ADDENDA AND ERRATA: *ON NONDEGENERACY OF CURVES*

WOUTER CASTRYCK AND JOHN VOIGHT

This note gives some addenda and errata for the article *On nondegeneracy of curves* [6].

Errata

(1) Beginning of Section 5: We write that every genus g hyperelliptic curve over a perfect field k is birationally equivalent (over k) to a curve of the form
$$y^2 + q(x)y = p(x)$$
where $p(x), q(x) \in k[x]$ satisfy $2 \deg q(x) \leq \deg p(x)$ and $\deg p(x) \in \{2g+1, 2g+2\}$. This is false for (and only for) $k = \mathbb{F}_2$.

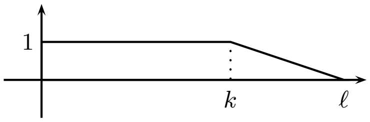
Namely, this will fail for any hyperelliptic curve C over $k = \mathbb{F}_2$ for which the degree 2 morphism $\pi : C \to \mathbb{P}^1$ splits completely over k, meaning that above each point $0, 1, \infty \in \mathbb{P}^1(k)$ there are two distinct k-rational points of C. For any other perfect field, the statement is true. This is easily deduced from a result of Enge [7, Theorem 7].

In particular, since we assume $\#k \geq 17$ in this context anyway, this erratum has no effect on any further statement.

(2) Section 6 (Curve of genus 4, hyperboloidal case),"Then $Q \cong \mathbb{P}^2_k \times \mathbb{P}^2_k$ and V can be projected": Should be "Then $Q \cong \mathbb{P}^1_k \times \mathbb{P}^1_k$".

(3) Proof of Lemma 10.5, "The dual loop $\mathcal{P}^\vee$ walks through the normal vectors of $\Delta^{(1)}$": In fact it walks through the *direction vectors of the edges* of $\Delta^{(1)}$. The same conclusion follows.

(4) Poof of Theorem 12.1, "More generally, let $k, \ell \in \mathbb{Z}_{\geq 2}$ satisfy $k \leq \ell$, let $\Delta^{(1)}$ be the trapezium



and let $\Delta = \Delta^{(1)(-1)}$": We overlooked that $\Delta^{(1)(-1)}$ need not be a lattice polygon: it may take some of its vertices outside $\mathbb{Z}^2$. This does not cause problems because this paragraph is only applied to the cases $k = \ell$ and $k = \ell - 1$, corresponding to (9) and (10), respectively. For these values of k and ℓ the polygon $\Delta^{(1)(-1)}$ *does* take its vertices in $\mathbb{Z}^2$.

In fact, using the combinatorial criterion from Lemma 10.2, one can verify that $\Delta^{(1)(-1)}$ is a lattice polygon if and only if $\ell \leq (2g-2)/3$, where $g = k+\ell+2$. This confirms a well-known inequality on the Maroni invariants

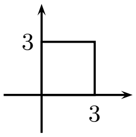
Date: December 5, 2014.

of a trigonal curve (where the inequality is proven using the Riemann-Roch theorem).

Addenda

(1) The bound $\#k \leq 17$ in our main theorem: Concerning nondegenerate curves of low genus over small finite fields, we have since proven [5] that there are exactly two curves of genus at most 3 over a finite field that are *not* nondegenerate, one over $\mathbb{F}_2$ and one over $\mathbb{F}_3$.

(2) Genus 4 hyperboloidal curves: In our summary in Section 7, we state that every curve of genus at most 4 over an algebraically closed field k can be modeled by a nondegenerate polynomial having one of the nine listed figures as Newton polytope. In fact, all genus 4 hyperboloidal curves can be described by a single polytope. Indeed, if $f(x, y)$ has a Newton polytope of type (h.1) or (h.2), then applying a change of variables to $x^3y^3f(x^{-1}, y^{-1})$ of the form $(x, y) \mapsto (x + a, y + b)$ for $a, b \in k$ yields a square 3×3 Newton polytope. So replacing the two polytopes of class (h) by the single polytope



(h) genus 4 hyperboloidal

results in a list that is both more condensed and pleasing.

