Computing Néron-Severi groups and cycle class groups

Poonen, B.; Testa, D.; Luijk, R.M. van

COMPOSITIO MATHEMATICA

Computing Néron–Severi groups and cycle class groups

Bjorn Poonen, Damiano Testa and Ronald van Luijk

Compositio Math. **151** (2015), 713–734.

doi:10.1112/S0010437X14007878

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
150 YEARS

Compositio Math. 151 (2015) 713–734
doi:10.1112/S0010437X14007878

Computing Néron–Severi groups and cycle class groups

Bjorn Poonen, Damiano Testa and Ronald van Luijk

Abstract

Assuming the Tate conjecture and the computability of étale cohomology with finite coefficients, we give an algorithm that computes the Néron–Severi group of any smooth projective geometrically integral variety, and also the rank of the group of numerical equivalence classes of codimension p cycles for any p.

1. Introduction

Let k be a field, and let k^{sep} be a separable closure. Let X be a smooth projective geometrically integral k-variety, and let $X^{\mathrm{sep}} := X \times_k k^{\mathrm{sep}}$.

If $k = \mathbb{C}$, then the Lefschetz $(1,1)$ theorem identifies the Néron–Severi group $\operatorname{NS} X$ (see § 3 for definitions) with the subgroup of $\mathrm{H}^2(X(\mathbb{C}), \mathbb{Z})$ mapping into the subspace $\mathrm{H}^{1,1}(X)$ of $\mathrm{H}^2(X(\mathbb{C}), \mathbb{C})$. Analogously, if k is a finitely generated field, then the Tate conjecture describes $(\operatorname{NS} X^{\mathrm{sep}}) \otimes \mathbb{Q}_\ell$ in terms of the action of $\operatorname{Gal}(k^{\mathrm{sep}}/k)$ on $\mathrm{H}^2_{\text{ét}}(X^{\mathrm{sep}}, \mathbb{Q}_\ell(1))$, for any prime $\ell \neq \operatorname{char} k$.

Can such descriptions be transformed into algorithms for computing $\operatorname{NS} X^{\mathrm{sep}}$? To make sense of this question, we assume that k is replaced by a finitely generated subfield over which X is defined; then X and k admit a finite description suitable for computer input (see § 7.1). Using the Lefschetz $(1,1)$ theorem involves working over the uncountable field $\mathbb{C}$, while using the Tate conjecture involves an action of an uncountable Galois group on a vector space over an uncountable field $\mathbb{Q}_\ell$, so it is not clear a priori that either approach can be made into an algorithm.

In this paper, assuming only the ability to compute the finite Galois modules $\mathrm{H}^i_{\text{ét}}(X^{\mathrm{sep}}, \mu_{\ell^n})$ for each $i \leqslant 2$ and n, we give an algorithm for computing $\operatorname{NS} X^{\mathrm{sep}}$ that terminates if and only if the Tate conjecture holds for X (Remark 8.34). Moreover, if k is finite, then we can even avoid computing the Galois modules $\mathrm{H}^i_{\text{ét}}(X^{\mathrm{sep}}, \mu_{\ell^n})$, by instead using point-counting to compute the zeta function of X, as is well known (Theorem 8.36(b)). In any case, we give an algorithm to compute $\mathrm{H}^i_{\text{ét}}(X^{\mathrm{sep}}, \mu_{\ell^n})$ for any variety in characteristic 0 (Theorem 7.9) and any variety that lifts to characteristic 0 (Corollary 7.10); also, after the first version of the present article was made available, Madore and Orgogozo announced an algorithm to compute it in general [MO14, Théorème 0.9] (they work over an algebraically closed ground field, but the cohomology groups are unchanged in passing from k^{sep} to $\overline{k}$).

Combining our results with the truth of the Tate conjecture for K3 surfaces X over finitely generated fields of characteristic not 2 [Nyg83, Nyg85, Mau14, Cha13, Mad14] yields

Received 24 October 2012, accepted 8 November 2013, received in final form 28 July 2014, published online 4 February 2015.
2010 Mathematics Subject Classification 14C22 (primary), 14C25, 14F20, 14G25, 14G27 (secondary).
Keywords: Néron–Severi groups, cycle class groups, Tate conjecture.
The first author was supported by the Guggenheim Foundation and National Science Foundation grants DMS-0841321 and DMS-1069236.

an unconditional algorithm for computing $\operatorname{NS} X^{\text{sep}}$ for all such K3 surfaces (Theorem 8.38). (See [Tat94, § 5] and [And96] for some other cases in which the Tate conjecture is known.) We also provide an unconditional algorithm for computing the torsion subgroup $(\operatorname{NS} X^{\text{sep}})_{\text{tors}}$ for any X over any finitely generated field k (Theorem 8.32).

Finally, we also prove statements for cycles of higher codimension. In particular, we describe a conditional algorithm that computes the rank of the group $\operatorname{Num}^p X^{\text{sep}}$ of codimension p cycles modulo numerical equivalence (Theorem 8.15).

If k^{sep} is replaced by an algebraic closure $\overline{k}$ in any of the results above, the resulting analogue holds (Remarks 8.17 and 8.35).

2. Previous approaches

Several techniques exist in the literature for obtaining information on Néron–Severi groups.

- Lower bounds on the rank are often obtained by exhibiting divisors explicitly.
- An initial upper bound is given by the second Betti number, which is computable (see Proposition 8.2).
- Over $\mathbb{C}$, Hodge theory provides the improved upper bound $h^{1,1}$, which again is computable. (Indeed, software exists for computing all the Hodge numbers $h^{p,q} := \dim \mathrm{H}^q(X, \Omega^p)$, as a special case of computing cohomology of coherent sheaves on projective varieties [Vas98, Appendix C.3].)
- Over a finite field k, computation of the zeta function can yield an improved upper bound: see § 8.5 for details.
- Over finitely generated fields k, one can spread out X to a smooth projective scheme $\mathcal{X}$ over a finitely generated $\mathbb{Z}$-algebra and reduce modulo maximal ideals to obtain injective specialization homomorphisms $(\operatorname{NS} X^{\text{sep}}) \otimes \mathbb{Q} \to (\operatorname{NS} \mathcal{X}_{\overline{F}}) \otimes \mathbb{Q}$ where F is the finite residue field (see [vanL07b, Proposition 6.2] or [MP12, Proposition 3.6], for example). Combining this with the method of the previous item bounds the rank of $\operatorname{NS} X^{\text{sep}}$. In some cases, one can prove directly that certain elements of $(\operatorname{NS} \mathcal{X}_{\overline{F}}) \otimes \mathbb{Q}$ are not in the image of the specialization homomorphism, to improve the bound [EJ11a].
- The previous item can be improved also by using more than one reduction if one takes into account that the specialization homomorphisms preserve additional structure, such as the intersection pairing in the case $\dim X = 2$ [vanL07a] or the Galois action [EJ11b]. In the $\dim X = 2$ case, the discriminant of the intersection pairing can be obtained, up to a square factor, either from explicit generators for $(\operatorname{NS} \mathcal{X}_{\overline{F}}) \otimes \mathbb{Q}$ [vanL07a] or from the Artin–Tate conjecture [Klo07]. Charles proved that for a K3 surface X over a number field, the information from reductions is sufficient to determine the rank of $\operatorname{NS} X^{\text{sep}}$, assuming the Hodge conjecture for 2-cycles on $X \times X$ [Cha14].
- If X is a quotient of another variety Y by a finite group G, then the natural map
$$(\operatorname{NS} X^{\text{sep}}) \otimes \mathbb{Q} \to ((\operatorname{NS} Y^{\text{sep}}) \otimes \mathbb{Q})^G$$
is an isomorphism. For instance, this has been applied to **Delsarte surfaces**, i.e., surfaces in $\mathbb{P}^3$ defined by a homogeneous form with four monomials, using that they are quotients of Fermat surfaces [Shi86].
- When X is an elliptic surface, the rank of $\operatorname{NS} X^{\text{sep}}$ is related to the rank of the Mordell–Weil group of the generic fiber [Tat95, p. 429], [Shi72, Corollary 1.5], [Shi90, Corollary 5.3]. This has been generalized in various ways, for example to fibrations into abelian varieties [Kah09], [Ogu09, Theorem 1.1].

- When X is a K3 surface of degree 2 over a number field, the Kuga–Satake construction relates the Hodge classes on X to the Hodge classes on an abelian variety of dimension 2^{19}. Hassett, Kresch, and Tschinkel use this to give an algorithm to compute $\operatorname{NS} X^{\mathrm{sep}}$ for such X [HKT13, Proposition 19].

Also, [Sim08] shows that if one assumes the Hodge conjecture, then one can decide, given a nice variety X over $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ and a singular homology class $\gamma \in \mathrm{H}_{2p}(X(\mathbb{C}), \mathbb{Q})$, whether γ is the class of an algebraic cycle.

3. Notation

Given a module A over an integral domain R, let A_{tors} be its torsion submodule, let $\widetilde{A} := A/A_{\mathrm{tors}}$, and let $\operatorname{rk} A := \dim_K(A \otimes_R K)$ where $K := \operatorname{Frac} R$. If A is a submodule of another R-module B, the saturation of A in B is $\{b \in B : nb \in A \text{ for some nonzero } n \in R\}$. If A is a G-module for some group G, then A^G is the subgroup of invariant elements. We say that a G-module A is finite if it is so as a set, and finitely generated if it is so as an abelian group.

Given a field k, let $\overline{k}$ be an algebraic closure, let k^{sep} be the separable closure inside $\overline{k}$, let $G_k := \operatorname{Gal}(k^{\mathrm{sep}}/k) \simeq \operatorname{Aut}(\overline{k}/k)$, and let κ be the characteristic of k. A variety X over a field k is a separated scheme of finite type over k. For such X, let $X^{\mathrm{sep}} := X \times_k k^{\mathrm{sep}}$ and $\overline{X} := X \times_k \overline{k}$. Call X nice if it is smooth, projective, and geometrically integral.

Suppose that X is a nice k-variety. Let $\operatorname{Pic} X$ be its Picard group. Let $\mathbf{Pic}_{X/k}$ be the Picard scheme of X over k. There is an injection $\operatorname{Pic} X \to \mathbf{Pic}_{X/k}(k)$, but it is not always surjective. Let $\mathbf{Pic}^0_{X/k}$ be the connected component of the identity in $\mathbf{Pic}_{X/k}$. Let $\operatorname{Pic}^0 X \leqslant \operatorname{Pic} X$ be the group of isomorphism classes of line bundles such that the corresponding k-point of $\mathbf{Pic}_{X/k}$ lies in $\mathbf{Pic}^0_{X/k}$; any such line bundle $\mathscr{L}$ (or divisor representing it) is called algebraically equivalent to 0. Equivalently, a line bundle $\mathscr{L}$ is algebraically equivalent to 0 if there is a connected variety B and a line bundle $\mathscr{M}$ on $X \times B$ such that $\mathscr{M}$ restricts to the trivial line bundle above one point of B and to $\mathscr{L}$ above another (this holds even over the ground field k: take B to be a component H of $\mathbf{EffDiv}_X$ lying above a translate of $\mathbf{Pic}^0_{X/k}$ as in Lemma 8.29(a), (b)). Define the Néron–Severi group $\operatorname{NS} X$ as the quotient $\operatorname{Pic} X/\operatorname{Pic}^0 X$; it can be identified with the set of components of $\mathbf{Pic}_{X/k}$ containing the class of a divisor of X over k (which is stronger than assuming that the component has a k-point). Then $\operatorname{NS} X$ is a finitely generated abelian group [Nér52, p. 145, Théorème 2] (see [SGA6, XIII.5.1] for another proof). Let $\mathbf{Pic}^{\tau}_{X/k}$ be the finite union of connected components of $\mathbf{Pic}_{X/k}$ parametrizing classes of line bundles whose class in $\operatorname{NS} \overline{X}$ is torsion.

Let $\mathscr{Z}^p(X)$ be the group of codimension p cycles on X. Let $\operatorname{Num}^p X$ be the quotient of $\mathscr{Z}^p(X)$ by the subgroup of cycles numerically equivalent to 0. Then $\operatorname{Num}^p X$ is a finite-rank free abelian group. Let $\mathscr{Z}^1(X)^{\tau}$ be the set of divisors $z \in \mathscr{Z}^1(X)$ having a positive multiple that is algebraically equivalent to 0. Let $(\operatorname{Pic} X)^{\tau}$ be the image of $\mathscr{Z}^1(X)^{\tau}$ under $\mathscr{Z}^1(X) \to \operatorname{Pic} X$.

If $m \in \mathbb{Z}_{>0}$ and $\kappa \nmid m$, and $i, p \in \mathbb{Z}$, let $\mathrm{H}^i(X^{\mathrm{sep}}, (\mathbb{Z}/m\mathbb{Z})(p))$ be the étale cohomology group; this is a finite abelian group. For each prime $\ell \neq \kappa$, define

$$\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p)) := \varprojlim_n \mathrm{H}^i(X^{\mathrm{sep}}, (\mathbb{Z}/\ell^n\mathbb{Z})(p)),$$

a finitely generated $\mathbb{Z}_\ell$-module, and define

$$\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Q}_\ell(p)) := \mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

a finite-dimensional $\mathbb{Q}_\ell$-vector space; its dimension $b_i(X)$ is independent of p, and is called an ℓ-adic Betti number.

Let X be a nice k-variety. Let $K(X)$ be its Grothendieck group of coherent sheaves. For a coherent sheaf $\mathscr{F}$ on a projective variety X, define $\chi(\mathscr{F}) := \sum_{i\geqslant 0}(-1)^i \dim \mathrm{H}^i(X,\mathscr{F})$; this induces a homomorphism $\chi\colon K(X)\to\mathbb{Z}$ sending the class $\mathrm{cl}(\mathscr{F})$ of $\mathscr{F}$ to $\chi(\mathscr{F})$.

4. Group-theoretic lemmas

Given any prime ℓ, let $\ell' := \ell$ if $\ell \neq 2$, and $\ell' := 4$ if $\ell = 2$.

Lemma 4.1 (cf. [Min87, § 1]). *Let ℓ be a prime. Let G be a group acting through a finite quotient on a finite-rank free $\mathbb{Z}$-module or $\mathbb{Z}_\ell$-module Λ. If G acts trivially on $\Lambda/\ell'\Lambda$, then G acts trivially on Λ.*

Proof. Let $n := \mathrm{rk}\,\Lambda$. Write $\ell' =: \ell^s$. For $r \geqslant s$, let $U_r := 1 + \ell^r M_n(\mathbb{Z}_\ell)$. It suffices to show that there are no non-identity elements of finite order in the kernel U_s of $\mathrm{GL}_n(\mathbb{Z}_\ell)\to\mathrm{GL}_n(\mathbb{Z}_\ell/\ell'\mathbb{Z}_\ell)$. In fact, for $r\geqslant s$ the binomial theorem shows that $1+A\in U_r - U_{r+1}$ implies $(1+A)^\ell \in U_{r+1}-U_{r+2}$, so by induction any non-identity $1+A\in U_s$ has infinitely many distinct powers, and cannot be of finite order. □

Lemma 4.2. *Let a topological group G act continuously on a finite-rank free $\mathbb{Z}_\ell$-module Λ. Let $r := \mathrm{rk}\,\Lambda^G$. Then the following hold:*

(a) *the continuous cohomology group $\mathrm{H}^1(G,\Lambda)[\ell^\infty]$ is finite;*

(b) *$\#(\Lambda/\ell^n\Lambda)^G = O(\ell^{rn})$ as $n\to\infty$.*

Proof. For each n, taking continuous group cohomology of $0\to\Lambda\xrightarrow{\ell^n}\Lambda\to\Lambda/\ell^n\Lambda\to 0$ yields

$$0 \to \frac{\Lambda^G}{\ell^n(\Lambda^G)} \to \left(\frac{\Lambda}{\ell^n\Lambda}\right)^G \to \mathrm{H}^1(G,\Lambda)[\ell^n]\to 0. \tag{4.3}$$

(a) By (4.3) for $n=1$, the group $\mathrm{H}^1(G,\Lambda)[\ell]$ is finite. So if $\mathrm{H}^1(G,\Lambda)[\ell^\infty]$ is infinite, it contains a copy of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, contradicting the $Y=0$ case of [Tat76, Proposition 2.1].

(b) In (4.3), the group on the left has size ℓ^{rn}, and the group on the right has size $O(1)$ as $n\to\infty$, by (a). □

5. Upper bound on the rank of the group of Tate classes

Setup 5.1. Let k be a finitely generated field. Let $G := G_k$. Let X be a nice variety over k. Let $d := \dim X$. Fix $p\in\{0,1,\dots,d\}$. For each $m\in\mathbb{Z}_{>0}$ with $\kappa\nmid m$, define

$$T_m := \mathrm{H}^{2p}(X^{\mathrm{sep}},(\mathbb{Z}/m\mathbb{Z})(p)).$$

Fix a prime $\ell\neq\kappa$. Define $T := \mathrm{H}^{2p}(X^{\mathrm{sep}},\mathbb{Z}_\ell(p))$, and $V := \mathrm{H}^{2p}(X^{\mathrm{sep}},\mathbb{Q}_\ell(p))$.

An element of V is called a Tate class if it is fixed by a (finite-index) open subgroup of G. Let $V^{\mathrm{Tate}}\leqslant V$ be the $\mathbb{Q}_\ell$-subspace of Tate classes. Let M be the $\mathbb{Z}_\ell$-submodule of elements of T mapping to Tate classes in V. Let $r := \mathrm{rk}\,M = \dim V^{\mathrm{Tate}}$.

Lemma 5.2. *For each $i,n\in\mathbb{Z}_{\geqslant 0}$, there is an exact sequence*

$$0\to\frac{\mathrm{H}^i(X^{\mathrm{sep}},\mathbb{Z}_\ell(p))}{\ell^n\mathrm{H}^i(X^{\mathrm{sep}},\mathbb{Z}_\ell(p))}\to\mathrm{H}^i(X^{\mathrm{sep}},(\mathbb{Z}/\ell^n\mathbb{Z})(p))\to\mathrm{H}^{i+1}(X^{\mathrm{sep}},\mathbb{Z}_\ell(p))[\ell^n]\to 0.$$

Proof. Use [Mil80, Lemma V.1.11] to take cohomology of

$$0 \to \mathbb{Z}_\ell(p) \xrightarrow{\ell^n} \mathbb{Z}_\ell(p) \to (\mathbb{Z}/\ell^n\mathbb{Z})(p) \to 0. \qquad \square$$

Corollary 5.3. *For each $n \geqslant 0$, there is an exact sequence*

$$0 \to \frac{T}{\ell^n T} \to T_{\ell^n} \to \mathrm{H}^{2p+1}(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p))[\ell^n] \to 0.$$

Proof. Take $i = 2p$ in Lemma 5.2. $\square$

Corollary 5.4. *For each $n \geqslant 0$, there is a canonical injection $M/\ell^n M \hookrightarrow T_{\ell^n}$.*

Proof. Since M is saturated in T, we have an injection $M/\ell^n M \hookrightarrow T/\ell^n T$. Compose with the first map in Corollary 5.3. $\square$

Lemma 5.5. *Let $t \in \mathbb{Z}_{\geqslant 0}$ be such that $\ell^t T_{\mathrm{tors}} = 0$. Assume that G acts trivially on $T_{\ell'}$.*

(a) *For any $n \geqslant t$, we have $\# T^G_{\ell^n} \geqslant \ell^{r(n-t)}$.*
(b) *We have $\# T^G_{\ell^n} = O(\ell^{rn})$ as $n \to \infty$.*
(c) *We have*

$$r = \min\left\{ \left\lfloor \frac{\log \# T^G_{\ell^n}}{\log \ell^{n-t}} \right\rfloor : n > t \right\}.$$

Proof. By Corollary 5.4, G acts trivially on $M/\ell' M$, and hence also on $M/\ell M$ and $\widetilde{M}/\ell'\widetilde{M}$. The G-orbit of each element of $\widetilde{M}$ is finite by definition of Tate class, and $\widetilde{M}$ is finitely generated as a $\mathbb{Z}_\ell$-module, so G acts through a finite quotient on $\widetilde{M}$. By Lemma 4.1, G acts trivially on $\widetilde{M}$.

(a) Multiplication by ℓ^t on M kills M_{tors}, so it factors as $M \to \widetilde{M} \twoheadrightarrow \ell^t M$. Hence G acts trivially on $\ell^t M$, so for $n \geqslant t$, the quotient $\ell^t M/\ell^n M$ is contained in $(M/\ell^n M)^G$. By Corollary 5.4, we deduce the inequality $\# T^G_{\ell^n} \geqslant \#(M/\ell^n M)^G \geqslant \#(\ell^t M/\ell^n M) \geqslant \ell^{r(n-t)}$.

(b) By definition of M, we have $\widetilde{T}^G \subseteq \widetilde{M} = \widetilde{M}^G \subseteq \widetilde{T}^G$, so $\operatorname{rk} \widetilde{T}^G = r$. Dividing the first two terms in Corollary 5.3 by the images of T_{tors} yields

$$0 \to \frac{\widetilde{T}}{\ell^n \widetilde{T}} \to \frac{T_{\ell^n}}{I_n} \to \mathrm{H}^{2p+1}(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p))[\ell^n] \to 0,$$

where I_n is the image of T_{tors} in T_{ℓ^n}. This implies the second inequality in

$$\# T^G_{\ell^n} \leqslant \# I^G_n \cdot \# \left(\frac{T_{\ell^n}}{I_n}\right)^G \leqslant \# I^G_n \cdot \# \left(\frac{\widetilde{T}}{\ell^n \widetilde{T}}\right)^G \cdot \#(\mathrm{H}^{2p+1}(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p))[\ell^n])^G.$$

Since $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}_\ell(p))$ is a finitely generated $\mathbb{Z}_\ell$-module for each i, the first and third factors on the right are $O(1)$. On the other hand, Lemma 4.2(b) yields $\#(\widetilde{T}/\ell^n \widetilde{T})^G = O(\ell^{rn})$. Multiplying shows that $\# T^G_{\ell^n} = O(\ell^{rn})$.

(c) The statement follows by combining the previous items. $\square$

6. Cycles under field extension

In this section, assume Setup 5.1.

Proposition 6.1.

(a) *For any extension L of k, the natural map $\operatorname{Num}^p X \to \operatorname{Num}^p X_L$ is injective.*

(b) *The image of $\operatorname{Num}^p X \to \operatorname{Num}^p \overline{X}$ is a finite-index subgroup of $(\operatorname{Num}^p \overline{X})^G$.*

(c) *If $\kappa > 0$, the index of $\operatorname{Num}^p X^{\mathrm{sep}}$ in $\operatorname{Num}^p \overline{X}$ is finite and equal to a power of κ.*

If Num^p is replaced by NS everywhere, then the same three statements hold.

Proof.

(a) If $z \in \mathcal{Z}^p(X)$ has intersection number 0 with all p-cycles on X_L, then in particular it has intersection number 0 with all p-cycles on X.

(b) Suppose that $[z] \in (\operatorname{Num}^p \overline{X})^G$, where $z \in \mathcal{Z}^p(\overline{X})$. Then z comes from some $z_L \in \mathcal{Z}^p(X_L)$ for some finite extension L of k. Let $n := [L : k]$. Then $n[z] = \operatorname{tr}_{L/k}[z]$ comes from $\operatorname{tr}_{L/k} z_L \in \mathcal{Z}^p(X)$. Hence the cokernel of $\operatorname{Num}^p X \to (\operatorname{Num}^p \overline{X})^G$ is torsion, but it is also finitely generated, so it is finite.

(c) We may assume that $k = k^{\mathrm{sep}}$. Then $G = \{1\}$, so (b) implies that $\operatorname{Num}^p X^{\mathrm{sep}}$ is of finite index in $\operatorname{Num}^p \overline{X}$. Moreover, in the proof of (b), $[L : k]$ is always a power of κ, so the index is a power of κ.

Statement (a) for NS follows from the fact that the formation of $\mathbf{Pic}^0_{X/k}$ respects field extension [Kle05, Proposition 9.5.3]. The proofs of (b) and (c) for NS are the same as for Num^p. □

Proposition 6.2. *If k is finite, then the natural homomorphisms $\operatorname{Pic} X \to (\operatorname{Pic} X^{\mathrm{sep}})^G$ and $\operatorname{NS} X \to (\operatorname{NS} X^{\mathrm{sep}})^G$ are isomorphisms.*

Proof. That $\operatorname{Pic} X \to (\operatorname{Pic} X^{\mathrm{sep}})^G$ is an isomorphism follows from the Hochschild–Serre spectral sequence for étale cohomology and the vanishing of the Brauer group of k. Lang's theorem [Lan56] implies $\mathrm{H}^1(k, \operatorname{Pic}^0 X^{\mathrm{sep}}) = 0$, so taking Galois cohomology of

$$0 \to \operatorname{Pic}^0 X^{\mathrm{sep}} \to \operatorname{Pic} X^{\mathrm{sep}} \to \operatorname{NS} X^{\mathrm{sep}} \to 0$$

shows that the homomorphism $\operatorname{Pic} X = (\operatorname{Pic} X^{\mathrm{sep}})^G \to (\operatorname{NS} X^{\mathrm{sep}})^G$ is surjective. On the other hand, its image is $\operatorname{NS} X$. □

7. Hypotheses and conjectures

Our computability results rely on the ability to compute étale cohomology with finite coefficients. Some of the results are conditional also on the Tate conjecture and related conjectures. We now formulate these hypotheses precisely, so that they can be referred to in our main theorems.

7.1 Explicit representation of objects

To specify an ideal in a polynomial ring over $\mathbb{Z}$ in finitely many indeterminates, we give a finite list of generators. To specify a finitely generated $\mathbb{Z}$-algebra A, we give an ideal I in a polynomial ring R as above such that A is isomorphic to R/I. To specify a finitely generated field k, we give a finitely generated $\mathbb{Z}$-algebra A that is a domain such that k is isomorphic to $\operatorname{Frac} A$. To specify a continuous G_k-action on a finitely generated abelian group A, we give a finite Galois extension k' of k together with an action of $\operatorname{Gal}(k'/k)$ on A such that there exists a k-embedding $k' \hookrightarrow k^{\mathrm{sep}}$ such that the original G_k-action is the composition $G_k \twoheadrightarrow \operatorname{Gal}(k'/k) \to \operatorname{Aut} A$. To specify a G_k-action on finitely many finitely generated abelian groups, we use the same k' for all of them. To specify a projective variety X, we give its homogeneous ideal for a particular embedding of X in some projective space. To specify a codimension p cycle on X, we give an explicit integer combination of codimension p integral subvarieties of X.

Definition 7.1. Given k, X, and p as in Setup 5.1, to compute a G_k-module homomorphism f from $\mathcal{Z}^p(X^{\mathrm{sep}})$ to an (abstract) finitely generated G_k-module A means to compute

- a finite Galois extension k' of k,
- an explicit finitely generated $\mathrm{Gal}(k'/k)$-module A', and
- an algorithm that takes as input a finite separable extension L of k' and an element of $\mathcal{Z}^p(X_L)$ and returns an element of A',

such that there exists a k-embedding $k' \hookrightarrow k^{\mathrm{sep}}$ and an isomorphism $A' \xrightarrow{\sim} A$ such that the composition $\mathcal{Z}^p(X_L) \to A' \xrightarrow{\sim} A$ factors as $\mathcal{Z}^p(X_L) \to \mathcal{Z}^p(X^{\mathrm{sep}}) \xrightarrow{f} A$ for some (or equivalently, every) k'-embedding $L \hookrightarrow k^{\mathrm{sep}}$.

Remark 7.2. A similar definition can be made for G_k-module homomorphisms defined only on a G_k-submodule of $\mathcal{Z}^p(X^{\mathrm{sep}})$.

Remark 7.3. If k is a finitely generated field of characteristic 0, we can explicitly identify finite extensions of k with subfields of $\mathbb{C}$ consisting of computable numbers as follows. (To say that $z \in \mathbb{C}$ is computable means that there is an algorithm that given $n \in \mathbb{Z}_{\geqslant 1}$ returns an element $\alpha \in \mathbb{Q}(i)$ such that $|z - \alpha| < 1/n$.) Let $t_1, \ldots, t_n$ be a transcendence basis for k over $\mathbb{Q}$. Embed $\mathbb{Q}(t_1, \ldots, t_n)$ in $\mathbb{C}$ by mapping t_j to $\exp(2^{1/j})$; these are algebraically independent over $\mathbb{Q}$ by the Lindemann–Weierstrass theorem. As needed, embed finite extensions of $\mathbb{Q}(t_1, \ldots, t_n)$ (starting with k) into $\mathbb{C}$ by writing down the minimal polynomial of each new field generator over the subfield generated so far, together with an approximation to an appropriate root in $\mathbb{C}$ good enough to distinguish it from the other roots.

Remark 7.3 will be useful in relating étale cohomology over $\overline{k}$ to singular cohomology over $\mathbb{C}$.

7.2 Computability of étale cohomology

Hypothesis 7.4 (Cohomology is computable). There is an algorithm that takes as input (k, X, ℓ) as in Setup 5.1 and $i, n \in \mathbb{Z}_{\geqslant 0}$, and returns a finite G_k-module isomorphic to $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$.

Remark 7.5. Hypothesis 7.4 implies also that we can compute the Tate twist

$$\mathrm{H}^i(X^{\mathrm{sep}}, (\mathbb{Z}/\ell^n\mathbb{Z})(p)) \simeq \mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})(p)$$

for any $p \in \mathbb{Z}$.

We will prove Hypothesis 7.4 for k of characteristic 0 (Theorem 7.9). In arbitrary characteristic, we show only that we can 'approximate $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ from below' (Proposition 7.7), but as mentioned in the introduction, a proof of Hypothesis 7.4 in full has been announced [MO14, Théorème 0.9].

Following a suggestion of Lenny Taelman, we use étale Čech cocycles. By [Art71, Corollary 4.2], every element of $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ can be represented by a Čech cocycle for some étale cover. Any étale cover $\mathcal{U} = (U_j \to X^{\mathrm{sep}})_{j \in J}$ may be refined by one for which J is finite and the morphisms $U_j \to X^{\mathrm{sep}}$ are of finite presentation; from now on, we assume that all étale covers satisfy these finiteness conditions. Then we can enumerate all étale Čech cochains.

Fix a projective embedding of X. Choose an étale Čech cocycle representing the class of $\mathscr{O}_{X^{\mathrm{sep}}}(1)$ in $\mathrm{H}^1(X^{\mathrm{sep}}, \mathbb{G}_m)$. Using the Kummer sequence

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 0$$

compute its coboundary: this is a cocycle representing the class of a hyperplane section in $\mathrm{H}^2(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ (we ignore the Tate twist for now). Compute its d-fold cup product in the group $\mathrm{H}^{2d}(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n) \simeq \mathbb{Z}/\ell^n\mathbb{Z}$; this represents D times the class of a point, where D is the degree of X. If $\ell \nmid D$, we can multiply by the inverse of (D mod ℓ) to obtain the class of a point. In general, let ℓ^m be the highest power of ℓ dividing D; repeat the construction above to obtain a cocycle η_D representing D times the class of a point in $\mathrm{H}^{2d}(X^{\mathrm{sep}}, \mathbb{Z}/\ell^{m+n}\mathbb{Z}) \simeq \mathbb{Z}/\ell^{m+n}\mathbb{Z}$. Search for another cocycle η_1 in the same group such that $D\eta_1 - \eta_D$ is the coboundary of another cochain on some refinement. Eventually η_1 will be found, and reducing its values modulo ℓ^n yields a cocycle representing the class of a point in $\mathrm{H}^{2d}(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$.

Lemma 7.6. *There is an algorithm that takes as input (k, X, ℓ) as in Setup 5.1 and $i, n \in \mathbb{Z}_{\geqslant 0}$ and two étale Čech cocycles representing elements of $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n)$, and decides whether their classes are equal.*

Proof. We can subtract the cocycles, so it suffices to test whether a cocycle η represents 0. By day, search for a cochain on some refinement whose coboundary is η. By night, search for a cocycle η' representing a class in $\mathrm{H}^{2d-i}(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$, an integer $j \in \{1, 2, \ldots, \ell^n - 1\}$, and a cochain whose coboundary differs from $\eta \cup \eta'$ by j times the class of a point in $\mathrm{H}^{2d}(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ (see [Liu02, p. 194, Exercise 2.17] for an explicit formula for the cup product). The search by day terminates if the class of η is 0, and the search by night terminates if the class of η is nonzero, by Poincaré duality [SGA4$\frac{1}{2}$, p. 71, Théorème 3.1]. □

Proposition 7.7. *There is an algorithm that takes as input (k, X, ℓ) as in Setup 5.1 and integers $i, n \in \mathbb{Z}_{\geqslant 0}$ such that, when left running forever, it prints out an infinite sequence $\Lambda_0 \subset \Lambda_1 \subset \cdots$ of finite G_k-modules that stabilizes at a G_k-module isomorphic to $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$.*

Proof. By enumerating Čech cocycles, we represent more and more classes inside the group $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$. At any moment, we may construct the G_k-module structure of the finite subgroup generated by the classes found so far and their Galois conjugates, by using Lemma 7.6 to test which $\mathbb{Z}/\ell^n\mathbb{Z}$-combinations of them are 0. Eventually this G_k-module is the whole of $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ (even if we do not yet have a way to detect when this has happened). □

Proposition 7.8. *There is an algorithm that takes as input (k, X, ℓ) as in Setup 5.1 and integers $i, n \in \mathbb{Z}_{\geqslant 0}$, where k is of characteristic 0, and computes a finite abelian group isomorphic to the singular cohomology group $\mathrm{H}^i(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z})$ for some embedding $k \hookrightarrow \mathbb{C}$ as in Remark 7.3. Similarly, one can compute a finitely generated abelian group isomorphic to $\mathrm{H}^i(X(\mathbb{C}), \mathbb{Z})$.*

Proof. One approach is to embed X in some $\mathbb{P}^n_k$ and compose $X(\mathbb{C}) \to \mathbb{P}^n(\mathbb{C})$ with the Mannoury embedding [Man00]

$$\mathbb{P}^n(\mathbb{C}) \hookrightarrow \mathbb{R}^{(n+1)^2}$$
$$(z_0 : \cdots : z_n) \mapsto \left(\frac{z_i \bar{z}_j}{\sum_k z_k \bar{z}_k} : 0 \leqslant i, j \leqslant n \right)$$

to identify $X(\mathbb{C})$ with a semialgebraic subset of Euclidean space, and then to apply [BPR06, Remark 11.19(b) and the results it refers to] to compute a finite triangulation of $X(\mathbb{C})$, which yields the cohomology groups with coefficients in $\mathbb{Z}$ or $\mathbb{Z}/\ell^n\mathbb{Z}$. For an alternative approach, see [Sim08, § 2.5]. □

Theorem 7.9. *Hypothesis 7.4 restricted to characteristic 0 is true.*

Proof. Identify k with a subfield of $\mathbb{C}$ as in Remark 7.3. By the standard comparison theorem, the étale cohomology group $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ is isomorphic to the singular cohomology group $\mathrm{H}^i(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z})$. Use Proposition 7.8 to compute the size of the latter. Run the algorithm in Proposition 7.7 and stop once $\#\Lambda_j$ equals this integer. Then $\Lambda_j \simeq \mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$. □

COROLLARY 7.10. *Hypothesis 7.4 restricted to varieties in positive characteristic that lift to characteristic* 0 *is true.*

Proof. If X lifts to a nice variety $\mathcal{X}$ in characteristic 0, then we can search for a suitable $\mathcal{X}$ until we find one, and then compute the size of $\mathrm{H}^i(\mathcal{X}^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$, which is isomorphic to the desired group $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$. Then run the algorithm in Proposition 7.7 as before. □

Remark 7.11. Our approach to Theorem 7.9 above was partially inspired by an alternative approach communicated to us by Lenny Taelman. His idea, in place of Proposition 7.7, was to enumerate étale Čech cocycles and compute their images under a comparison isomorphism

$$\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{H}^i(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z})$$

explicitly (this assumes that given an étale morphism $U \to X^{\mathrm{sep}}$ one can compute compatible triangulations of $U(\mathbb{C})$ and $X(\mathbb{C})$). Eventually a set of cocycles mapping bijectively onto the group $\mathrm{H}^i(X(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z})$ will be found. The Galois action could then be computed by searching for coboundaries representing the difference of each Galois conjugate of each cocycle with some other cocycle in the set.

7.3 The Tate conjecture

See [Tat94] for a survey of the relationships between the following two conjectures and many others.

CONJECTURE $\mathrm{T}^p(X,\ell)$ [Tate conjecture]. Assume Setup 5.1. The cycle class homomorphism

$$\mathcal{Z}^p(X^{\mathrm{sep}}) \otimes \mathbb{Q}_\ell \to V^{\mathrm{Tate}}$$

is surjective.

CONJECTURE $\mathrm{E}^p(X,\ell)$ [Numerical equivalence equals homological equivalence]. Assume Setup 5.1. An element of $\mathcal{Z}^p(X^{\mathrm{sep}})$ is numerically equivalent to 0 if and only if its class in V is 0.

Remark 7.12. Conjecture $\mathrm{E}^1(X,\ell)$ holds (see [Tat94, p. 78]).

Given (k, X, p, ℓ) as in Setup 5.1, with k finite, let V_μ be the largest G-invariant subspace of V on which all eigenvalues of the Frobenius are roots of unity. We have $V^{\mathrm{Tate}} \leqslant V_\mu$.

PROPOSITION 7.13. *Fix X, p, and ℓ, and assume Conjecture $\mathrm{E}^p(X,\ell)$. Then the following integers are equal:*

(a) *the $\mathbb{Z}$-rank of the G_k-module $\mathrm{Num}^p X^{\mathrm{sep}}$,*
(b) *the $\mathbb{Z}$-rank of the image of $\mathcal{Z}^p(X^{\mathrm{sep}})$ in V, and*
(c) *the $\mathbb{Q}_\ell$-dimension of the image of $\mathcal{Z}^p(X^{\mathrm{sep}}) \otimes \mathbb{Q}_\ell$ in V.*

The integer in (c) is less than or equal to

(d) *the $\mathbb{Q}_\ell$-dimension of V^{Tate} and*
(e) *the $\mathbb{Z}_\ell$-rank of the G_k-module M of § 5,*

which, if k is finite, are less than or equal to

(f) *the $\mathbb{Q}_\ell$-dimension of V_μ.*

If, moreover, $\mathrm{T}^p(X,\ell)$ holds, then all the integers (including (f) if k is finite) are equal. Conversely, if (c) equals (d), then $\mathrm{T}^p(X,\ell)$ holds.

Proof. The only nontrivial statements are

- the equality of (b) and (c), which is [Tat94, Lemma 2.5], and
- the fact that $\mathrm{T}^p(X,\ell)$ and $\mathrm{E}^p(X,\ell)$ for k finite together imply the equality of (d) and (f); this follows from [Tat94, Theorem 2.9, (b)⇒(c)]. □

8. Algorithms

8.1 Computing rank and torsion of étale cohomology

Proposition 8.1. *There is an algorithm that takes as input a nice variety X over $\mathbb{F}_q$, and returns its zeta function*

$$Z_X(T) := \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} T^n\right) \in \mathbb{Q}(T).$$

Proof. From [Kat01, Corollary of Theorem 3], we obtain an upper bound B on the sum of the ℓ-adic Betti numbers $b_i(X)$. Then $Z_X(T)$ is a rational function of degree at most B. Compute $\#X(\mathbb{F}_{q^n})$ for $n \in \{1, 2, \ldots, 2B\}$; this determines the mod T^{2B+1} Taylor expansion of $Z_X(T)$, which is enough to determine $Z_X(T)$. □

Proposition 8.2. *There is an algorithm that takes as input a finitely generated field k and a nice variety X over k, and returns $b_0(X), \ldots, b_{2\dim X}(X)$.*

Proof. First assume that $k = \mathbb{F}_q$. Using Proposition 8.1, we compute the zeta function $Z_X(T)$. For each i, the Betti number $b_i(X)$ equals the number of complex poles of $Z_X(T)^{(-1)^i}$ with absolute value $q^{-i/2}$, counted with multiplicity; this number can be computed numerically since the absolute value of each zero or pole is an integer power of $\sqrt{q}$.

In the general case, we spread out X to a smooth projective scheme $\mathcal{X}$ over a finitely presented $\mathbb{Z}$-algebra $R = \mathbb{Z}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Search for a finite field $\mathbb{F}$ and a point $a \in \mathbb{F}^n$ satisfying $f_1(a) = \cdots = f_m(a) = 0$; eventually we will succeed; then $\mathbb{F}$ is an explicit R-algebra. Set $\mathcal{X}_\mathbb{F} = \mathcal{X} \times_R \mathbb{F}$. Standard specialization theorems (e.g., [SGA4$\frac{1}{2}$, V, Théorème 3.1]) imply that $b_i(X) = b_i(\mathcal{X}_\mathbb{F})$ for all i, so we reduce to the case of the previous paragraph. □

The following statement and proof were suggested by Olivier Wittenberg.

Proposition 8.3. *Assume Hypothesis 7.4. There is an algorithm that takes as input (k, X, ℓ) as in Setup 5.1 and an integer i and returns a finite group that is isomorphic to $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}_\ell)_{\mathrm{tors}}$.*

Proof. For each j, let $\mathrm{H}^j := \mathrm{H}^j(X^{\mathrm{sep}}, \mathbb{Z}_\ell)$. For integers j, n with $n \geqslant 0$, let $a_{j,n} := \#\mathrm{H}^j[\ell^n]$ and $b_j := b_j(X) = \dim_{\mathbb{Q}_\ell}(\mathrm{H}^j \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$. Since $\mathrm{H}^j_{\mathrm{tors}}$ is finite, $\#\mathrm{H}^j_{\mathrm{tors}}/\ell^n \mathrm{H}^j_{\mathrm{tors}} = \#\mathrm{H}^j_{\mathrm{tors}}[\ell^n] = a_{j,n}$, so $\#\mathrm{H}^j/\ell^n\mathrm{H}^j = \ell^{nb_j} \cdot a_{j,n}$. From Lemma 5.2 we find

$$\#\mathrm{H}^j(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z}) = \#\big(\mathrm{H}^j/\ell^n\mathrm{H}^j\big) \cdot \#\big(\mathrm{H}^{j+1}[\ell^n]\big) = \ell^{nb_j} \cdot a_{j,n} \cdot a_{j+1,n}. \tag{8.4}$$

The left side is computable by Hypothesis 7.4, and b_j is computable by Proposition 8.2. Since $a_{j,n} = 1$ for $j < 0$ and for $j > 2\dim X$, for any given n, we can use (8.4) to compute $a_{j,n}$ for all j, by ascending or descending induction. Compute

$$1 = a_{i,0} \leqslant a_{i,1} \leqslant a_{i,2} \leqslant \cdots \leqslant a_{i,N} \leqslant a_{i,N+1}$$

until $a_{i,N} = a_{i,N+1}$. Then $\mathrm{H}^i_{\mathrm{tors}}$ has exponent ℓ^N and $\mathrm{H}^i_{\mathrm{tors}}$ is isomorphic to $\bigoplus_{n=1}^N (\mathbb{Z}/\ell^n\mathbb{Z})^{r_n}$ with r_n such that $\ell^{r_n} a_{i,n-1} a_{i,n+1} = a_{i,n}^2$. □

Remark 8.5. The proof of Proposition 8.3 did not require the full strength of Hypothesis 7.4: computability of the group $\mathrm{H}^j(X^{\mathrm{sep}}, \mathbb{Z}/\ell^n\mathbb{Z})$ for all $j < i$ or for all $j \geqslant i$ would have sufficed.

Remark 8.6. If k is of characteristic 0 (or X lifts to characteristic 0), then combining Theorem 7.9 (or Corollary 7.10) with Proposition 8.3 lets us compute the group $\mathrm{H}^i(X^{\mathrm{sep}}, \mathbb{Z}_\ell)_{\mathrm{tors}}$ unconditionally.

8.2 Computing $\mathrm{Num}^p X^{\mathrm{sep}}$

Throughout this section, we assume Setup 5.1.

Lemma 8.7. *There is an algorithm that takes as input k, p, X, and cycles $y \in \mathscr{Z}^p(X)$ and $z \in \mathscr{Z}^{d-p}(X)$, and returns the intersection number $y.z$.*

Proof. First, if y and z are integral cycles intersecting transversely, use Gröbner bases to compute the degree of their intersection. If y and z are arbitrary cycles whose supports intersect transversely, use bilinearity to reduce to the previous sentence. In general, search for a rational equivalence between y and another p-cycle y' such that the supports of y' and z intersect transversely; eventually y' will be found; then apply the previous sentence to compute $y'.z$. □

Remark 8.8. It should be possible to make the algorithm in the proof of Lemma 8.7 much more efficient, by following a proof of Chow's moving lemma instead of finding y' by brute force enumeration.

Remark 8.9. Alternatively, if y and z are integral cycles of complementary dimension that do not necessarily intersect properly, their structure sheaves $\mathscr{O}_y$ and $\mathscr{O}_z$ admit resolutions $\mathscr{F}^\bullet$ and $\mathscr{G}^\bullet$ (complexes of locally free $\mathscr{O}_X$-modules), and then

$$y.z = \sum_{i,j \geqslant 0} (-1)^{i+j} \chi(\mathscr{F}^i \otimes \mathscr{G}^j); \tag{8.10}$$

this should lead to another algorithm. (Formula (8.10) can be explained as follows: replace y and z by rationally equivalent cycles y' and z' that intersect transversely; then, in $K(X)$,

$$\begin{aligned} \mathrm{cl}(\mathscr{O}_{y'} \otimes \mathscr{O}_{z'}) &= \mathrm{cl}(\mathscr{O}_{y'})\,\mathrm{cl}(\mathscr{O}_{z'}) \quad \text{(by [SGA6, p. 49, Proposition 2.7])} \\ &= \mathrm{cl}(\mathscr{O}_y)\,\mathrm{cl}(\mathscr{O}_z) \quad \text{(by [SGA6, p. 59, Corollaire 1], using } \dim y + \dim z = d) \\ &= \sum_{i \geqslant 0} (-1)^i\,\mathrm{cl}(\mathscr{F}^i) \sum_{j \geqslant 0} (-1)^j\,\mathrm{cl}(\mathscr{G}^j) \\ &= \sum_{i,j \geqslant 0} (-1)^{i+j}\,\mathrm{cl}(\mathscr{F}^i \otimes \mathscr{G}^j) \quad \text{(by [SGA6, p. 49, (2.15 bis)]).} \end{aligned}$$

Since $\mathscr{O}_{y'} \otimes \mathscr{O}_{z'}$ is a direct sum of skyscraper sheaves, applying $\chi\colon K(X) \to \mathbb{Z}$ yields $y'.z'$ on the left, which equals $y.z$.)

Similarly, one could prove the simpler but asymmetric formula $y.z = \sum_{i \geqslant 0} (-1)^i \chi(\mathscr{F}^i \otimes \mathscr{O}_z)$.

The following lemma describes a decision problem for which we do not have an algorithm that always terminates, but only a *one-sided* test, i.e., an algorithm that halts if the answer is YES, but runs forever without reaching a conclusion if the answer is NO.

Lemma 8.11. *There is an algorithm that takes as input k, p, X, a finite extension L of k, and a finite list of cycles $z_1, \dots, z_s \in \mathcal{Z}^p(X_L)$, and halts if and only if the images of $z_1, \dots, z_s$ in $\operatorname{Num}^p \overline{X}$ are $\mathbb{Z}$-independent.*

Proof. Enumerate s-tuples $(y_1, \dots, y_s)$ of elements of $\mathcal{Z}^{d-p}(X_{L'})$ as L' ranges over finite extensions of L. As each s-tuple is computed, compute also the intersection numbers $y_i.z_j \in \mathbb{Z}$ and halt if $\det(y_i.z_j) \neq 0$. □

Remark 8.12. If $p = 1$ and $d = 2$, and h is any ample divisor on X, and z is an integer combination of the h and the z_i, then the Hodge index theorem shows that the numerical class of z is 0 if and only if $z.h = 0$ and $z.z_j = 0$ for all j; thus the independence in Lemma 8.11 can be tested by calculating intersection numbers of already-known divisors without having to search for elements y_i. If $p = 1$ and $d > 2$, and we assume the Hodge standard conjecture [Got69, § 4, Conjecture Hdg(X)], then the numerical class of z is 0 if and only if $z.h^{d-1} = 0$ and $z.z_j.h^{d-2} = 0$ for all j; thus again the search for the y_j is unnecessary, conjecturally. A similar argument applies for higher p if we assume not only the Hodge standard conjecture but also that an algebraic cycle λ as in the Lefschetz standard conjecture [Got69, § 3, Conjecture $B(X)$] can be found algorithmically so that one can compute the primitive decomposition of z and the z_j before computing intersection numbers.

Remark 8.13. In Lemma 8.11, if L is separable over k, then it would be the same to ask for independence in $\operatorname{Num}^p X^{\mathrm{sep}}$, by Proposition 6.1(a).

Corollary 8.14. *There is an algorithm that takes as input k, p, and X, and that when left running forever, prints out an infinite sequence of nonnegative integers whose maximum equals $\operatorname{rk} \operatorname{Num}^p X^{\mathrm{sep}}$.*

Proof. Enumerate finite s-tuples $(z_1, \dots, z_s)$ of elements of $\mathcal{Z}^p(X_L)$ for all $s \geqslant 0$ and all finite separable extensions L of k, and run the algorithm of Lemma 8.11 (using Remark 8.13) on all of them in parallel, devoting a fraction 2^{-i} of the algorithm's time to the ith process. Each time one of the processes halts, print its value of s. □

Theorem 8.15 (Computing $\operatorname{Num}^p X^{\mathrm{sep}}$).

(a) *Assume Hypothesis 7.4. Then there is an algorithm that takes as input (k, X, p, ℓ) as in Setup 5.1 such that, assuming $\mathrm{E}^p(X, \ell)$,*

- *the algorithm terminates if and only if $\mathrm{T}^p(X, \ell)$ holds, and*
- *if the algorithm terminates, it returns $\operatorname{rk} \operatorname{Num}^p X^{\mathrm{sep}}$.*

(b) *There is an unconditional algorithm that takes k, p, X, and a nonnegative integer ρ as input, and computes the following, assuming that $\rho = \operatorname{rk} \operatorname{Num}^p X^{\mathrm{sep}}$:*

  (i) *a finitely generated torsion-free G_k-module N together with a G_k-equivariant injection $\operatorname{Num}^p X^{\mathrm{sep}} \hookrightarrow N$ with finite cokernel,*

  (ii) *the composition $\mathcal{Z}^p(X^{\mathrm{sep}}) \to \operatorname{Num}^p X^{\mathrm{sep}} \hookrightarrow N$ in the sense of Definition 7.1, and*

  (iii) *the rank of $\operatorname{Num}^p X$.*

Proof. (a) Let ℓ' be as in § 4. Use Hypothesis 7.4 to compute $T_{\ell'}$. Replace k by a finite Galois extension to assume that G_k acts trivially on $T_{\ell'}$. Let M and r be as in § 5.

Use the algorithm of Proposition 8.3 to compute an integer t such that $\ell^t T_{\text{tors}} = 0$. By day, use Hypothesis 7.4 to compute the groups T_{ℓ^n} for $n = t+1, t+2, \dots$, and the upper bounds $\lfloor \log \# T_{\ell^n}^G / \log \ell^{n-t} \rfloor$ on r given by Lemma 5.5(c). By night, compute lower bounds on $\operatorname{rk} \operatorname{Num}^p X^{\text{sep}}$ as in Corollary 8.14. Stop if the bounds ever match, which happens if and only if equality holds in the inequality $\operatorname{rk} \operatorname{Num}^p X^{\text{sep}} \leqslant r$, which by Proposition 7.13 happens if and only if $\mathrm{T}^p(X, \ell)$ holds. In this case, we have computed $\operatorname{rk} \operatorname{Num}^p X^{\text{sep}}$.

(b) (i) Search for a finite Galois extension k' of k, for p-cycles $y_1, \dots, y_s$, and for codimension p cycles $z_1, \dots, z_t$ over k' until the intersection matrix $(y_i.z_j)$ has rank ρ. The assumption $\rho = \operatorname{rk} \operatorname{Num}^p X^{\text{sep}}$ guarantees that such k', y_i, z_j will be found eventually. Let Y be the free abelian group with basis equal to the set consisting of the y_i and their Galois conjugates, so Y is a G_k-module. The intersection pairing defines a homomorphism $\phi\colon \operatorname{Num}^p X^{\text{sep}} \to \operatorname{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$ whose image has rank equal to $\rho = \operatorname{rk} \operatorname{Num}^p X^{\text{sep}}$. Since $\operatorname{Num}^p X^{\text{sep}}$ is torsion-free, ϕ is injective. Compute the saturation N of the $\mathbb{Z}$-span of $\phi(z_1), \dots, \phi(z_s)$ in $\operatorname{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$. Because of its rank, N equals the saturation of $\phi(\operatorname{Num}^p X^{\text{sep}})$. Thus N is a finitely generated torsion-free G_k-module containing a finite-index G_k-submodule $\phi(\operatorname{Num}^p X^{\text{sep}})$ isomorphic to $\operatorname{Num}^p X^{\text{sep}}$.

(ii) Given $z \in \mathcal{Z}^p(X_L)$ for some finite separable extension L of k', computing its intersection number with each basis element of Y yields the image of z in N.

(iii) Because of Proposition 6.1(b), $\operatorname{rk} \operatorname{Num}^p X = \operatorname{rk} N^{G_k}$, which is computable. □

Remark 8.16. If we can bound the exponent of $T_{\text{tors}} = \mathrm{H}^{2p}(X^{\text{sep}}, \mathbb{Z}_\ell)_{\text{tors}}$ without using Proposition 8.3, then Theorem 8.15(a) requires Hypothesis 7.4 only for $i = 2p$. In particular, this applies if $\operatorname{char} k = 0$ or if $\operatorname{char} k > 0$ and X lifts to characteristic 0, by Remark 8.6. Actually, if $\operatorname{char} k = 0$, we do not need Hypothesis 7.4 at all, because Theorem 7.9 says that it is true!

Remark 8.17. The analogue of Theorem 8.15 with X^{sep} replaced by $\overline{X}$ also holds, as we now explain. By Proposition 6.1(c), $\operatorname{Num}^p X^{\text{sep}}$ is of finite index in $\operatorname{Num}^p \overline{X}$, so in the proof of Theorem 8.15(b)(i), the homomorphism ϕ extends to a G_K-equivariant injective homomorphism $\overline{\phi}\colon \operatorname{Num}^p \overline{X} \to \operatorname{Hom}_{\mathbb{Z}}(Y, \mathbb{Z})$. Because of finite index, the image of $\overline{\phi}$ is contained in the N defined there. The cokernel of $\operatorname{Num}^p \overline{X} \to N$ is finite.

Remark 8.18. For each $p \in \{0, 1, \dots, d\}$, let N_p be the N in Theorem 8.15(b)(i), and define $Q_p := N_p \otimes \mathbb{Q}$. Then for any $p, q \in \mathbb{Z}_{\geqslant 0}$ with $p + q \leqslant d$, we can compute a bilinear pairing $Q_p \times Q_q \to Q_{p+q}$ that corresponds to the intersection pairing: indeed, each Q_p is spanned by classes of cycles, whose intersections in the Chow ring can be computed by an argument similar to that used to prove Lemma 8.7.

8.3 Checking algebraic equivalence of divisors

Lemma 8.19. *There is an algorithm that takes as input k, X, a finite extension L of k, and an element $z \in \mathcal{Z}^1(X_L)$, and halts if and only if z is algebraically equivalent to* 0.

Proof. Enumerate all possible descriptions of an algebraic family of divisors on X_L with a pair of L-points of the base (it is easy to check when such a description is valid), and check for each whether the difference of the cycles corresponding to the two points equals z. □

Lemma 8.20. *There is an algorithm that takes as input k, X, a finite extension L of k and $z \in \mathcal{Z}^1(X_L)$, and decides whether z lies in $\mathcal{Z}^1(X_L)^\tau$, i.e., whether the Néron–Severi class of z is torsion, i.e., whether z is numerically equivalent to* 0.

Proof. By day, search for a positive integer n and a family of divisors showing that nz is algebraically equivalent to 0. By night, run the algorithm of Lemma 8.11 for $s = 1$, which halts if and only if the image of z in $\operatorname{Num}^1 \overline{X}$ is nonzero, i.e., if and only if $z \notin \mathcal{Z}^1(X_L)^\tau$. One of these processes will halt. $\square$

8.4 Computing the Néron–Severi group

In this section, k is an *arbitrary* field.

Lemma 8.21.

(a) *Let X be a nice k-variety. There exists a divisor $B \in \mathcal{Z}^1_{X/k}$ such that for any ample divisor D, the class of $D + B$ is very ample.*

(b) *There is an algorithm that takes as input a finitely generated field k and a k-variety X and computes a B as in (a).*

Proof. Let K be a canonical divisor on X (this is computable if k is finitely generated). Let A be a very ample divisor on X (e.g., embed X in some projective space, and choose a hyperplane section). By [Kee08, Theorem 1.1(2)], $B := K + (\dim X + 1)A$ has the required property. $\square$

Given an effective Cartier divisor of X, we have an associated closed subscheme $Y \subseteq X$. Call a closed subscheme $Y \subseteq X$ a divisor if it arises this way. When we speak of the Hilbert polynomial of an effective Cartier divisor on a closed subscheme X of $\mathbb{P}^n$, we are referring to the Hilbert polynomial of the associated closed subscheme of X.

Lemma 8.22. *There is an algorithm that takes as input a finitely generated field k, a closed subscheme $X \subseteq \mathbb{P}^n_k$, and an effective divisor $D \subset X$, and computes the Hilbert polynomial of D.*

Proof. This is evident already from [Her26, Satz 2], which can be applied repeatedly to construct a minimal free resolution of $\mathscr{O}_D$. $\square$

Let $\operatorname{Hilb} X = \bigcup_P \operatorname{Hilb}_P X$ denote the Hilbert scheme of X, where P ranges over polynomials in $\mathbb{Q}[t]$.

Lemma 8.23. *There is an algorithm that takes as input a finitely generated field k, a closed subscheme $X \subseteq \mathbb{P}^n_k$, and a polynomial $P \in \mathbb{Q}[t]$, and computes the universal family $\mathcal{Y} \to \operatorname{Hilb}_P X$.*

Proof. This is a consequence of work of Gotzmann. Let $S = \bigoplus_{d \geqslant 0} S_d := k[x_0, \ldots, x_n]$, so $\operatorname{Proj} S = \mathbb{P}^n_k$. Given $d, r \in \mathbb{Z}_{\geqslant 0}$, let $\operatorname{Gr}_r(S_d)$ be the Grassmannian parametrizing r-dimensional subspaces of the k-vector space S_d. Then [Got78, § 3] (see also [IK99, Theorem C.29 and Corollary C.30]) specifies $d_0 \in \mathbb{Z}_{\geqslant 0}$ such that for $d \geqslant d_0$, one can compute $r \in \mathbb{Z}_{\geqslant 0}$ and a closed subscheme $W \subseteq \operatorname{Gr}_r(S_d)$ such that $W \simeq \operatorname{Hilb}_P \mathbb{P}^n$; under this isomorphism a subspace $V \subseteq S_d$ corresponds to the subscheme defined by the ideal I_V generated by the polynomials in V. Moreover, I_V and its saturation have the same dth graded part (see [IK99, Corollary C.18]).

Let $f_1, \ldots, f_m$ be generators of a homogeneous ideal defining X. Choose $d \in \mathbb{Z}$ such that $d \geqslant d_0$ and $d \geqslant \deg f_i$ for all i. Let $g_1, \ldots, g_M$ be all the polynomials obtained by multiplying each f_i by all monomials of degree $d - \deg f_i$. By the saturation statement above, $\operatorname{Proj}(S/I_V) \subseteq X$ if and only if $g_j \in V$ for all j. This lets us construct $\operatorname{Hilb}_P X$ as an explicit closed subscheme of $\operatorname{Hilb}_P \mathbb{P}^n$. Now $\operatorname{Hilb}_P X$ is known as an explicit subscheme of the Grassmannian, so we have explicit equations also for the universal family over it. $\square$

Lemma 8.24. *Let X be a nice k-variety. There exists an open and closed subscheme $\mathbf{EffDiv}_X \subseteq \operatorname{Hilb} X$ such that for any field extension $L \supseteq k$ and any $s \in (\operatorname{Hilb} X)(L)$, the closed subscheme of X_L corresponding to s is a divisor on X_L if and only if $s \in \mathbf{EffDiv}_X(L)$.*

Proof. See [BLR90, p. 215] for the definition of the functor $\mathbf{EffDiv}_X$ (denoted there by $\operatorname{Div}_{X/S}$ for $S = \operatorname{Spec} k$) and its representability by an open subscheme of $\operatorname{Hilb} X$. To see that it is also closed, we apply the valuative criterion for properness to the inclusion $\mathbf{EffDiv}_X \to \operatorname{Hilb} X$: if a k-scheme S is the spectrum of a discrete valuation ring and Z is a closed subscheme of $X \times S$ that is flat over S and the generic fiber Z_η of $Z \to S$ is a divisor, then Z equals the closure of Z_η in $X \times S$, which is an effective Weil divisor on $X \times S$ and hence a relative effective Cartier divisor since $X \times S$ is regular. □

The existence of the scheme $\mathbf{EffDiv}_X$ in Lemma 8.24 immediately implies the following.

Corollary 8.25. *Let X be a nice k-variety. Let Y be a closed subscheme of X. Let L be a field extension of k. Then Y is a divisor on X if and only if Y_L is a divisor on X_L.*

Remark 8.26. Corollary 8.25 holds more generally for any finite-type k-scheme X, as follows from fpqc descent applied to the ideal sheaf of $Y_L \subseteq X_L$.

Lemma 8.27. *There is an algorithm that takes as input a finitely generated field k, a smooth k-variety X, and a closed subscheme $Y \subseteq X$, and decides whether Y is a divisor in X.*

Proof. By [EGAIV(4), Proposition 21.7.2] or [Eis95, Theorem 11.8a.], Y is a divisor if and only if all associated primes of Y are of codimension 1 in X. So choose an affine cover (X_i) of X, compute the associated primes of the ideal of $Y \cap X_i$ in X_i for each i (the first algorithm was given in [Her26]), and check whether they all have codimension 1 in X_i (a modern method for computing dimension uses that the Hilbert polynomial of an ideal equals the Hilbert polynomial of an associated initial ideal, which can be computed from a Gröbner basis). □

Lemma 8.28. *Let $\pi\colon H \to P$ be a proper morphism of schemes of finite type over a field k. Suppose that the fibers of π are connected (in particular, nonempty). Then π induces a bijection on connected components.*

Proof. Let $H_1, \dots, H_n$ be the connected components of H. Let $P_i := \pi(H_i)$, so P_i is connected. Since π is proper, the P_i are closed. Since the fibers of π are connected, the P_i are disjoint. Since the fibers are nonempty, $\bigcup P_i = P$. Since the P_i are finite in number, they are open too, so they are the connected components of P. □

Let $\pi\colon \mathbf{EffDiv}_X \to \mathbf{Pic}_{X/k}$ be the proper morphism sending a divisor to its class. If $\mathbf{Pic}^c_{X/k}$ is a finite union of connected components of $\mathbf{Pic}_{X/k}$ and L is a field extension of k, let $\operatorname{Pic}^c X_L$ be the set of classes in $\operatorname{Pic} X_L$ such that the corresponding point of $(\mathbf{Pic}_{X/k})_L$ lies in $(\mathbf{Pic}^c_{X/k})_L$, and let $\operatorname{NS}^c X_L$ be the image of $\operatorname{Pic}^c X_L$ in $\operatorname{NS} X_L$.

Lemma 8.29.

(a) *Let X be a nice k-variety. Let $\mathbf{Pic}^c_{X/k}$ be any finite union of connected components of $\mathbf{Pic}_{X/k}$. Assume the following:*

For every field extension $L \supseteq k$, every divisor on X_L with class in $\operatorname{Pic}^c X_L$ is linearly equivalent to an effective divisor. (8.30)

Let $H := \pi^{-1}(\mathbf{Pic}^c_{X/k})$. Then $\pi\colon H(L) \to \operatorname{Pic} X_L$ induces a bijection

$$\{\text{connected components of } H_L \text{ that contain an } L\text{-point}\} \longrightarrow \operatorname{NS}^c X_L. \tag{8.31}$$

(b) *For any* $\mathbf{Pic}^c_{X/k}$ *as in (a), there is a divisor* F *on* X *such that the translate* $F + \mathbf{Pic}^c_{X/k}$ *satisfies (8.30).*

(c) *There is an algorithm that takes as input a finitely generated field* k*, a nice* k*-variety* X*, a divisor* $D \in \mathcal{Z}^1(X)$*, and a positive integer* e*, and computes the following for* $\mathbf{Pic}^c_{X/k}$ *defined as the (possibly empty) union of components of* $\mathbf{Pic}_{X/k}$ *corresponding to classes of divisors* E *over* $\overline{k}$ *such that* eE *is numerically equivalent to* D*:*

  (i) *a divisor* F *as in (b) for* $\mathbf{Pic}^c_{X/k}$*,*

  (ii) *the variety* H *in (a) for* $F + \mathbf{Pic}^c_{X/k}$*,*

  (iii) *the universal family* $Y \to H$ *of divisors corresponding to points of* H*,*

  (iv) *a finite separable extension* k' *of* k *and a finite subset* $\mathcal{S} \subseteq \mathcal{Z}^1(X_{k'})$ *such that there exists a* k*-homomorphism* $k' \hookrightarrow k^{\mathrm{sep}}$ *such that the composition*

$$\mathcal{Z}^1(X_{k'}) \to \mathcal{Z}^1(X^{\mathrm{sep}}) \to \operatorname{NS} X^{\mathrm{sep}}$$

  restricts to a bijection $\mathcal{S} \to \operatorname{NS}^c X^{\mathrm{sep}}$*.*

Proof. (a) Taking $L = \overline{k}$ in (8.30) shows that $H \xrightarrow{\pi} \mathbf{Pic}^c_{X/k}$ is surjective. The fibers of the map $\pi\colon H(L) \to \operatorname{Pic}^c X_L$ are linear systems, and are nonempty by (8.30), so the reduced geometric fibers of $\pi\colon H \to \mathbf{Pic}^c_{X/k}$ are projective spaces. In particular, $\pi_L\colon H_L \to (\mathbf{Pic}^c_{X/k})_L$ has connected fibers, so by Lemma 8.28, it induces a bijection on connected components. Under this bijection, the connected components of H_L that contain an L-point map to the connected components of $(\mathbf{Pic}^c_{X/k})_L$ containing the class of a divisor over L. The set of the latter components is $\operatorname{NS}^c X_L$.

(b) Let A be an ample divisor on X. For each of the finitely many geometric components C of $\mathbf{Pic}^c_{X/k}$, choose a divisor D_C on $X_{\overline{k}}$ whose class lies in C, and let $n_C \in \mathbb{Z}$ be such that $n_C A + D_C$ is ample. Let $n = \max n_C$, so $nA + D_C$ is ample for all C. Let B be as in Lemma 8.21(a). Let $F = B + nA$. If L is a field extension of k and E is a divisor on X_L with class in $\operatorname{Pic}^c X_L$, let C be the geometric component containing the class of $E_{\overline{L}}$ (for some compatible choice of $\overline{k} \subseteq \overline{L}$); then E is numerically equivalent to D, so $nA + E$ is ample too, so $F + E = B + (nA + E)$ is very ample by choice of B, so $F + E$ is linearly equivalent to an effective divisor.

(c) Fix a projective embedding of X, and let A be a hyperplane section.

(i) Let $n \in \mathbb{Z}_{>0}$ be such that $nA + D$ is ample. (To compute such an n, try $n = 1, 2, \ldots$ until $|nA + D|$ determines a closed immersion.) Compute B as in Lemma 8.21(b). Let $F = B + nA$. Suppose that L is an extension of k and E is a divisor on X_L such that eE is numerically equivalent to D. Then $e(nA + E)$ is numerically equivalent to $enA + D = (e-1)nA + (nA + D)$, which is a positive combination of the ample divisors A and $nA + D$, so $nA + E$ is ample. By choice of B, the divisor $F + E = B + (nA + E)$ is very ample and hence linearly equivalent to an effective divisor.

(ii) By the Riemann–Roch theorem, the Euler characteristic $\chi(F + sD + tA)$ is a polynomial $f(s, t)$ of total degree at most $d := \dim X$. For any $s \in \mathbb{Z}$, we can compute $t \in \mathbb{Z}$ such that $F + sD + tA$ is linearly equivalent to an effective divisor, whose Hilbert polynomial can be computed by Lemma 8.22, so the polynomial $\chi(F + sD + tA)$ can be found by interpolation. Let $P(t) := f(1/e, t)$. Compute the universal family $\mathcal{Y} \to \operatorname{Hilb}_P X$ as in Lemma 8.23.

Suppose that E is such that eE is numerically equivalent to D. Then the polynomial $\chi(F+sE+tA)$ equals $f(s/e, t)$ since its values match whenever $e|s$. In particular, $\chi(F+E+tA) = P(t)$; i.e., $P(t)$ is the Hilbert polynomial of an effective divisor linearly equivalent to $F+E$. Thus the subscheme $H \subseteq \mathbf{EffDiv}_X \subseteq \operatorname{Hilb} X$ is contained in $\operatorname{Hilb}_P X$, which is a union of connected components of $\operatorname{Hilb} X$. By definition, H is a union of connected components of $\mathbf{EffDiv}_X$, which by Lemma 8.24 is a union of connected components of $\operatorname{Hilb} X$, so H is a union of connected components of $\operatorname{Hilb}_P X$. To compute H, compute the (finitely many) connected components of $\operatorname{Hilb}_P X$; to check whether a component C belongs to H, choose a point h in C over some extension of k, apply Lemma 8.27 to $\mathcal{Y}_h$ to test whether $\mathcal{Y}_h$ is a divisor, and if so, apply Lemma 8.20 to $e\mathcal{Y}_h - D$ to check whether $e\mathcal{Y}_h$ is numerically equivalent to D.

(iii) Compute $Y \to H$ as the part of $\mathcal{Y} \to \operatorname{Hilb}_P X$ above H.

(iv) Compute the connected components of $H_{k^{\text{sep}}}$, which really means computing a finite separable extension k' and the connected components of $H_{k'}$ such that these components are geometrically connected. For each connected component C of $H_{k'}$, use the algorithm of [Har88] to decide whether it has a k^{sep}-point, and, if so, choose a k'-point h of C, enlarging k' if necessary, and take the fiber Y_h. Let $\mathcal{S}$ be the set of such divisors Y_h, one for each component C with a k^{sep}-point. By (a), the map $\mathcal{S} \to \operatorname{NS} X^{\text{sep}}$ is a bijection onto $\operatorname{NS}^c X^{\text{sep}}$. □

Theorem 8.32 (Computing $(\operatorname{NS} X^{\text{sep}})_{\text{tors}}$). *There is an algorithm that takes as input a finitely generated field k and a nice k-variety X, and computes the G_k-homomorphism*

$$\mathcal{Z}^1(X^{\text{sep}})^{\tau} \to (\operatorname{NS} X^{\text{sep}})_{\text{tors}}$$

sending a divisor to its Néron–Severi class, in the sense of Definition 7.1 and Remark 7.2.

Proof. Apply Lemma 8.29(c) with $D = 0$ and $e = 1$ to obtain a finite Galois extension k' and a subset $\mathcal{D} \subseteq \mathcal{Z}^1(X_{k'})$ mapping bijectively to $(\operatorname{NS} X^{\text{sep}})_{\text{tors}}$. For each pair $D_1, D_2 \in \mathcal{D}$, run Lemma 8.19 in parallel on $D_1 + D_2 - D_3$ for all $D_3 \in \mathcal{D}$ to find the unique D_3 algebraically equivalent to $D_1 + D_2$; this determines the group law on $\mathcal{D}$. Similarly compute the G_k-action. Similarly, given a finite separable extension L of k' and $z \in \mathcal{Z}^1(X_L)^{\tau}$, we can find the unique $D \in \mathcal{D}$ algebraically equivalent to z. □

If $\mathcal{D} \subseteq \mathcal{Z}^1(X_{k^{\text{sep}}})$, let $(\operatorname{NS} X^{\text{sep}})^{\mathcal{D}}$ be the saturation of the G_k-submodule generated by the image of $\mathcal{D}$ in $\operatorname{NS} X^{\text{sep}}$, and let $\mathcal{Z}^1(X^{\text{sep}})^{\mathcal{D}}$ be the set of divisors in $\mathcal{Z}^1(X^{\text{sep}})$ whose algebraic equivalence class lies in $(\operatorname{NS} X^{\text{sep}})^{\mathcal{D}}$.

Theorem 8.33 (Computing $\operatorname{NS} X^{\text{sep}}$).

(a) *Given a finitely generated field k, a nice k-variety X, a finite separable extension L of k in k^{sep} and a finite subset $\mathcal{D} \subseteq \mathcal{Z}^1(X_L)$, we can compute the G_k-homomorphism*

$$\mathcal{Z}^1(X^{\text{sep}})^{\mathcal{D}} \to (\operatorname{NS} X^{\text{sep}})^{\mathcal{D}}$$

in the sense of Definition 7.1 and Remark 7.2.

(b) *There is an algorithm that takes as input k and X as above and a nonnegative integer ρ, and computes the G_k-homomorphism $\mathcal{Z}^1(X^{\text{sep}}) \to (\operatorname{NS} X^{\text{sep}})$ in the sense of Definition 7.1 and Remark 7.2 assuming that $\rho = \operatorname{rk} \operatorname{NS} X^{\text{sep}}$.*

Remark 8.34. Assume Hypothesis 7.4 and $\mathrm{T}^1(X, \ell)$. (Conjecture $\mathrm{E}^1(X, \ell)$ is proved.) Then Theorem 8.15(a) lets us compute $\operatorname{rk} \operatorname{NS} X^{\text{sep}}$, so Theorem 8.33(b) lets us compute $\operatorname{NS} X^{\text{sep}}$. Recall also that Hypothesis 7.4 is true when restricted to characteristic 0 (Theorem 7.9) or varieties that lift to characteristic 0 (Corollary 7.10).

Proof of Theorem 8.33.

(a) Enlarge L to assume that it is Galois over k, and replace $\mathcal{D}$ by the union of its $\operatorname{Gal}(L/k)$-conjugates. There exist $D_1, \ldots, D_t \in \mathcal{D}$ whose images in $(\operatorname{Num}^1 X^{\text{sep}}) \otimes \mathbb{Q}$ form a $\mathbb{Q}$-basis for the image of the span of $\mathcal{D}$. Then there exist 1-dimensional cycles $E_1, \dots, E_t$ on X_L such that $\det(D_i.E_j) \neq 0$ (the E_i exist over a finite extension of L, but can be replaced by their traces down to L), and each $D \in \mathcal{D}$ has a positive integer multiple numerically equivalent to an element of the $\mathbb{Z}$-span of $\mathcal{D}$. Search for such $D_1, \dots, D_t, E_1, \dots, E_t$ and for numerical relations as above for each $D \in \mathcal{D}$ (use Lemma 8.20 to verify relations). Let $e := |\det(D_i \cdot E_j)|$. Let Δ be the span of the image of $\mathcal{D}$ in $\operatorname{Num}^1 X^{\mathrm{sep}}$. Let Δ' be the saturation of Δ in $\operatorname{Num}^1 X^{\mathrm{sep}}$. Then $(\Delta' : \Delta)$ divides e. For each coset of $e\Delta$ in Δ, choose a representative divisor D in the $\mathbb{Z}$-span of $\mathcal{D}$, and check whether the set $\mathcal{S}$ of Lemma 8.29(c) is nonempty to decide whether the numerical equivalence class of D is in $e\Delta'$; if so, choose a divisor in $\mathcal{S}$. The classes of these new divisors, together with those of $D_1, \dots, D_t$, generate Δ'. Moreover, we know the integer relations between all of these, so we can compute integer combinations $F_1, \dots, F_t$ whose classes form a *basis* for Δ'. Then

$$(\operatorname{NS} X^{\mathrm{sep}})^{\mathcal{D}} \simeq (\mathbb{Z}F_1 \oplus \cdots \oplus \mathbb{Z}F_t) \oplus (\operatorname{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$$

as abelian groups, and $(\operatorname{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$ can be computed by Theorem 8.32.

The homomorphism $\mathcal{Z}^1(X^{\mathrm{sep}})^{\mathcal{D}} \to (\operatorname{NS} X^{\mathrm{sep}})^{\mathcal{D}}$ is computed as follows: given any divisor $z \in \mathcal{Z}^1(X^{\mathrm{sep}})^{\mathcal{D}}$ (defined over some finite separable extension L' of L in k^{sep}), compute an integer combination F of the F_i such that $F.E_j = z.E_j$ for all j, and apply the homomorphism of Theorem 8.32 to compute the class of $z - F$ in $(\operatorname{NS} X^{\mathrm{sep}})_{\mathrm{tors}}$.

Applying this to all conjugates of our generators of $(\operatorname{NS} X^{\mathrm{sep}})^{\mathcal{D}}$ lets us compute the G_k-action on our model of $(\operatorname{NS} X^{\mathrm{sep}})^{\mathcal{D}}$.

(b) Assume that $\rho = \operatorname{rk} \operatorname{NS} X^{\mathrm{sep}}$. Then, for any divisors $D_1, \dots, D_\rho \in \mathcal{Z}^1(X^{\mathrm{sep}})$, their algebraic equivalence classes form a $\mathbb{Z}$-basis for a free subgroup of finite index in $\operatorname{NS} X^{\mathrm{sep}}$ if and only if there exist 1-cycles $E_1, \dots, E_\rho$ on X^{sep} such that $\det(D_i.E_j) \neq 0$. Search for a finite separable extension L of k in k^{sep}, divisors $D_1, \dots, D_\rho \in \mathcal{Z}^1(X_L)$, and 1-cycles $E_1, \dots, E_\rho$ on X_L until such are found with $\det(D_i.E_j) \neq 0$. Then apply (a) to $\mathcal{D} := \{D_1, \dots, D_\rho\}$. □

Remark 8.35. Theorems 8.32 and 8.33 hold for $\overline{X}$ instead of X^{sep}: the same proofs work, except that we need an algorithm for deciding whether a variety has a $\overline{k}$-point; fortunately, this is even easier than deciding whether a variety has a k^{sep}-point!

8.5 An alternative approach over finite fields

When k is a finite field, we can compute $\operatorname{rk} \operatorname{Num}^p X^{\mathrm{sep}}$ without assuming Hypothesis 7.4, but still assuming $\mathrm{T}^p(X, \ell)$ and $\mathrm{E}^p(X, \ell)$. The arguments in this section are mostly well known.

The following is a variant of Theorem 8.15(a). Recall that for any (k, X, p, ℓ) as in Setup 5.1 with k finite, we let V_μ denote the largest G-invariant subspace of $V = \mathrm{H}^{2p}(X^{\mathrm{sep}}, \mathbb{Q}_\ell(p))$ on which all eigenvalues of the Frobenius are roots of unity.

Theorem 8.36.

(a) *There is an algorithm A that takes as input (k, X, p, ℓ) as in Setup 5.1, with k a finite field $\mathbb{F}_q$, and returns* $\dim V_\mu$.

(b) *There is an algorithm B that takes as input (k, X, p, ℓ) as in Setup 5.1, with k a finite field $\mathbb{F}_q$, such that, assuming* $\mathrm{E}^p(X, \ell)$,

- *algorithm B terminates on this input if and only if* $\mathrm{T}^p(X, \ell)$ *holds, and*
- *if algorithm B terminates, it returns* $\operatorname{rk} \operatorname{Num}^p X^{\mathrm{sep}}$.

Proof.

(a) By Proposition 8.1 there is an algorithm that computes the zeta function $Z_X(T) \in \mathbb{Q}(T)$ of X. Then $\dim V_\mu$ is the number of complex poles λ of $Z_X(T)$ such that λ is a root of unity times q^{-p}, counted with multiplicity.

(b) Algorithm B first runs algorithm A to compute $v_\mu := \dim V_\mu$, and then runs the algorithm of Corollary 8.14 until it prints v_μ, in which case algorithm B returns v_μ. If $\mathrm{T}^p(X,\ell)$ and $\mathrm{E}^p(X,\ell)$ hold, Proposition 7.13 implies that v_μ equals $\operatorname{rk}\operatorname{Num}^p X^{\mathrm{sep}}$, and the algorithm of Corollary 8.14 eventually prints the latter, so algorithm B terminates with the correct output.

Assume $\mathrm{E}^p(X,\ell)$. Proposition 7.13 implies that $\operatorname{rk}\operatorname{Num}^p X^{\mathrm{sep}} \leqslant v_\mu$ with equality if and only if $\mathrm{T}^p(X,\ell)$ holds. So if algorithm B terminates, then $\mathrm{T}^p(X,\ell)$ holds. □

COROLLARY 8.37. *There is an algorithm to compute* $\mathrm{NS}\, X^{\mathrm{sep}}$ *(in the same sense as Theorem 8.33(b)) and its subgroup* $\mathrm{NS}\, X$ *for any nice variety* X *over a finite field such that* $\mathrm{T}^1(X,\ell)$ *holds for some* ℓ.

Proof. Apply Theorem 8.36(b), using that $\mathrm{E}^p(X,\ell)$ holds for $p=1$, to obtain $\operatorname{rk}\mathrm{NS}\, X^{\mathrm{sep}}$. Then Theorem 8.33(b) lets us compute the Galois module $\mathrm{NS}\, X^{\mathrm{sep}}$. By Proposition 6.2, computing its G_k-invariant subgroup yields $\mathrm{NS}\, X$. □

8.6 K3 surfaces

We now apply our results to K3 surfaces, to improve upon the results of [Cha14] and [HKT13] mentioned in § 2.

THEOREM 8.38. *There is an unconditional algorithm to compute the* G_k*-module* $\mathrm{NS}\, X^{\mathrm{sep}}$ *for any K3 surface* X *over a finitely generated field* k *of characteristic not* 2*. We can also compute the group* $(\mathrm{NS}\, X^{\mathrm{sep}})^{G_k}$*, in which* $\mathrm{NS}\, X$ *has finite index. If* k *is finite, we can compute* $\mathrm{NS}\, X$ *itself.*

Proof. By [Del81], K3 surfaces lift to characteristic 0. By [Mad14, Theorem 1], $\mathrm{T}^1(X,\ell)$ holds for any K3 surface X over a finitely generated field k of characteristic not 2. Hence Remark 8.34 lets us compute the G_k-module $\mathrm{NS}\, X^{\mathrm{sep}}$. From this we obtain $(\mathrm{NS}\, X^{\mathrm{sep}})^{G_k}$. By Proposition 6.1, $\mathrm{NS}\, X$ is of finite index in $(\mathrm{NS}\, X^{\mathrm{sep}})^{G_k}$. If k is finite, then $\mathrm{NS}\, X = (\mathrm{NS}\, X^{\mathrm{sep}})^{G_k}$ by Proposition 6.2. □

Remark 8.39. For K3 surfaces X over a finite field k of characteristic not 2, Corollary 8.37 yields another way to compute $\mathrm{NS}\, X^{\mathrm{sep}}$, without lifting to characteristic 0, but still using [Mad14, Theorem 1].

ACKNOWLEDGEMENTS

We thank Saugata Basu, François Charles, Bas Edixhoven, Robin Hartshorne, David Holmes, Moshe Jarden, János Kollár, Andrew Kresch, Martin Olsson, Lenny Taelman, Burt Totaro, David Vogan, Claire Voisin, Olivier Wittenberg, and the referee for helpful comments. We thank the Banff International Research Station, the American Institute of Mathematics, the Centre Interfacultaire Bernoulli, and the Mathematisches Forschungsinstitut Oberwolfach for their hospitality and support.

REFERENCES

And96 Y. André, *On the Shafarevich and Tate conjectures for hyper-Kähler varieties*, Math. Ann. **305** (1996), 205–248; doi:10.1007/BF01444219, MR 1391213 (97a:14010).

Art71 M. Artin, *On the joins of Hensel rings*, Adv. Math. **7** (1971), 282–296; MR 0289501 (44 #6690).

BPR06 S. Basu, R. Pollack and M.-F. Roy, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, second edition (Springer, Berlin, 2006); MR 2248869 (2007b:14125).

BLR90 S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21 (Springer, Berlin, 1990); MR 1045822 (91i:14034).

Cha13 F. Charles, *The Tate conjecture for $K3$ surfaces over finite fields*, Invent. Math. **194** (2013), 119–145; doi:10.1007/s00222-012-0443-y, MR 3103257.

Cha14 F. Charles, *On the Picard number of K3 surfaces over number fields*, Algebra Number Theory **8** (2014), 1–17; doi:10.2140/ant.2014.8.1, MR 3207577.

Del81 P. Deligne, *Relèvement des surfaces $K3$ en caractéristique nulle*, in *Algebraic surfaces*, Lecture Notes in Mathematics, vol. 868 (Springer, Berlin, 1981), 58–79 (in French). Prepared for publication by Luc Illusie; MR 638598 (83j:14034).

EGAIV(4) A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Publ. Math. Inst. Hautes Études Sci. 32 (1967), 361 (in French); MR 0238860 (39 #220).

Eis95 D. Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150 (Springer, New York, 1995); MR 1322960 (97a:13001).

EJ11a A.-S. Elsenhans and J. Jahnel, *The Picard group of a $K3$ surface and its reduction modulo p*, Algebra Number Theory **5** (2011), 1027–1040.

EJ11b A.-S. Elsenhans and J. Jahnel, *On the computation of the Picard group for $K3$ surfaces*, Math. Proc. Cambridge Philos. Soc. **151** (2011), 263–270; doi:10.1017/S0305004111000326, MR 2823134 (2012i:14015).

Got78 G. Gotzmann, *Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes*, Math. Z. **158** (1978), 61–70 (in German); MR 0480478 (58 #641).

Got69 A. Grothendieck, *Standard conjectures on algebraic cycles*, in *Algebraic geometry (Internat. Colloq. Tata Inst. Fund. Res. Bombay, 1968)* (Oxford University Press, London, 1969), 193–199; MR 0268189 (42 #3088).

Har88 D. Haran, *Quantifier elimination in separably closed fields of finite imperfectness degree*, J. Symbolic Logic **53** (1988), 463–469; doi:10.2307/2274518, MR 947853 (89i:03057).

HKT13 B. Hassett, A. Kresch and Y. Tschinkel, *Effective computation of Picard groups and Brauer–Manin obstructions of degree two $K3$ surfaces over number fields*, Rend. Circ. Mat. Palermo (2) **62** (2013), 137–151; doi:10.1007/s12215-013-0116-8, MR 3031574.

Her26 G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788 (in German); doi:10.1007/BF01206635, MR 1512302.

IK99 A. Iarrobino and V. Kanev, *Power sums, Gorenstein algebras, and determinantal loci*, Lecture Notes in Mathematics, vol. 1721 (Springer, Berlin, 1999), appendix C by Iarrobino and Steven L. Kleiman; MR 1735271 (2001d:14056).

Kah09 B. Kahn, *Démonstration géométrique du théorème de Lang-Néron et formules de Shioda–Tate*, in *Motives and algebraic cycles*, Fields Institute Communications, vol. 56 (American Mathematical Society, Providence, RI, 2009), 149–155 (French, with English and French summaries); MR 2562456 (2010j:14083).

Kat01 N. M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), 29–44. Dedicated to Professor Chao Ko on the occasion of his 90th birthday; MR 1803934 (2002d:14028).

Kee08 D. S. Keeler, *Fujita's conjecture and Frobenius amplitude*, Amer. J. Math. **130** (2008), 1327–1336; doi:10.1353/ajm.0.0015, MR 2450210 (2009i:14006).

Kle05 S. L. Kleiman, *The Picard scheme*, in *Fundamental algebraic geometry*, Mathematical Surveys and Monographs, vol. 123 (American Mathematical Society, Providence, RI, 2005), 235–321; MR 2223410.

Klo07 R. Kloosterman, *Elliptic K3 surfaces with geometric Mordell–Weil rank 15*, Canad. Math. Bull. **50** (2007), 215–226; doi:10.4153/CMB-2007-023-2, MR 2317444 (2008f:14055).

Lan56 S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563; MR 0086367 (19,174a).

Liu02 Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6 (Oxford University Press, Oxford, 2002), translated from the French by Reinie Erné; MR 1917232 (2003g:14001).

Mad14 K. Madapusi Pera, *The Tate conjecture for K3 surfaces in odd characteristic*, Invent. Math. (2014), doi:10.1007/s00222-014-0557-5.

MO14 D. A. Madore and F. Orgogozo, *Calculabilité de la cohomologie étale modulo ℓ*, Preprint (2014), arXiv:1304.5376v3.

Man00 G. Mannoury, *Surfaces-images*, Nieuw Arch. Wisk. (2) **4** (1900), 112–129.

Mau14 D. Maulik, *Supersingular K3 surfaces for large primes. With an appendix by Andrew Snowden*, Duke Math. J. **163** (2014), 2357–2425; doi:10.1215/00127094-2804783.

MP12 D. Maulik and B. Poonen, *Néron–Severi groups under specialization*, Duke Math. J. **161** (2012), 2167–2206; doi:10.1215/00127094-1699490, MR 2957700.

Mil80 J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33 (Princeton University Press, Princeton, NJ, 1980); MR 559531 (81j:14002).

Min87 H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. Reine Angew. Math. **101** (1887), 196–202.

Nér52 A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166 (in French); MR 0056951 (15,151a).

Nyg83 N. O. Nygaard, *The Tate conjecture for ordinary K3 surfaces over finite fields*, Invent. Math. **74** (1983), 213–237; doi:10.1007/BF01394314, MR 723215 (85h:14012).

Nyg85 N. Nygaard and A. Ogus, *Tate's conjecture for K3 surfaces of finite height*, Ann. of Math. (2) **122** (1985), 461–507; doi:10.2307/1971327, MR 819555 (87h:14014).

Ogu09 K. Oguiso, *Shioda–Tate formula for an abelian fibered variety and applications*, J. Korean Math. Soc. **46** (2009), 237–248; doi:10.4134/JKMS.2009.46.2.237, MR 2494474 (2009m:14011).

SGA4$\frac{1}{2}$ P. Deligne, *Cohomologie étale, Séminaire de Géométrie Algébrique du Bois-Marie (SGA 4$\frac{1}{2}$)*, Lecture Notes in Mathematics, vol. 569 (Springer, Berlin 1977); Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier; MR 0463174 (57 #3132).

SGA6 P. Berthelot, A. Grothendieck and L. Illusie, *Théorie des intersections et théorème de Riemann–Roch*, in *Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6)*, Lecture Notes in Mathematics, vol. 225 (Springer, Berlin, 1971); Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre (French); MR 0354655 (50 #7133).

Shi72 T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59; MR 0429918 (55 #2927).

Shi86 T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), 415–432; doi:10.2307/2374678, MR 833362 (87g:14033).

Shi90 T. Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Pauli **39** (1990), 211–240; MR 1081832 (91m:14056).

Sim08 C. Simpson, *Algebraic cycles from a computational point of view*, Theoret. Comput. Sci. **392** (2008), 128–140; doi:10.1016/j.tcs.2007.10.008, MR 2394989 (2008m:14021).

Tat76 J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274; MR 0429837 (55 #2847).

Tat94 J. Tate, *Conjectures on algebraic cycles in l-adic cohomology*, in *Motives (Seattle, WA, 1991)*, Proceedings of Symposia in Applied Mathematics, vol. 55 (American Mathematical Society, Providence, RI, 1994), 71–83; MR 1265523 (95a:14010).

Tat95 J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki **9** (1995), 415–440, Exp. No. 306; MR 1610977.

vanL07a R. van Luijk, *K3 surfaces with Picard number one and infinitely many rational points*, Algebra Number Theory **1** (2007), 1–15; MR 2322921 (2008d:14058).

vanL07b R. van Luijk, *An elliptic K3 surface associated to Heron triangles*, J. Number Theory **123** (2007), 92–119; doi:10.1016/j.jnt.2006.06.006, MR 2295433 (2007k:14077).

Vas98 W. V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, vol. 2 (Springer, Berlin, 1998); with chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman; MR 1484973 (99c:13048).

Bjorn Poonen poonen@math.mit.edu
Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, MA 02139-4307, USA

Damiano Testa adomani@gmail.com
Mathematics Institute, University of Warwick,
Coventry CV4 7AL, UK

Ronald van Luijk rvl@math.leidenuniv.nl
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA,
Leiden, The Netherlands