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, almost all smooth plane projective curves of a given odd degree admit a non-trivial rational 2-torsion point on their Jacobian. We extend this observation to curves given by Laurent polynomials with a fixed Newton polygon, provided that the polygon satisfies a certain combinatorial property. This includes many classical families, such as hyperelliptic curves of odd genus and $C_{a,b}$ curves. In the hyperelliptic case, we give an alternative proof using an explicit description of the 2-torsion subgroup.

1. Introduction

The starting point of this note 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 $\Theta_{\text{geom}}$: 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 $\Theta_{\text{arith}}$ (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 generically 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
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 $\Delta$ 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

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

admits a solution in $\mathbb{Z}^2$. Then any sufficiently general Laurent polynomial $f \in k[x^{\pm 1}, y^{\pm 1}]$ that is supported on $\Delta$ 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 $\Delta$ be a lattice polygon satisfying the conditions of Lemma 1, where in addition we assume that $\Delta$ is not unimodularly equivalent to

$$\begin{cases} (3, 1) \\ 1 \\ 0 \\ for \ some \ k \geq 1 \end{cases} \quad or \quad \begin{cases} (k, 2) \\ (\ell, 1) \\ 1 \\ 0 \\ for \ some \ 0 \leq k < \ell \geq 3 \ with \ k \ even \ and \ \ell \ odd. \end{cases}$$

Then there exists a non-empty Zariski open subset $S_\Delta/F_2$ of the space of Laurent polynomials that are supported on $\Delta$ 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 $S_\Delta$ explicitly. As a consequence, if $k$ is a finite field of characteristic 2, then the proportion of Laurent polynomials that are supported on $\Delta$, 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 $\Delta$, i.e. the analogue of $d \to \infty$ in the smooth plane curve case.)

This observation seems new even for hyperelliptic curves of odd genus. In this case we can give an alternative proof yielding sufficient conditions having a more arithmetic flavor (such as being ordinary); see Section 4. Another interesting class of examples is given by the polygons

$$\begin{cases} b \\ 0 \\ a \end{cases}$$

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

---

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

---

2.
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 \(g_2^1 \sim 2P\), so there is indeed always a \(k\)-rational half-canonical divisor, regardless of the parity of \(g\).

Finally, the case \(b = 3, a \geq 4\) corresponds to trigonal curves having maximal Maroni invariant (that is trigonal curves for which the series \((h^0(ng_3^1))_{n \in \mathbb{Z}_{\geq 0}}\) 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 \(g_3^1\).

**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].

### 2. Half-canonical divisors from toric geometry

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

\[ \Delta(f) = \conv \{ (i, j) \in \mathbb{Z}^2 \mid c_{i,j} \neq 0 \} \]

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

\[ f_\tau = \frac{\partial f_\tau}{\partial x} = \frac{\partial f_\tau}{\partial y} = 0 \quad \text{with} \quad f_\tau = \sum_{(i,j) \in \tau \cap \mathbb{Z}^2} c_{i,j}x^iy^j \]

has no solutions over an algebraic closure of \(k\). For a given Newton polygon \(\Delta = \Delta(f)\), the condition of non-degeneracy is generically satisfied, in the sense that it is characterized by the non-vanishing of

\[ \rho_\Delta := \Res_\Delta \left( f, x \frac{\partial f}{\partial x}, y \frac{\partial f}{\partial y} \right) \in \mathbb{Z}[c_{i,j}](i, j) \in \Delta \cap \mathbb{Z}^2 \]

(where \(\Res_\Delta\) is the sparse resultant; \(\rho_\Delta\) does not vanish identically in any characteristic [CV, §2]).

Let \(C_f\) be the curve in \(\mathbb{T}_k^2 = \Spec k[x^{\pm 1}, y^{\pm 1}]\) cut out by \(f\) and let \(\Tor_k(\Delta(f))\) be the toric surface corresponding to \(\Delta(f)\); it is a compactification of \(\mathbb{T}_k^2\) to which the self-action of \(\mathbb{T}_k^2\) extends algebraically. There is a natural dimension-preserving bijection between the orbits of this extended action and the faces of \(\Delta(f)\); for each face \(\tau\), write \(O(\tau)\) for the corresponding orbit. Then geometrically, the condition of non-degeneracy means that \(C_f\) is a non-singular curve in \(\mathbb{T}_k^2 = O(\Delta(f))\) compactifying to a curve \(C'_f\) in \(\Tor_k(\Delta(f))\) that does not contain any of the zero-dimensional \(O(\tau)\)’s and that intersects the one-dimensional \(O(\tau)\)’s transversally.
In particular, since $\text{Tor}_k(\Delta(f))$ is normal, non-degeneracy implies that $C'_f$ is a non-singular complete model of $C_f$. See [CDV, §2] for a more detailed description of this construction.

**Example 4.** Assume that $\Delta(f) = \text{conv}\{(0,0), (d,0), (0,d)\}$, i.e. $f$ is a degree-$d$ polynomial with non-zero coefficients at $1, x^d, y^d$. In this case $\text{Tor}_k(\Delta(f))$ is just the projective plane, and the toric orbits are $\mathbb{T}^2 = O(\Delta(f))$, the three coordinate points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ (which are the orbits of the form $O(\text{vertex})$), and the three coordinate axes from which the coordinate points are removed (these are the orbits of the form $O(\text{edge})$). Then $f$ is non-degenerate with respect to its Newton polygon if and only if $C_f$ compactifies to 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.

**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 $\mathbb{P}_k(1 : g + 1 : 1)$. Here again, $f$ is non-degenerate with respect to its Newton polygon if and only if $C'_f$ is a non-singular curve that is non-tangent to the coordinate axes and 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 $\tau \subset \Delta(f)$ let $\nu_\tau \in \mathbb{Z}^2$ be the inward pointing primitive normal vector to $\tau$, let $p_\tau$ be any element of $\tau \cap \mathbb{Z}^2$, and let $D_\tau$ be the $k$-rational divisor on $C'_f$ cut out by $O(\tau)$. If $f$ is non-degenerate with respect to its Newton polygon, then one can show

\[
\text{div} \frac{dx}{xy \frac{df}{dy}} = \sum_{\tau \text{ edge}} (-\langle \nu_\tau, p_\tau \rangle - 1) D_\tau.
\]

Here $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^2$. See [CDV, Cor. 3] for an elementary but elaborate proof of (2). It is possible to give a more conceptual proof using adjunction theory.

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

\[
\text{div} \frac{dy}{xy \frac{df}{dx}},
\]
Proof of Lemma 1. Assume that \( f \) is such that \( \Delta(f) = \Delta \) and that it is non-degenerate with respect to its Newton polygon (which, as mentioned above, is a non-empty Zariski open condition). Let \((i_0, j_0) \in \mathbb{Z}^2\) be a solution to the given system of congruences. Then the translated polygon \((-i_0, -j_0) + \Delta\) is such that all corresponding \((\nu_\tau, p_\tau)\)'s are odd. So by applying the above to \(x^{i_0}y^{j_0}f\), we find that
\[
\sum_{\tau \text{ edge}} -\frac{\langle \nu_\tau, p_\tau \rangle - 1}{2} D_\tau
\]
is a \(k\)-rational half-canonical divisor on \(C'_x - i_0y - j_0f = C'_f\). \(\square\)

Remark 7. Let \( \Delta = \text{conv}\{(0,0), (d,0), (0,d)\} \) with \(d\) odd. Then 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\(^2\) In general, the according weaker condition reads that \(C_f\) compactifies to a non-singular curve in \(\text{Tor}_k(\Delta)\). Here we have to revisit Remark 6 however: there do exist instances of absolutely irreducible Laurent polynomials \(f \in k[x^\pm 1, y^\pm 1]\) for which \(C_f\) compactifies to a non-singular curve in \(\text{Tor}_k(\Delta(f))\), yet for which \(\partial f/\partial y\) does vanish identically (example: \(f = 1 + x^2y^2 + x^3y^2\)). For these instances of \(f\) 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 non-degenerate Laurent polynomials, that can be seen as consequences to (2); see for instance [CV] and the references therein:

- the geometric genus of \(C_f\) equals \#(\(\Delta(f)^c \cap \mathbb{Z}^2\)), where \(\Delta(f)^c\) denotes the interior of \(\Delta(f)\), and
- in case \#(\(\Delta(f)^c \cap \mathbb{Z}^2\)) \(\geq 2\), \(C_f\) is hyperelliptic if and only if \(\Delta(f)^c \cap \mathbb{Z}^2\) is contained in a line.

3. Proof of the main result

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

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

\(^2\)The reader might want to note that there always exists an automorphism of \( \mathbb{P}^2_k \) that puts our smooth plane curve in a non-degenerate position (at least if \#k is sufficiently large). But for more general instances of \( \Delta \), the automorphism group of \( \text{Tor}_k(\Delta) \) may be much smaller (e.g. the only automorphisms may be the ones coming from the \( T^2_k \)-action), in which case it might be impossible to resolve tangency to the one-dimensional toric orbits.
(up to unimodular equivalence). This assertion follows from Koelman’s classification; see [Koe, Ch. 4] or [Cas, Thm. 10]. As a consequence, any two-dimensional $\Delta$ for which $\pi_\Delta$ is not surjective must contain one of the polygons (a-d) as an ‘onion skin’, i.e. as a lattice polygon obtained by subsequently taking the convex hull of the interior lattice points. But using the criterion from [HS, Lem. 9-11] one sees that the only polygons in (a-d) that can appear as convex hull of the interior lattice points of a strictly bigger lattice polygon $\Gamma$ are the polygons (a) with $k = 1$ or $k = 2$, the polygon (b) and the polygon (c). The only corresponding instance of $\Gamma$ for which $\pi_\Gamma$ is not surjective is

\[
\begin{pmatrix}
-1, 2 \\
0, -1
\end{pmatrix}
\]

which, again by [HS, Lem. 9-11], is an onion skin only of itself. This ends the classification.

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

- $\Delta(f) = \Delta$ and $f$ is non-degenerate with respect to its Newton polygon (i.e. the genericity assumption from Lemma [11]), and
- for at least one solution $(i_0, j_0) \in \Delta \cap \mathbb{Z}^2$ to the system of congruences (1), the corresponding coefficient $c_{i_0,j_0}$ is non-zero.

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

**Remark 11.** Here again, one can weaken the non-degeneracy condition as described in Remark [4]. When that stronger version is applied to $\Delta = \text{conv}\{(0, 0), (d, 0), (0, d)\}$ 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 $\Theta_{\arithmetic}$ such that $2\Theta_{\arithmetic} = \text{div} \, dx$. (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 $\Theta_{\text{geom}}$ such that

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

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

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

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 $\alpha, G, H$ such that

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

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 $f | (\alpha + H^2 x)$ or $f | G^2$. Using (1) 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 $f \nmid (\alpha + H^2 x)$. 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.  

We end this section by discussing some asymptotic consequences to Theorem 2.
Growing field size. Let $\Delta$ 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 $\rho_\Delta$, the proportion of Laurent polynomials $f \in k[x^{\pm 1}, y^{\pm 1}]$ that are non-degenerate with respect to their Newton polygon $\Delta(f) = \Delta$ (amongst all Laurent polynomials that are supported on $\Delta$) converges to 1 as $\#k \to \infty$. Then Theorem 2 implies:

$$\lim_{\#k \to \infty} \text{Prob}(\text{Jac}(C'_f)(k)[2] \neq 0 \mid f \in k[x^{\pm 1}, y^{\pm 1}] \text{ is non-degenerate with respect to its Newton polygon } \Delta(f) = \Delta) = 1.$$ 

As soon as $\#(\Delta^\circ \cap \mathbb{Z}^2) \geq 2$ 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 $\text{GL}_g(F_2)$ 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 $1, \frac{2}{5}, \frac{5}{7}, \frac{32}{45}, \ldots$ (converging to about 0.71121).

In the table below we denote by $\Box_i$ 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 $\Box_2, \Box_3, \ldots$ 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 $\Delta(f) = \Box_2, \Box_3, \ldots$. An entry ‘-’ means that we did not do the computation because it would take too long. The computations were carried out using Magma [BCP].

| $k$ | $\Box_2$ $(g = 1)$ | $\Box_3$ $(g = 4)$ | $\Box_4$ $(g = 9)$ | $H_7$ $(g = 7)$ | $H_8$ $(g = 8)$ | $E$ $(g = 3)$ |
|-----|-----------------|-----------------|-----------------|----------------|----------------|-------------|
| $\mathbb{F}_2$ | 0/0 | 0.370 | 0.958 | 0.995 | 0.670 | 0.143 |
| $\mathbb{F}_4$ | 0.750 | 0.621 | 1.000 | 1.000 | 0.795 | 0.449 |
| $\mathbb{F}_8$ | 0.884 | 0.654 | 1.000 | 1.000 | 0.852 | 0.591 |
| $\mathbb{F}_{16}$ | 0.940 | 0.697 | 1.000 | 1.000 | 0.872 | 0.661 |
| $\mathbb{F}_{32}$ | 0.968 | 0.704 | 1.000 | 1.000 | 0.877 | 0.696 |
| $\mathbb{F}_{64}$ | 0.986 | - | 1.000 | 1.000 | 0.880 | 0.694 |
| $\mathbb{F}_{128}$ | 0.992 | - | 1.000 | 1.000 | 0.889 | 0.708 |
| $\mathbb{F}_{256}$ | 0.996 | - | 1.000 | 1.000 | 0.888 | - |
| asymptotic prediction | 1 | 0.7111 $\approx 0.711$ | 1 | 1 | $\frac{5}{7} \approx 0.714$ | $\frac{5}{7} \approx 0.714$ |

Note that the conditions of Theorem 2 are satisfied for $\Box_2$, $\Box_4$ and $H_7$. So here we proved that the proportion converges to 1. In the case of $H_8$, by the material in Section 4 we have the following asymptotic prediction:
Corollary [16] we know that the proportion converges to \( \frac{8}{9} \). In the other two cases \( \Box_4 \) and \( E \) we have no clue, so our best guess is that these follow the \( \text{GL}_9(F_2) \)-model.

**Growing polygon.** Let \( k \) be a finite field of characteristic 2. If \( \Delta \) 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 Laurent polynomials \( f \in k[x^{\pm 1}, y^{\pm 1}] \) that are non-degenerate with respect to their Newton polygon \( \Delta(f) = (2n+1)\Delta \) (amongst all Laurent polynomials that are supported on \((2n+1)\Delta\)) converges to a certain strictly positive constant.

If \( \text{Tor}_k(\Delta) \) is smooth then this is certainly true for the larger proportion of Laurent polynomials \( f \) satisfying the weaker condition from Remark 7, namely that \( C_f \) compactifies to a non-singular curve in \( \text{Tor}_k((2n+1)\Delta) \). Indeed, using [Poo2, Thm. 1.1] one can show that this proportion converges to

\[
Z_{\text{Tor}_k(\Delta)}((\#k)^{-3})^{-1} = (1 - (\#k)^{-1})(1 - (\#k)^{-2})^{r(\Delta)-2}(1 - (\#k)^{-3})
\]

as \( n \to \infty \); here \( Z_{\text{Tor}_k(\Delta)} \) is the Hasse-Weil Zeta function of \( \text{Tor}_k(\Delta) \), and \( r(\Delta) \) is the number of vertices of \( \Delta \).

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

\[
\lim_{n \to \infty} \text{Prob} \left( \text{Jac}(C_f)(k)[2] \neq 0 \mid f \in k[x^{\pm 1}, y^{\pm 1}] \text{ is non-degenerate with respect to its Newton polygon } \Delta(f) = (2n+1)\Delta \right) = 1.
\]

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 \( \Delta = \text{conv}\{ (0,0), (1,0), (0,1) \} \) one recovers the claim made before [CEZB, Thm. 4.2] (taking into account Remark 7).

### 4. Hyperelliptic curves of odd genus

Let \( C \) be a hyperelliptic curve of genus \( g \) over a perfect field \( k \). Then \( C \) has a smooth weighted projective plane model

\[
C : \quad Y^2 + H(X,Z)Y = F(X,Z),
\]

where \( H \) and \( F \) in \( k[X,Z] \) are homogeneous of degrees \( g + 1 \) and \( 2g + 2 \) respectively. The Newton polygon of (the defining polynomial of) the corresponding affine model \( y^2 + H(x,1)y - F(x,1) = 0 \) 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.

The purpose of this section is to show that we can replace ‘sufficiently general’ by ‘ordinary’ in this case (Corollary 14), and to give explicit examples of the rational half-canonical divisors from the proof of Theorem 2.
Theorem 12. Let $C/k$ be a hyperelliptic curve over a perfect field $k$ of characteristic 2 given by a smooth model $(5)$. The Jacobian of $C$ has no rational point of order 2 if and only if $H(X, Z)$ is a power of an irreducible odd-degree polynomial in $k[X, Z]$.

Corollary 13. 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 14. 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 15. 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 $(5)$ over $\mathbb{F}_2$ that define a curve of genus $g$ whose Jacobian has at least one rational point of order 2.

Corollary 16. The limit $\lim_{r \to \infty} c_{g,r}$ exists and we have

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

Proof of Theorem 12. All we need to do is describe the two-torsion of the Jacobian $\text{Jac}(C)$ 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]. 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 $(a : b) \in \mathbb{P}_k^1$ of $H = H(X, Z)$. This gives $n$ points, where $n \in \{1, \ldots, g+1\}$ is the number of distinct roots of $H$. 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

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

then we have a homomorphism

$$
A \quad \longrightarrow \quad \text{Jac}(C)(\overline{k})[2]
$$

$$
(c_{(a:b)} \mod 2)_{(a:b)} \quad \longmapsto \quad \left( \sum_{(a:b)} c_{(a:b)} Q_{(a:b)} \right) - \left( \frac{1}{2} \sum_{(a:b)} c_{(a:b)} D \right).
$$

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 $\text{Jac}(C)(\overline{k})[2]$ 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 \#Jac(C)(\overline{k})[2] = 2^{n-1} by \[EP\], Thm. 1.3.

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

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

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

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

**Proof of Corollary 13.** Let n be the degree of the radical R of H. The 2-rank of C equals n − 1 (as in the proof of Theorem 12 see e.g. \[EP\], Thm. 1.3). So if the 2-rank is odd, then R has even degree, which implies that H is not a power of an odd-degree polynomial. In particular, Theorem 12 implies that C has a non-trivial k-rational 2-torsion point.

**Proof of Corollary 14.** This is a special case of Corollary 13 since in characteristic 2, the 2-rank of an ordinary abelian variety equals its dimension.

**Proof of Corollary 15.** If there is no rational point of order 2, then H is a power of a polynomial of odd degree dividing \deg(H) = 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.

**Proof of Corollary 16.** As \(r \to \infty\), the proportion of equations (5) for which H is not separable becomes negligible. By Theorem 12 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}.

**Remark 17.** In Corollary 16 instead of working with the proportion of equations (5), we can work with the corresponding proportion of \(\mathbb{F}_2\)-isomorphism classes of hyperelliptic curves of genus g. This is because the subset of equations (5) 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 \(\mathbb{F}_2\) (being invariant under the \text{Gal}(\mathbb{F}_2, \mathbb{F}_2)-action). See also \[Zhu\].

Theorem 2 proves Corollary 14 for sufficiently general curves. We finish by showing that the 2-torsion points from both proofs are equal. The proof of Theorem 2 provides \(\Theta_{\text{arith}} \) and \(\Theta_{\text{geom}} \) with \(2\Theta_{\text{arith}} \sim 2\Theta_{\text{geom}} \), hence the class of \(T = \Theta_{\text{arith}} - \Theta_{\text{geom}} \) is two-torsion. We have \(2\Theta_{\text{arith}} = \text{div} dx \). To compute \(2\Theta_{\text{geom}} \), we need to take an appropriate model as in the proof of Lemma 1. The bivariate polynomial \(y^2 + H(x, 1)y + F(x, 1) \) 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

\[ f = x^{-1}(y + H(x, 1) + y^{-1}F(x, 1)). \]
Then $\Theta_{\text{geom}}$ is given by $2\Theta_{\text{geom}} = \text{div} \frac{1}{xy} \, dx$, so we compute

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

We find

$$T = \Theta_{\text{arith}} - \Theta_{\text{geom}} = \frac{1}{2} \text{div} \frac{f}{y} = \frac{1}{2} \text{div} H(x, 1),$$

where $\text{div} H(x, 1)$ is twice the sum of all points $P_{(a:b)}$ as $(a:b)$ ranges over the roots of $H(X, Z)$ in $\mathbb{P}^1_k$ (with multiplicity), minus $(g + 1)$ times the divisor $D$ of degree 2 at infinity. So both proofs give the same 2-torsion point in cases where they both apply.

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)

[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)

[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, to appear in Algebra & Number Theory

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

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

[Kob] N. Kobitz, 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)

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

[Poo] 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)

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

[Zhu] H. Zhu, Hyperelliptic curves over $\mathbb{F}_2$ of every 2-rank without extra automorphisms, Proc. Amer. Math. Soc. 134(2), 323-331 (2006)
E-mail: wouter.castryck@wis.kuleuven.be.
Address: Departement Wiskunde, KU Leuven, Celestijnenlaan 200B, 3001 Leuven, Belgium.

E-mail: marco.streng@gmail.com.
Address: Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

E-mail: d.testa@warwick.ac.uk.
Address: Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom.