve over a perfect field k of characteristic 2 given by a smooth model (8). The Jacobian of C has* no *rational point of order 2 if and only if $H_1(X,Z)$ is a power of an irreducible odd-degree polynomial in $k[X,Z]$.*

Corollary 24. *Let C/k be a hyperelliptic curve of odd 2-rank over a perfect field k of characteristic 2. Then the Jacobian of C has a k-rational point of order 2.*

Corollary 25. *Let C/k be an ordinary hyperelliptic curve of odd genus over a perfect field k of characteristic 2. Then the Jacobian of C has a k-rational point of order 2.*

Corollary 26. *Let C/k be a hyperelliptic curve of genus $2^m - 1$ over a perfect field k of characteristic 2, for some integer $m \geq 2$. If the Jacobian of C has no k-rational point of order 2, then it has 2-rank zero, but it is not supersingular.*

Finally, for integers $g, r \geq 1$, let $c_{g,r}$ be the proportion of equations (8) over $\mathbf{F}_{2^r}$ that define a curve of genus g whose Jacobian has at least one rational point of order 2.

Corollary 27. *The limit* $\lim_{r\to\infty} c_{g,r}$ *exists and we have*

$$\lim_{r\to\infty} c_{g,r} = \begin{cases} 1 & \textit{if } g \textit{ is odd,} \\ g/(g+1) & \textit{if } g \textit{ is even.} \end{cases}$$

Proof of Theorem 23. All we need to do is describe the two-torsion of the Jacobian $\mathrm{Jac}(C)$ of C. Since we were not able to find a ready-to-use statement in the literature, we give a stand-alone treatment, even though what follows is undoubtedly known to several experts in the field; for instance, it is implicitly contained in [EP, PZ]. Let $\overline{k}$ be an algebraic closure of k. Note that C has a unique point $Q_{(a:b)} = (a : \sqrt{F(a,b)} : b) \in C(\overline{k})$ for every root $(a:b) \in \mathbf{P}^1_{\overline{k}}$ of $H_1 = H_1(X,Z)$. This gives n points, where $n \in \{1,\ldots,g+1\}$ is the number of distinct roots of H_1. Let D be the divisor of zeroes of a vertical line, so D is effective of degree 2. All such divisors D are linearly equivalent, and are linearly equivalent to $2Q_{(a:b)}$ for each $(a:b)$. In particular, if we let

$$A = \ker\left(\bigoplus_{(a:b)}(\mathbf{Z}/2\mathbf{Z}) \xrightarrow{\Sigma} (\mathbf{Z}/2\mathbf{Z})\right),$$

then we have a homomorphism

$$\begin{array}{ccc} A & \longrightarrow & \mathrm{Jac}(C)(\overline{k})[2] \\ (c_{(a:b)} \bmod 2)_{(a:b)} & \longmapsto & (\sum_{(a:b)} c_{(a:b)} Q_{(a:b)}) - (\frac{1}{2}\sum_{(a:b)} c_{(a:b)})D. \end{array}$$

In fact, this map is an isomorphism. Indeed, it is injective because if the divisor of a function is invariant under the hyperelliptic involution, then so is the function itself, i.e. it is contained in $\overline{k}(x)$. But at the points $Q_{(a:b)}$ such functions can only admit poles or zeroes having an even order. Surjectivity follows from the fact that $\mathrm{Jac}(C)(\overline{k})[2]$ is generated by divisors that are supported on the Weierstrass locus of C. This can be seen using Cantor's algorithm [Kob, Appendix.§6-7], for the application of which one needs to transform the curve to a so-called imaginary model; this is always possible over $\overline{k}$. Alternatively, surjectivity follows from the injectivity and the fact that $\#\mathrm{Jac}(C)(\overline{k})[2] = 2^{n-1}$ by [EP, Thm. 1.3].

Then in particular, the rational 2-torsion subgroup $\mathrm{Jac}(C)(k)[2]$ is isomorphic to the subgroup of elements of A that are invariant under $\mathrm{Gal}(\overline{k}/k)$, that is, to

$$A_k = \ker\left(\bigoplus_{P|H_1}(\mathbf{Z}/2\mathbf{Z}) \to (\mathbf{Z}/2\mathbf{Z}) : (c_P)_P \mapsto \sum_P c_P \deg(P)\right)$$

where the sum is taken over the irreducible factors P of H_1.

The only way for A_k to be trivial is for H_1 to be the power of an irreducible factor P of odd degree. □

Proof of Corollary 24. Let n be the degree of the radical R of H_1. The 2-rank of C equals $n-1$ (as in the proof of Theorem 23; see e.g. [EP, Thm. 1.3]). So if the 2-rank is odd, then R has even degree, which implies that H_1 is not a power of an irreducible odd-degree polynomial. In particular, Theorem 23 implies that C has a non-trivial k-rational 2-torsion point. $\square$

Proof of Corollary 25. This is a special case of Corollary 24 since in characteristic 2, the 2-rank of an ordinary abelian variety equals its dimension. $\square$

Proof of Corollary 26. If there is no rational point of order 2, then H_1 is a power of a polynomial of odd degree dividing $\deg H_1 = g + 1 = 2^m$. In other words, it is a power of a linear polynomial and hence the 2 rank of C is zero. There are no supersingular hyperelliptic curves of genus $2^m - 1$ in characteristic 2 by [SZ, Thm. 1.2]. $\square$

Proof of Corollary 27. As $r \to \infty$, the proportion of equations (8) for which H_1 is not separable becomes negligible. By Theorem 23 it therefore suffices to prove the corresponding limit for the proportion of degree $g + 1$ polynomials that are *not* irreducible of odd degree. If g is odd then this proportion is clearly 1. If g is even then this is the same as the proportion of reducible polynomials of degree $g + 1$, which converges to $1 - (g + 1)^{-1}$. $\square$

Remark 28. In Corollary 27, instead of working with the proportion of equations (8), we can work with the corresponding proportion of $\mathbf{F}_{2^r}$-isomorphism classes of hyperelliptic curves of genus g. This is because the subset of equations (8) that define a hyperelliptic curve of genus g whose only non-trivial geometric automorphism is the hyperelliptic involution (inside the affine space of all equations of this form) is non-empty [Poo1], open, and defined over $\mathbf{F}_2$ (being invariant under the $\mathrm{Gal}(\overline{\mathbf{F}}_2, \mathbf{F}_2)$-action). See also [Zhu].

We finish by identifying the 2-torsion point from the proof of Theorem 2 in the hyperelliptic case with one of the 2-torsion points from the proof of Theorem 23. The former proof provides Θ_{arith} and Θ_{geom} with $2\Theta_{\mathrm{arith}} \sim 2\Theta_{\mathrm{geom}}$, hence the class of $T = \Theta_{\mathrm{arith}} - \Theta_{\mathrm{geom}}$ is two-torsion. We have $2\Theta_{\mathrm{arith}} = \operatorname{div} dx$. To compute $2\Theta_{\mathrm{geom}}$, we need to take an appropriate model as in the proof of Lemma 1. The bivariate polynomial $y^2 + H_1(x, 1)y + H_0(x, 1)$ gives an affine model of our hyperelliptic curve C, and if g is odd, then the system from Lemma 1 admits the solution $(1, 1)$. By the proof of that lemma, we should then look at the toric model C'_f where

$$f = x^{-1}(y + H_1(x, 1) + y^{-1}H_0(x, 1)).$$

Then Θ_{geom} is given by $2\Theta_{\mathrm{geom}} = \operatorname{div} \frac{1}{xy\frac{\partial f}{\partial y}} dx$, so we compute

$$\frac{\partial f}{\partial y} = x^{-1}(1 + y^{-2}H_0(x, 1)) = x^{-1}y^{-1}\ H_1(x, 1).$$

We find

$$T = \Theta_{\mathrm{arith}} - \Theta_{\mathrm{geom}} = \frac{1}{2}\operatorname{div} xy\frac{\partial f}{\partial y} = \frac{1}{2}\operatorname{div} H_1(x, 1),$$

where $\operatorname{div} H_1(x, 1)$ is twice the sum of all points $P_{(a:b)}$ as $(a : b)$ ranges over the roots of $H_1(X, Z)$ in $\mathbf{P}^1_k$ (with multiplicity), minus $(g + 1)$ times the divisor D of degree 2 at infinity. This is the 2-torsion point from the proof of Theorem 23 corresponding to the element $(1, 1, \ldots, 1) \in A_k$.

Acknowledgements

We sincerely thank Christophe Ritzenthaler, Arne Smeets and the anonymous referees for several helpful comments. The first author was supported financially by FWO-Vlaanderen.

References

[BCP] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, pp. 235265 (1997)

[CEZB] B. Cais, J. Ellenberg, D. Zureick-Brown, *Random Dieudonné modules, random p-divisible groups, and random curves over finite fields*, to appear in J. Math. Inst. Jussieu

[Cas] W. Castryck, *Moving out the edges of a lattice polygon*, Discrete and Computational Geometry **47**(3), pp. 496-518 (2012)

[CC] W. Castryck, F. Cools, *Linear pencils encoded in the Newton polygon*, preprint

[CDV] W. Castryck, J. Denef, F. Vercauteren, *Computing zeta functions of nondegenerate curves*, Int. Math. Res. Pap. **2006**, pp. 1-57 (2006)

[CFHS] W. Castryck, A. Folsom, H. Hubrechts, A.V. Sutherland, *The probability that the number of points on the Jacobian of a genus* 2 *curve is prime*, Proc. London Math. Soc. **104**(6), pp. 1235-1270 (2012)

[CV] W. Castryck, J. Voight, *On nondegeneracy of curves*, Algebra & Number Theory **3**(3), pp. 255-281 (2009)

[CLS] D. Cox, J. Little, H. Schenck, *Toric varieties*, Graduate Studies in Mathematics **124** (2011)

[DV1] J. Denef, F. Vercauteren, *Computing zeta functions of hyperelliptic curves over finite fields of characteristic* 2, Proc. of 'Advances in Cryptology – CRYPTO 2002', Lect. Not. Comp. Sc. **2442**, pp. 308-323 (2002)

[DV2] J. Denef, F. Vercauteren, *Computing zeta functions of $C_{a,b}$ curves using Monsky-Washnitzer cohomology*, Fin. Fields App. **12**(1), pp. 78-102 (2006)

[EP] A. Elkin, R. Pries, *Ekedahl-Oort strata of hyperelliptic curves in characteristic* 2, Algebra & Number Theory **7**(3), pp. 507-532 (2013)

[FP] S. Farnell, R. Pries, *Families of Artin-Schreier curves with Cartier-Manin matrix of constant rank*, Linear Algebra and its Applications **439**(7), pp. 2158-2166 (2013)

[HS] C. Haase, J. Schicho, *Lattice polygons and the number* $2i + 7$, American Mathematical Monthly **116**(2), pp. 151-165 (2009)

[Har] R. Hartshorne, *Generalized divisors on Gorenstein curves and a theorem of Noether*, J. Math. Kyoto Univ. **26**(3), pp. 375-386 (1986)

[KS] N. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society (1999)

[Kob] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics **3**, Springer (1999)

[Koe] R. Koelman, *The number of moduli of families of curves on toric surfaces*, Ph.D. thesis, Katholieke Universiteit Nijmegen (1991)

[Man] Y. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Translations, Series 2 **45**, pp. 245264 (1965) (originally in Izv. Akad. Nauk SSSR Ser. Mat. **25**, pp. 153-172 (1961))

[Mum] D. Mumford, *Theta characteristics of an algebraic curve*, Ann. Sci. de l'É.N.S. **4**(2), pp. 181-192 (1971)

[Poo1] B. Poonen, *Varieties without extra automorphisms. II. Hyperelliptic curves*, Math. Res. Lett. **7** (1), pp. 77-82 (2000)

[Poo2] B. Poonen, *Bertini theorems over finite fields*, Ann. Math. **160**, pp. 1099-1127 (2004)

[PZ] R. Pries, H. Zhu, *The p-rank stratification of Artin-Schreier curves*, Annales de l'Institut Fourier **62**(2), pp. 707-726 (2012)

[Ser] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique* p, Oeuvres (collected papers) **1**, Springer, pp. 544-568 (1986)
[SZ] J. Scholten, H. Zhu, *Hyperelliptic curves in characteristic* 2, Int. Math. Res. Not. **2002**(17), pp. 905-917 (2002)
[SV] K.-O. Stöhr, J. F. Voloch, *A formula for the Cartier operator on plane algebraic curves*, Journal für die reine und angewandte Mathematik **377**, pp. 49-64 (1987)
[Zhu] H. Zhu, *Hyperelliptic curves over* $\mathbf{F}_2$ *of every* 2*-rank without extra automorphisms*, Proc. Amer. Math. Soc. **134**(2), 323-331 (2006)

wouter.castryck@wis.kuleuven.be.
Departement Wiskunde, KU Leuven, Celestijnenlaan 200B, 3001 Leuven, Belgium.

marco.streng@gmail.com.
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

d.testa@warwick.ac.uk.
Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom.