IMPROVED RANK BOUNDS FROM 2-DESCENT ON HYPERELLIPTIC JACOBIANS

BRENDAN CREUTZ

Abstract. We describe a qualitative improvement to the algorithms for performing 2-descents to obtain information regarding the Mordell-Weil rank of a hyperelliptic Jacobian. The improvement has been implemented in the Magma Computational Algebra System and as a result, the rank bounds for hyperelliptic Jacobians are now sharper and have the conjectured parity.

1. Introduction

Suppose X is a smooth projective and geometrically irreducible curve over a global field k. It is an open question whether or not there is an algorithm to compute the set $X(k)$ of rational points on X. A related question is the determination of the group $J(k)$ of rational points on the Jacobian J of X. In the case that X is a hyperelliptic curve and k has characteristic different from 2, the method of 2-descent as described in [2, 4, 7] is sometimes successful in practice. In [5] it is shown how to incorporate additional information coming from a 2-descent on the variety $J^1 = \mathrm{Pic}^1_X$ which is a torsor under J. In particular an algorithm for computing a set denoted $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$ is given and the following result is proven.

Theorem 1.1 ([5, Theorem 4.5 and Corollary 4.6])**.** *Let X be a hyperelliptic curve over a global field of characteristic different from 2. Suppose that X is everywhere locally solvable. Then $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$ is nonempty if and only if the torsor J^1 is divisible by 2 in the Tate-Shafarevich group, $Ш(J/k)$. Moreover, if $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k) = \emptyset$, then $\dim_{\mathbb{F}_2} Ш(J/k)[2] \geq 2$.*

The second statement of the theorem is deduced from the first using the fact that the group $Ш(J/k)[2]/2Ш(J/k)[4]$ has square order, a consequence of the fact that the Cassels-Tate pairing induces a nondegenerate alternating pairing on this quotient because X is everywhere locally soluble and, a fortiori, has divisors of degree 1 everywhere locally [8].

This is useful in determining the Mordell-Weil rank of the Jacobian since there is an exact sequence,

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^2(J/k) \to Ш(J/k)[2] \to 0\,.$$

Thus lower bounds for $Ш(J/k)[2]$ allow one to deduce sharper upper bounds for the rank of $J(k)$. As remarked on [5, p. 305], the hypothesis of Theorem 1.1 that X is everywhere locally solvable seems overly strict; one would expect that the theorem remains true under the weaker hypothesis that X has rational divisors of degree 1 everywhere locally. The purpose of this short note is to show that this is indeed the case. The key new ingredient is part of recent work of Bhargava-Gross-Wang [1] concerning the 2-Selmer set of J^1. Using this we prove the following result.

2010 *Mathematics Subject Classification.* 11G30, 11G10, 11Y50.

Key words and phrases. Curves, Descent, Mordell-Weil Group.

Theorem 1.2. *Let X be a hyperelliptic curve over a global field of characteristic different from 2. Suppose $\mathrm{Div}^1(X_{k_v}) \neq \emptyset$ for all completions v of k. Then $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$ is nonempty if and only if the torsor J^1 is divisible by 2 in $Ш(J/k)$. Moreover, if $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k) = \emptyset$, then $\dim_{\mathbb{F}_2} Ш(J/k)[2] \geq 2$.*

This improvement was motivated in part by a question of Michael Stoll, who noted that the rank bounds for Mordell-Weil groups of hyperelliptic Jacobians over $\mathbb{Q}$ computed by Magma [3] did not always have the parity one would expect assuming standard conjectures. Unlike the usual 2-descent on the Jacobian, computing $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$ and using Theorem 1.1 can indeed lead to bounds which can be improved by assuming parity or finiteness of $Ш(J/k)$. Specifically, if X has divisors of degree 1 everywhere locally and $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k) = \emptyset$, then $J^1(k) = \emptyset$ and J^1 represents a nontrivial element of $Ш(J/k)[2]$. However, if X does not have points everywhere locally Theorem 1.1 does not apply and, without further assumptions, we cannot conclude that $Ш(J/k)[2]/2Ш(J/k)[4]$ is nontrivial. Consequently we only get a lower bound of 1 for $\dim_{\mathbb{F}_2} Ш(J/k)[2]$ instead of 2. If X has divisors of degree 1 everywhere locally and $Ш(J/k)$ contains no non-trivial infinitely 2-divisible elements (as is widely conjectured but far from being proven), then $\dim_{\mathbb{F}_2} Ш(J/k)[2]$ is even [8]. So in such cases the bound obtained does not have the expected parity, but it is the best unconditional result that one can deduce using Theorem 1.1.

In the situation described above Theorem 1.2 applies, allowing us to repair this defect. This improvement has been implemented in Magma and, as a result, the rank bounds for hyperelliptic Jacobians are now sharper and have the expected parity. This has lead to improved rank bounds for 514 of the 66,158 genus 2 curves in the LMFDB [6], leaving a total of 628 curves for which the rank bound exceeds the (conjectural) analytic rank by an even integer.

A particular example is given by the curve [6, Genus 2 Curve 30453.a.30453.1] with model

$$X/\mathbb{Q} : y^2 + (x^3 + x^2 + 1)y = -x^6 + x^4 + 3x^3 + 4x^2 - 11x - 13\,.$$

The 2-Selmer group of the Jacobian is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $J(\mathbb{Q})$ has no points of order 2, from which we deduce that the rank of $J(\mathbb{Q})$ is at most 2. Computing $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/\mathbb{Q})$ as described in [5] we find that it is empty. Since $\mathrm{Div}^1(X_{\mathbb{Q}_p}) \neq \emptyset$ for all primes $p \leq \infty$, this implies that $J^1(\mathbb{Q}) = \emptyset$ and, hence, that J^1 represents a nontrivial element of $Ш(J/\mathbb{Q})[2]$. However, $X(\mathbb{Q}_2) = \emptyset$, so Theorem 1.1 above does not apply. So, without Theorem 1.2, the best unconditional bound for the rank of $J(\mathbb{Q})$ we can get is 1. Whereas Theorem 1.2 gives that $Ш(J/\mathbb{Q})[2]$ has rank at least 2 and therefore that $J(\mathbb{Q})$ has rank 0, unconditionally.

2. The proof of Theorem 1.2

We fix the following notation for the remainder of the paper. Let K be a field of characteristic different from 2 and let $\overline{K}$ be a separable closure of K. Let X/K be the hyperelliptic curve given by the affine equation $y^2 = f(x)$ with $f(x) \in K[x]$ a square free polynomial of even degree n. Let $J := \mathrm{Pic}^0_X$ be the Jacobian of X and let $J^1 := \mathrm{Pic}^1_X$ be the J-torsor over K pararmeterizing divisor classes of degree 1 on X. Recall that a 2-covering of J^1 is a $J[2]$-torsor $\rho\colon F \to J^1$ whose type (cf. [9, Section 2.3]) is given by the canonical inclusion $J[2](\overline{K}) \subset J(\overline{K}) = \mathrm{Pic}^0_X(\overline{K}) = \mathrm{Pic}^0(\overline{K}) \subset \mathrm{Pic}(\overline{X})$. Equivalently (cf. [9, Section 3.3]) there are isomorphisms $\psi\colon F_{\overline{K}} \to J_{\overline{K}}$ and $\phi\colon J^1_{\overline{K}} \to J_{\overline{K}}$ such that ϕ is compatible with the J-torsor

structure on J^1 and $\phi \circ \rho = [2] \circ \psi$. Let $\mathrm{Cov}^2(J^1/K)$ denote the set of K-isomorphism classes of 2-coverings of J^1.

By geometric class field theory, pulling back along the canonical map $X \to \mathrm{Pic}^1_X = J^1$ gives a bijective map $\mathrm{Cov}^2(J^1/K) \to \mathrm{Cov}^2(X/K)$, where $\mathrm{Cov}^2(X/K)$ is the set of K-isomorphism classes of 2-coverings of X, i.e., K-forms of the maximal unramified exponent 2 abelian covering of X.

Definition 2.1 ([5, Definition 5.3])**.** *A 2-covering of J^1 is good if the corresponding 2-covering of $\pi\colon Y \to X$ has the following property: for some (and hence any) Weierstrass point $\omega \in X(\overline{K})$, the pullback $\pi^*\omega$ is linearly equivalent to a K-rational divisor on Y. Define $\mathrm{Cov}^2_{\mathrm{good}}(J^1/K)$ to be the set of K-isomorphism classes of good 2-coverings of J^1.*

Given a pair $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$ of symmetric bilinear forms with $\mathrm{disc}(Ax - B) = f(x)$, the Fano variety of maximal linear subspaces contained in the base locus of the pencil of quadrics generated by (A, B) may be given the structure of a 2-covering of J^1 [1, Theorem 23].

Definition 2.2. *A 2-covering of $\rho\colon F \to J^1$ arises from a pencil of quadrics if F is the Fano variety of maximal linear subspaces in the base locus of the pencil of quadrics generated by $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$ with $\mathrm{disc}(Ax - B) = f(x)$. Define $\mathrm{Cov}^2_0(J^1/K)$ to be the set of K-isomorphism classes of 2-coverings of J^1 that arise from a pencil of quadrics.*

Lemma 2.3. *Notation as above, there is an equality $\mathrm{Cov}^2_0(J^1/K) = \mathrm{Cov}^2_{\mathrm{good}}(J^1/K)$ of subsets of $\mathrm{Cov}^2(J^1/K)$.*

Proof. Since the pullback map $\mathrm{Cov}^2(J^1/K) \to \mathrm{Cov}^2(X/K)$ is injective, it suffices to show that the images of $\mathrm{Cov}^2_0(J^1/K)$ and $\mathrm{Cov}^2_{\mathrm{good}}(J^1/K)$ are the same. By [1, Theorem 24] the image $\mathrm{Cov}^2_0(X/K)$ of $\mathrm{Cov}^2_0(J^1/K)$ is the set of isomorphism classes $C \to X$ which admit a lift to a degree 2 covering $C' \to C$ such that the composition $C' \to X$ is a K-form of the maximal abelian of exponent 2 covering of $X_{\overline{K}} := X \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, \overline{K}$ unramified outside $\mathfrak{m}$, for $\mathfrak{m} \in \mathrm{Div}(X)$ a (fixed) divisor of degree 2 corresponding to a pair of non-Weierstrass points conjugate under the hyperelliptic involution.

First we show that $\mathrm{Cov}^2_{\mathrm{good}}(X/K) \subset \mathrm{Cov}^2_0(X/K)$. Suppose $\pi\colon C \to X$ represents a class in $\mathrm{Cov}^2_{\mathrm{good}}(X/K)$ and let $\omega \in X(\overline{K})$ be a Weierstrass point. Then, by definition, there is some $d \in \mathrm{Div}(C)$ linearly equivalent to $\pi^*\omega$. Since ω is a Weierstrass point, there is some $g \in \overline{K}(X)^\times$ such that $2\omega - \mathfrak{m} = \mathrm{div}(g)$. Then $\mathrm{div}(\pi^* g) = 2\pi^*\omega - \pi^*\mathfrak{m}$ is linearly equivalent to the K-rational principal divisor $2d - \pi^*\mathfrak{m} = \mathrm{div}(f)$. By Hilbert's Theorem 90 we may assume $f \in K(C)^\times$. The degree 2 cover corresponding to the quadratic extension $K(C)(\sqrt{f})$ gives the desired lift $C' \to C$.

Now let us show that $\mathrm{Cov}^2_0(X/K) \subset \mathrm{Cov}^2_{\mathrm{good}}(X/K)$. Suppose $\pi\colon C \to X$ represents a class in $\mathrm{Cov}^2_0(X/K)$. For each Weierstrass point $\omega \in X(\overline{K})$ there is a function $f_\omega \in \overline{K}(X)$ such that $\mathrm{div}(f_\omega) = 2\omega - \mathfrak{m}$. The maximal exponent 2 abelian covering of $X_{\overline{K}}$ unramified outside $\mathfrak{m}$ corresponds to the extension obtained by adjoining square roots of all f_ω, while its maximal unramified subcover corresponds to the extension obtained by adjoining square roots to all ratios $f_\omega / f_{\omega'}$. From this one sees that $C'_{\overline{K}} \to C_{\overline{K}}$ is the double cover ramified at $\pi^{-1}(\mathfrak{m}) = \pi^*\mathfrak{m} \subset \mathrm{Div}(C_{\overline{K}})$. Any K-form $C' \to C$ of this must be given by adjoining a square root of a function $f \in K(C)^\times$ with divisor of the form $\mathrm{div}(f) = 2d - \pi^*\mathfrak{m}$, for some

$d \in \mathrm{Div}(C)$. Then, since $\mathfrak{m}$ and 2ω are linearly equivalent, we have that $2d - 2\pi^*\omega \in \mathrm{Div}(\overline{C})$ is principal. But since $C \to X$ is a *maximal* unramified exponent 2 abelian covering of X we must have that $d - \pi^*\omega$ is principal, i.e., that $\pi^*\omega$ is linearly equivalent to a k-rational divisor. Hence $C \to X$ represents a class in $\mathrm{Cov}_{\mathrm{good}}(X/K)$. □

Proof of Theorem 1.2. We maintain the notation introduced at the beginning of this section, specializing to the case that $K = k$ is a global field and suppose X/k has divisors of degree 1 everywhere locally. By [5, Lemma 6.1(2)] the 'descent map' on $\mathrm{Cov}^2_{\mathrm{good}}(J^1/k)$ induces a bijection $\mathrm{Cov}^2_{\mathrm{good}}(J^1/k) \cap \mathrm{Sel}^2(J^1/k) \to \mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$, where $\mathrm{Sel}^2(J^1/k)$ denotes the set of isomorphism classes of locally soluble 2-coverings of J^1. By [1, Theorem 31], $\mathrm{Sel}^2(J^1/k) \subset \mathrm{Cov}^2_0(J^1/k)$. Hence $\mathrm{Sel}^2(J^1/k)$ and $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k)$ are in bijection. Furthermore, $\mathrm{Sel}^2(J^1/k)$ is empty if and only if the class of J^1 is not divisible by 2 in $Ш(J/k)$ [5, Proposition 2.3]. One deduces the final statement of the theorem using the Cassels-Tate pairing exactly as in [5, Corollary 4.6] □

Remark 2.4. *If X does not have divisors of degree 1 everywhere locally, then* [1, Theorem 28] *shows that $\mathrm{Sel}^2(J^1/k) \cap \mathrm{Cov}^2_0(J^1/k) = \mathrm{Sel}^2(J^1/k) \cap \mathrm{Cov}^2_{\mathrm{good}}(J^1/k) = \emptyset$. In this situation one also has $\mathrm{Sel}^2_{\mathrm{alg}}(J^1/k) = \emptyset$ (cf.* [5, Remark, p. 305]*). It is still possible in this situation, however, that $\mathrm{Sel}^2(J^1/k) \neq \emptyset$. This shows that it is not possible to generalize the theorem further to the case that X does not have divisors of degree 1 everywhere locally, even if J^1 is assumed to have points everywhere locally.*

Acknowledgements. The author would like to thank Steve Donnelly and Michael Stoll for helpful discussions, Drew Sutherland for testing the algorithm on the genus two curves in the LMFDB [6] and the anonymous referee for suggestions which improved the exposition.

References

[1] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser. ↑1, 3, 4

[2] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. ↑1

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑2

[4] J. W. S. Cassels, *The Mordell-Weil group of curves of genus* 2, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, Boston, Mass., 1983, pp. 27–60. ↑1

[5] Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, Algorithmic number theory: Proceedings of the 10th Biennial International Symposium (ANTS-X) held in San Diego, July 9–13, 2012 (Everett W. Howe and Kiran S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Science Publishers, 2013, pp. 295–315. ↑1, 2, 3, 4

[6] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2017. [Online; accessed 26 July 2017]. ↑2, 4

[7] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. ↑1

[8] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. ↑1, 2

[9] Alexei N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. ↑2

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
E-mail address: brendan.creutz@canterbury.ac.nz