Below the nine figures, we write "Moreover, these classes are disjoint." In this phrase, "class" refers to one of the (a), . . . , (h), and not necessarily to a single polytope: this might perhaps not be semantically clear. By replacing (h.1) and (h.2) by the above polytope, this ambiguity is removed.

(3) Lemma 5.1, Lemma 9.2: We give a criterion for a Δ-nondegenerate curve of genus $g \geq 2$ to be hyperelliptic, namely, it is hyperelliptic if and only if the interior lattice points of Δ are collinear. Adding a small technical condition, the converse statement of Lemma 9.2 (characterizing trigonal curves) holds as well.

Lemma 9.2. *Let $f \in k[x^{\pm 1}, y^{\pm 1}]$ be nondegenerate and suppose that the interior lattice points of $\Delta(f)$ are not collinear. Let $\Delta^{(1)}$ be the convex hull of these interior lattice points.*

(a) *If $\Delta^{(1)}$ has no interior lattice points, then $V(f)$ is either trigonal or isomorphic to a smooth plane quintic.*

(b) *If $V(f)$ is trigonal or isomorphic to a smooth plane quintic, and $\Delta^{(1)}$ has at least 4 lattice points on the boundary, then $\Delta^{(1)}$ has no interior lattice points.*

Proof. Part (a) is proved in the original paper. For (b), using the canonical divisor K_Δ from Proposition 1.7, one sees that the canonical embedding of $V(f)$ in $\mathbb{P}_k^{g-1}$ is contained in $X(\Delta^{(1)})_k$. According to a theorem of Koelman [11], the condition of having at least 4 lattice points on the boundary ensures that $X(\Delta^{(1)})$ is generated by quadrics. Now since $V(f)$ is trigonal or isomorphic to a smooth plane quintic, by Petri's theorem the intersection of *all* quadrics containing $V(f)$ is a surface of sectional genus 0. Hence this surface must be $X(\Delta^{(1)})_k$ and $\Delta^{(1)}$ must have genus 0. □

The condition that $\Delta^{(1)}$ should have at least 4 lattice points on the boundary is necessary. For example, let k be algebraically closed and let $\Delta = \operatorname{conv}\{(2,0),(0,2),(-2,-2)\}$. Then Δ is a lattice polytope of genus 4, hence all Δ-nondegenerate curves are trigonal. However, $\Delta^{(1)}$ contains $(0,0)$ in its interior. Note that $X(\Delta^{(1)})_k \subset \mathbb{P}^3_k$ is the cubic $xyz = w^3$.

The above lemma has recently been extended to arbitrary gonalities [4, 9].

(4) Dominance in genus 4: Under the assumption $k = \overline{k}$, we proved that every curve of genus 4 is nondegenerate. If k is any perfect field, one can still consider the map

$$\bigsqcup_{g(\Delta)=4} M_\Delta \;\to\; \mathcal{M}_4,$$

but now it will no longer be surjective on k-rational points. Indeed, this follows from our analysis of the conic and hyperboloidal cases. One can refine this analysis as follows and show that every curve of genus 4 over k is *potentially nondegenerate*, i.e., becomes nondegenerate over a finite extension of k: in fact, a quadratic extension of k will do, as long as $\#k$ is large enough.

In the conical case, we have that the k-rational quadric Q has a singular point, and so after a linear change of variable is realized as the cone over a plane conic C. The conic C may have $C(k) = \emptyset$, but after a quadratic extension K of k, we have $C \times_k \overline{K} \cong \mathbb{P}^1_K$, and then the rest of the argument follows, still assuming $\#k \geq 23$. (In a manner similar to the one we used in Addenda (1) above [5], one could determine the set of all conical genus 4 curves that are not nondegenerate.) This argument works even when $\operatorname{char} k = 2$.

In the hyperboloidal case (the general case), the quadric Q is smooth. Standard results in the theory of quadratic forms over fields k with $\operatorname{char} k \neq 2$ imply that Q splits, so that $Q \cong \mathbb{P}^1_k \times \mathbb{P}^1_k$, if and only if $Q(k) \neq \emptyset$ and the discriminant of Q is a square in k: if $Q(k) \neq \emptyset$ then Q splits a hyperbolic plane; by scaling, the orthogonal complement is of the form $x^2 - dy^2$, so if $d \in k^{\times 2}$ then Q splits, and conversely. It follows that any quadric over k splits over an at most quadratic extension. To proceed, we then project V to a plane quintic, which requires $\#k$ to be sufficiently large: one could make this explicit, using the Bertini theorem over finite fields due to Poonen [13] and analyze explicitly the finitely many exceptions. Assuming that V has been so projected (extending k further, if necessary), the rest of the argument holds.

(5) Curves over large fields that are *not* nondegenerate: Our dimension estimates for $\mathcal{M}_g^{\mathrm{nd}}$ imply that a general curve of genus $g \geq 5$ is not nondegenerate. However, how does one prove that a given curve V over k of genus $g \geq 5$ is not nondegenerate? This question was asked to us by David Harvey. Here are a couple of possible approaches.

First, there is gonality: nondegenerate curves have low gonality. (In fact, this gives an easier a priori reason why generic curves of sufficiently large genus cannot be nondegenerate than the one we mentioned in Remark 2.3, unirationality of $\mathcal{M}_g^{\mathrm{nd}}$.) Indeed, the gonality of a Δ-nondegenerate curve is bounded above by the lattice width $\operatorname{lw}(\Delta)$ (typically this bound is sharp;

this is the content of the results mentioned above [4, 9]). An old estimate by Tóth and Makai Jr. [8] shows that

$$\mathrm{lw}(\Delta)^2 \leq \frac{8}{3}\mathrm{Vol}(\Delta).$$

Using Pick's theorem $\mathrm{Vol}(\Delta) = g + r/2 - 1$ and Scott's bound $r \leq 2g + 7$ (for $g \geq 1$), it follows that the gonality of nondegenerate curves is $O(\sqrt{g})$. On the other hand, the generic gonality of a curve of genus g is $\lceil g/2 \rceil + 1$. So, from a sufficiently large lower bound on the gonality of V, this argument can be used to show that V cannot be nondegenerate.

Example. The maximal lattice width of a lattice polygon of genus 7 is 4 (can be verified using a case-by-case analysis [4]). So pentagonal genus 7 curves cannot be nondegenerate.

To give an explicit example, the modular curve $X_1(19)$ is of genus 7. We take a defining equation from Sutherland's tables [15].

```
> QQ := Rationals(); R<x,y> := PolynomialRing(QQ,2);
> X19 := y^5 - (x^2 + 2)*y^4 - (2*x^3 + 2*x^2 + 2*x - 1)*y^3
         + (x^5 + 3*x^4 + 7*x^3 + 6*x^2 + 2*x)*y^2
         - (x^5 + 2*x^4 + 4*x^3 + 3*x^2)*y + x^3 + x^2;
> C := Curve(AffineSpace(QQ,2),X19);
```

Let's prove that it has gonality 5.

```
> m := CanonicalEmbedding(C);
> I := Ideal(Image(m));
> BettiTable(GradedModule(I));
[
    [ 1, 0, 0, 0, 0, 0 ],
    [ 0, 10, 16, 0, 0, 0 ],
    [ 0, 0, 0, 16, 10, 0 ],
    [ 0, 0, 0, 0, 0, 1 ]
]
```

If $X_1(19)$ would have gonality 4 (or less), it would have Clifford index 2 (or less) which according to Green's canonical conjecture (proven for curves of Clifford index at most 2 by Schreyer [14]) would mean that the number of leading zeroes on the third row would be at most 2. This contradiction shows that $X_1(19)$ is not nondegenerate.

Proving lower bounds on the gonality is typically very hard, though. A more practical approach uses the fact that nondegenerate curves have low rank quadrics in their canonical ideal. Assume that V is not hyperelliptic, trigonal, or birational to a smooth plane quintic (cases in which V typically *is* nondegenerate). Then by Petri's theorem the canonical ideal of V is generated by $n = (g-2)(g-3)/2$ quadrics in $\mathbb{P}^{g-1}_k$, say $Q_1, \ldots, Q_n$. To each Q_i one can associate a matrix M_i. The (possibly reducible) hypersurface in $\mathbb{P}^{n-1}_k$ defined by

$$\det(x_1 M_1 + x_2 M_2 + \cdots + x_n M_n) = 0$$

is called the *discriminant hypersurface* $\mathfrak{D}(V)$ of V. The discriminant hypersurface is well-defined up to automorphisms of $\mathbb{P}^{n-1}_k$ and describes the singular quadrics in the canonical ideal. The singular points of $\mathfrak{D}(V)$ correspond to the corank ≥ 2 quadrics. Typically, $\mathfrak{D}(V)$ is smooth.

However, in the nondegenerate case, the discriminant hyper surface $\mathfrak{D}(V)$ is never smooth. Indeed, the canonical ideal contains the defining quadrics of $X(\Delta^{(1)})_k$ (cf. Khovanskii [10, Proposition 1.7]), which are binomials, hence of rank at most 4. This proves the claim (except for $g = 5$, but here a case-by-case analysis shows that there is always a rank 3 binomial, i.e. one of the form $x^2 - yz$). So if one can prove that the discriminant hypersurface is smooth, this shows that V cannot be nondegenerate.

Example. We begin with an intersection of 3 quadrics in projective 4-space.

```
> QQ := Rationals(); S<X,Y,Z,U,W> := PolynomialRing(QQ,5);
> quadrics := [  X*Z - 2*X*W + Y*U + U^2,
>               -X^2 + X*Y + Y^2 - U*W + 2*W^2,
>                X*Y - Y^2 + Z^2 - U^2 + U*W  ];
> C := Scheme(ProjectiveSpace(QQ,4),quadrics);
> IsIrreducible(C); Dimension(C);
true
1
> SingularPoints(C); HasSingularPointsOverExtension(C);
{@ @}
false
```

Since this intersection is a smooth irreducible curve, it must be a canonical genus 5 curve having gonality 4. Now we construct the discriminant curve.

```
> T<x1,x2,x3> := PolynomialRing(QQ,3);
> M1 := Matrix(T,5,5,[ 0, 0, 1, 0,-2,
                       0, 0, 0, 1, 0,
                       1, 0, 0, 0, 0,
                       0, 1, 0, 2, 0,
                      -2, 0, 0, 0, 0 ]);
```

After similarly defining `M2` and `M3`, we can define the discriminant curve:

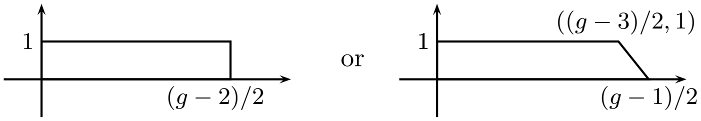
```
> disc := Determinant(x1*M1 + x2*M2 + x3*M3);
> SingularPoints(DC); HasSingularPointsOverExtension(DC);
{@ @}
false
```

Since the discriminant curve is non-singular, our curve cannot be nondegenerate.

(6) Inspired by recent work by Brodsky, Joswig, Morrison and Sturmfels [2], we note that for $g \geq 11$, if Δ is a lattice polygon with g interior lattice points, then Δ attains the upper bound $\dim \mathcal{M}_\Delta = 2g + 1$ if and only if M is trigonal. By Theorem 12.1 and the discussion at the end of [6, §11] it suffices to prove this for maximal polygons. First, suppose that $g^{(1)} > 0$. If $g \geq 14$, then Scott's bound yields $g \leq 3g^{(1)} + 7$ and therefore $g^{(1)} \geq 3$. Since $\dim \mathcal{M}_\Delta \leq 2g + 3 - g^{(1)}$ by Corollary 10.6, we obtain $\dim \mathcal{M}_\Delta < 2g + 1$. On the other hand, if $11 \leq g \leq 13$, then one can exhaustively compute the upper bound $\dim \mathcal{M}_\Delta \leq \#(\Delta \cap \mathbb{Z}^2) - c(\Delta) - 3$ from Corollary 8.4, for all maximal polygons in this range (using a complete enumeration of such polygons [3]), each time verifying that it is strictly smaller than $2g + 1$. To conclude, suppose that $g^{(1)} = 0$ and $g \geq 7$: then the curves under consideration are either hyperelliptic or trigonal by Lemma 5.1 and Lemma

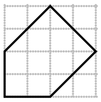
9.2; smooth plane quintics ($g = 6$) are excluded because $g \geq 7$. In the hyperelliptic case, we have $\dim \mathcal{M}_\Delta \leq 2g - 1$. So the remark follows.

Using Koelman's classification of polygons for which $g^{(1)} = 0$, a similar analysis shows that the only maximal polygon attaining the upper bound has interior polygon

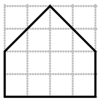


depending on the parity of g. (These are the polygons that we used to prove sharpness of the upper bound $\dim \mathcal{M}_\Delta \leq 2g + 1$.)

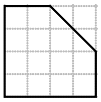
For $g \leq 10$ we can again perform an exhaustive search to list all maximal polygons Δ for which $\mathcal{M}_\Delta \geq 2g+1$. Apart from the above trigonal polygons we find that



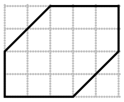
$g = 6, g^{(1)} = 1$



$g = 7, g^{(1)} = 1$



$g = 8, g^{(1)} = 1$



$g = 10, g^{(1)} = 2$

attain dimension $2g + 1$, while in genus 7 we also have our exceptional polygon reaching $2g + 2 = 14$ (trinodal sextics).

References

[1] V. Batyrev and B. Nill, *Multiples of lattice polytopes without interior lattice points*, Mosc. Math. J. **7** (2007), vol. 2, 195–207.

[2] S. Brodsky, M. Joswig, R. Morrison, B. Sturmfels, *Moduli of tropical plane curves*, Research in the Mathematical Sciences, to appear

[3] W. Castryck, *Moving out the edges of a lattice polygon*, Discrete and Computational Geometry **47** (2012), no. 3, 496–518.

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

[5] W. Castryck and J. Voight, *Nondegenerate curves of low genus over small finite fields*, Arithmetic, Geometry, Cryptography and Coding Theory 2009, Contemporary Mathematics **521**, Amer. Math. Soc., Providence, RI, 2010, 21–28.

[6] W. Castryck and J. Voight, *On nondegeneracy of curves*, Algebra & Number Theory **3** (2009), 255–281.

[7] A. Enge, *How to distinguish hyperelliptic curves in even characteristic*, Proceedings of Public-key Cryptography and Computational Number Theory (Warsaw 2000), de Gruyter, Berlin, 2001, 49–58.

[8] L. F. Tóth and E. Makai Jr., *On the thinnest non-separable lattice of convex plates*, Studia Scientiarium Mathematicarum Hungarica **9** (1974), 191–193.

[9] R. Kawaguchi, *The gonality and the Clifford index of curves on a toric surface*, preprint.

[10] A. G. Khovanskiĭ, *Newton polyhedra, and toroidal varieties*, Functional Anal. Appl. **11** (1977), no. 4, 289–296.

[11] R. Koelman, *A criterion for the ideal of a projectively embedded toric surface to be generated by quadrics*, Beiträge zur Algebra und Geometrie **34** (1993), no. 1, 57–62.

[12] R. Koelman, *The number of moduli of families of curves on toric surfaces*, Proefschrift, Katholieke Universiteit te Nijmegen, 1991.

[13] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. **160** (2004), no. 3, 1099–1127.

[14] F.-O. Schreyer, *Syzygies of canonical curves and special linear series*, Math. Ann. **275** (1986), 105–137.

[15] A.V. Sutherland, *Optimized equations for $X_1(N)$ for $N \leq 50$*, available at `http://math.mit.edu/~drew/`