

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 [BS09, Cas83, PS97] is sometimes successful in practice. In [Cre13] it is shown how to incorporate additional information coming from a 2-descent on the variety $J^1 = \text{Pic}_X^1$ which is a torsor under J . In particular an algorithm for computing a set denoted $\text{Sel}_{\text{alg}}^2(J^1/k)$ is given and the following result is proven.

Theorem 1.1 ([Cre13, 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 $\text{Sel}_{\text{alg}}^2(J^1/k)$ is nonempty if and only if the torsor J^1 is divisible by 2 in $\text{III}(J/k)$. Moreover, if $\text{Sel}_{\text{alg}}^2(J^1/k) = \emptyset$, then $\dim_{\mathbb{F}_2} \text{III}(J/k)[2] \geq 2$.*

The second statement of the theorem is deduced from the first using the fact that the group $\text{III}(J/k)[2]/2\text{III}(J/k)[4]$ has square order, a consequence of the fact that the Cassels-Tate pairing induces a nondegenerate alternating pairing on this quotient because X is assumed to have divisors of degree 1 everywhere locally [PS99]. This is useful in determining the Mordell-Weil rank of the Jacobian since there is an exact sequence,

$$0 \rightarrow J(k)/2J(k) \rightarrow \text{Sel}^2(J/k) \rightarrow \text{III}(J/k)[2] \rightarrow 0.$$

Thus lower bounds for $\text{III}(J/k)[2]$ allow one to deduce sharper upper bounds for the rank of $J(k)$. As remarked on [Cre13, p. 305], the hypothesis of Theorem 1.1 that X be everywhere locally solvable seems overly strict; one would expect that the theorem remains true under the weaker hypothesis that X has a rational divisor 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 [BGW17] concerning the 2-Selmer set of J^1 . Using this we prove the following result.

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

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 [BCP97] did not always have the parity one would expect assuming standard conjectures. Unlike the usual 2-descent on the Jacobian, computing $\text{Sel}_{\text{alg}}^2(J^1/k)$ and using Theorem 1.1 can indeed lead to bounds which can be improved by assuming parity or finiteness of $\text{III}(J/k)$. Specifically, if X has divisors of degree 1 everywhere locally and $\text{Sel}_{\text{alg}}^2(J^1/k) = \emptyset$, then $J^1(k) = \emptyset$ and J^1 represents a nontrivial element of $\text{III}(J/k)[2]$. However, if X does not have points everywhere locally Theorem 1.1 does not apply and, without further assumptions, we cannot conclude that $\text{III}(J/k)[2]/2\text{III}(J/k)[4]$ is nontrivial. Consequently we only get a lower bound of 1 for $\dim_{\mathbb{F}_2} \text{III}(J/k)[2]$ instead of 2. If $\text{III}(J/k)$ contains no non-trivial infinitely 2-divisible elements (as is widely conjectured but far from being proven), then $\dim_{\mathbb{F}_2} \text{III}(J/k)[2]$ is even [PS99]. 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.

A particular example is given by the curve

$$X/\mathbb{Q} : y^2 = 5x^6 + x^5 + x^4 - 4x^3 - 4x^2 + 5x - 1.$$

The polynomial on the right hand side above has Galois group S_6 over \mathbb{Q} , so $J(\mathbb{Q})$ has no points of order 2. The 2-Selmer group of the Jacobian is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, from which we deduce that the rank of $J(\mathbb{Q})$ is at most 2. Computing $\text{Sel}_{\text{alg}}^2(J^1/\mathbb{Q})$ as described in [Cre13] we find that it is empty. Since $\text{Div}^1(X_{\mathbb{Q}_p}) \neq \emptyset$ for all primes $p \leq \infty$, this implies that $J^1(\mathbb{Q}) = \emptyset$ and, hence, that J^1 represents a nontrivial element of $\text{III}(J/\mathbb{Q})[2]$. However, $X(\mathbb{Q}_3) = \emptyset$, 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 $\text{III}(J/\mathbb{Q})[2]$ has rank at least 2 and therefore that $J(\mathbb{Q})$ has rank 0, unconditionally.

2. THE PROOF OF THEOREM 1.2

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 . For any field extension K of k , let $\text{Cov}^2(J^1/K)$ denote the set of K -isomorphism classes of 2-coverings of $J_K = J \times_{\text{Spec}(k)} \text{Spec}(K)$. Given a pair of symmetric bilinear forms (A, B) such that $\text{disc}(Ax - B) = f(x)$, 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 [BGW17, Theorem 23]. In general, not every 2-covering of J^1 can be defined in this way. Let $\text{Cov}_0^2(J^1/K)$ denote the subset of $\text{Cov}^2(J^1/K)$ consisting of those isomorphism classes of 2-coverings that do arise in this way from a pair of symmetric bilinear forms. This set is in bijection with the set of $(\text{SL}_n/\mu_2)(K)$ orbits of pairs (A, B) with $\text{disc}(Ax - B) = f(x)$. We will show below that $\text{Cov}_0^2(J^1/K)$ is equal to the set $\text{Cov}_{\text{good}}^2(J^1/K)$ defined in [Cre13]. But before that, let us outline the proof of Theorem 1.1 given in [Cre13], and in so doing see how this allows us to deduce Theorem 1.2.

In [Cre13, Section 6] we defined a ‘descent map’ on $\text{Cov}_{\text{good}}^2(J^1/k)$ and proved that it induces a bijection $\text{Cov}_{\text{good}}^2(J^1/k) \cap \text{Sel}^2(J^1/k) \rightarrow \text{Sel}_{\text{alg}}^2(J^1/k)$. This does not require local solubility of X ; it only requires the weaker assumption that X has divisors of degree 1 everywhere locally. The second step is to prove that the set $\text{Sel}^2(J^1/k)$ of locally soluble coverings is contained in $\text{Cov}_{\text{good}}^2(J^1/k)$. This was shown in [Cre13, Proposition 6.2] under the assumption that X is everywhere locally solvable. When combined with the descent map, this implies that $\text{Sel}^2(J^1/k)$ and $\text{Sel}_{\text{alg}}^2(J^1/k)$ are in bijection, and the conclusion of the theorems follows. This same argument proves Theorem 1.2, provided we can verify that $\text{Sel}^2(J^1/k) \subset \text{Cov}_{\text{good}}^2(J^1/k)$ under the weaker hypothesis that X has divisors of degree 1 everywhere locally.

Bhargava, Gross and Wang show that $\text{Sel}^2(J^1/k) \subset \text{Cov}_0^2(J^1/k)$ when X has divisors of degree 1 everywhere locally [BGW17, Theorem 31]. It is therefore enough to show that $\text{Cov}_0^2(J^1/k) \subset \text{Cov}_{\text{good}}^2(J^1/k)$. We show that these sets are actually equal.

Lemma 2.1. *Let K be any field extension of k . Then $\text{Cov}_0^2(J^1/K) = \text{Cov}_{\text{good}}^2(J^1/K)$.*

Proof. By geometric class field theory, pulling back along the canonical map $X \rightarrow \text{Pic}_X^1 = J^1$ gives a bijective map $\text{Cov}^2(J^1/K) \rightarrow \text{Cov}^2(X/K)$, where $\text{Cov}^2(X/K)$ is the set of isomorphism classes of 2-coverings of X , i.e., K -forms of the maximal unramified exponent 2 abelian covering of X . Since this map is injective, it is enough to show that $\text{Cov}_0^2(J^1/K)$ and $\text{Cov}_{\text{good}}^2(J^1/K)$ have the same image in $\text{Cov}^2(X/K)$.

The image $\text{Cov}_{\text{good}}^2(X/K)$ of $\text{Cov}_{\text{good}}^2(J^1/K)$ is by definition (see [Cre13, Definition 5.3]) the set of isomorphism classes $\pi : C \rightarrow X_K$ with the property that $\pi^*\omega$ is linearly equivalent to a K -rational divisor for any Weierstrass point $\omega \in X(\overline{K})$. By [BGW17, Theorem 24] the image $\text{Cov}_0^2(X/K)$ of $\text{Cov}_0^2(J^1/K)$ is the set of isomorphism classes $C \rightarrow X_K$ which admit a lift to a degree 2 covering $C' \rightarrow C$ such that the composition $C' \rightarrow X_K$ is a K -form of the maximal abelian of exponent 2 covering of $X_{\overline{K}}$ unramified outside \mathfrak{m} , for $\mathfrak{m} \in \text{Div}(X)$ a (fixed) divisor of degree 2 corresponding to a pair of non-Weierstrass points conjugate under the hyperelliptic involution.

First we show that $\text{Cov}_{\text{good}}^2(X/K) \subset \text{Cov}_0^2(X/K)$. Suppose $\pi : C \rightarrow X_K$ represents a class in $\text{Cov}_{\text{good}}^2(X/K)$. Then there is some $d \in \text{Div}(C)$ linearly equivalent to $\pi^*\omega$. There is $g \in \overline{K}(X)^\times$ such that $2\omega - \mathfrak{m} = \text{div}(g)$. Then $\text{div}(\pi^*g) = 2\pi^*\omega - \pi^*\mathfrak{m}$ is linearly equivalent to the K -rational principal divisor $2d - \pi^*\mathfrak{m} = \text{div}(f)$. 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 $C' \rightarrow C$.

Now let us show that $\text{Cov}_0^2(X/K) \subset \text{Cov}_{\text{good}}^2(X/K)$. Suppose $\pi : C \rightarrow X_K$ represents a class in $\text{Cov}_0^2(X/K)$. For each Weierstrass point $\omega \in X(\overline{K})$ there is a function $f_\omega \in \overline{K}(X)$ such that $\text{div}(f_\omega) = 2\omega - \mathfrak{m}$. 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 $C'_{\overline{K}} \rightarrow C_{\overline{K}}$ is the double cover ramified at $\pi^{-1}(\mathfrak{m}) = \pi^*\mathfrak{m} \subset \text{Div}(C_{\overline{K}})$. Any K -form $C' \rightarrow C$ of this must be given by adjoining a square root of a function $f \in K(C)^\times$ with divisor of the form $\text{div}(f) = 2d - \pi^*\mathfrak{m}$, for some $d \in \text{Div}(C)$. Then for any Weierstrass point ω , we have that $2d - 2\pi^*\omega \in \text{Div}(C)$ is principal. But since $C \rightarrow X_K$ is a *maximal* unramified exponent 2 abelian covering of X_K

we must have that $d - \pi^*\omega$ is principal, i.e., that $\pi^*\omega$ is linearly equivalent to a k -rational divisor. Hence $C \rightarrow X_K$ represents a class in $\text{Cov}_{\text{good}}(X/K)$. \square

Remark 2.2. *If X does not have divisors of degree 1 everywhere locally, then [BGW17] shows that $\text{Sel}^2(J^1/k) \cap \text{Cov}_0^2(J^1/k) = \text{Sel}^2(J^1/k) \cap \text{Cov}_{\text{good}}^2(J^1/k) = \emptyset$. In this situation one also has $\text{Sel}_{\text{alg}}^2(J^1/k) = \emptyset$ (cf. [Cre13, Remark, p. 305]). It is still possible in this situation, however, that $\text{Sel}^2(J^1/k) \neq \emptyset$. 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.

REFERENCES

- [BGW17] 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](#), [2](#), [3](#), [4](#)
- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. [↑1](#)
- [BCP97] 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](#)
- [Cas83] 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. MR717589 [↑1](#)
- [Cre13] 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](#)
- [PS97] 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](#)
- [PS99] 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](#)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800, CHRISTCHURCH 8140, NEW ZEALAND

E-mail address: brendan.creutz@canterbury.ac.nz

URL: <http://www.math.canterbury.ac.nz/~bcreutz>