Generalized GCDs as Applications of Vojta's Conjecture

by

Nolan Robert Pyott

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2023

© Nolan Robert Pyott 2023

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Starting with an analysis of the result that for any coprime integers a and b, and some $\varepsilon > 0$, we have eventually that $\gcd(a^n - 1, b^n - 1) < a^{\varepsilon n}$ holds for all n, we are motivated to look for geometric reasons why this should hold. After some discussion on the general geometry and arithmetic needed to examine these questions, we take a quick look into how Vojta's conjectures provide a generalization of our first result. In particular, we also note a case where this implies a similar equality on particular elliptic curves.

Acknowledgments

First and foremost, I would like to thank my supervisor Professor David McKinnon for his essential guidance on this thesis. He enlightened my mathematical perspective on these topics considerably over many meetings and was always someone I knew could be relied upon. I'd also like to add a special thanks to my readers, Professors Jason Bell and Matthew Satriano, for their comments and suggestions, as well as bringing up interesting perspectives regarding this project. I'm very grateful as well for the support from coordinators Nancy Maloney and Jo-Ann Hardy in their assistance and information which helped me complete this milestone. I also extend my gratitude to the various staff and students who have helped me along my journey and cultivating my interest in research mathematics. On my list as well, I thank my colleagues at PostGrid for their understanding and accommodations as I worked to complete this thesis while continuing work. Lastly, I want to thank my girlfriend Angela for all of her emotional support throughout and helping to maintain our household when times were busy and sleep was short.

Table of Contents

1 Introduction

1.1 Overview

A persisting and fascinating example from which a lot of very difficult yet interesting questions may be asked is by considering integer sequences of the form $(d_n = a^n - b^n)_{n \geq 1}$ for some integers $a, b \in \mathbb{Z}$. From its very construction, some natural questions arise concerning divisibility given that $d_n | d_m$ whenever $n | m$, as well as the fact that for $b = 1$, the sequence $(a^n - 1)_{n \geq 1}$ is always one off from increasingly greater perfect power.

In a paper by Bugeaud, Corjava, and Zannier [BCZ02], the following interesting relationship between neighbouring sequences $a^n - 1$ and $b^n - 1$ is shown in regards to their greatest common divisor.

Theorem 1.1.1. *Given two multiplicatively independent integers $a, b \in \mathbb{Z}$ at least 2, and some $\varepsilon > 0$, we may eventually determine some $N \geq 1$ such that for $n \geq N$ thereafter*

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n).$$

When dealing with such sparse sequences, most methods of counting factors such as sieves will not suffice, and instead we turn towards Diophantine approximation. The proof produced by the authors here is first carried out with Schmidt's Subspace Theorem, which is a very powerful result in modern Diophantine approximation.

Our trick for analyzing these points will be to acknowledge that powers of integers fall into only so many primes, exactly the finite primes which divide our initial integers. From here, we are able to analyze the height relative to this finite set of primes and force a contradiction by using the tools of Diophantine geometry to conclude that infinitely many integers belong where only finitely many should be. This technique is standard such as the use of Roth's theorem on the so-called S-unit equation, or using Siegel's Theorem on elliptic curves to conclude finitely many integer points.

With this in mind, it is natural to explore generalizations of the [BCZ02] result to further geometries as well as related problems. One such tool which generalizes the Subspace Theorem and Siegel's Theorem is a main conjecture of Vojta. By using algebraic heights to relate GCDs and Vojta's conjecture, we will use blowups of projective space and products of elliptic curves to find various conditional results by Silverman. To obtain more context on Vojta's conjecture applied to blowups, we will mention McKinnon's paper to show a particular case of blowups of products of elliptic curves.

This thesis is heavy in background as most of the tools used by McKinnon and Silverman rely on the extensive machinery of algebraic geometry. Our first objective will be to cover the main definitions and theorems used to determine the canonical class on blowups and fibred products right from the definition of a sheaf. The machinery built up along the way will also be used to briefly cover Weil's height machine and some basic properties of the group law on elliptic curves.

1.2 An Initial Result

We begin this section by stating a special case of the Subspace Theorem, first introduced by Schmidt and generalized by Schlickewei to account for p-adic norms. While we will explore the p-adic norms later, it is enough for now to note that for any prime $p \in \mathbb{Z}$ we obtain a norm $|x|_p$ for any $x \in \mathbb{Q}$ by uniquely writing $x = p^k \frac{a}{b}$ with $a, b, k \in \mathbb{Z}$ and $\gcd(a, p) = \gcd(b, p) = \gcd(a, b) = 1$ and taking

$$|x|_p = p^{-k}.$$

It should also be clear by unique factorization that

$$|x| \cdot \prod_{p \text{ prime}} |x|_p = 1.$$

We sometimes write $|x|_\infty = |x|$ as our usual absolute value and collect all of these absolute values together into a set of places $M_{\mathbb{Q}}$. It should be noted that the real application to algebraic numbers would require us to define similar absolute values on algebraic extensions of $\mathbb{Q}$, which we will explore later. We now recount a simplification the Subspace Theorem from [Sch77] as stated in [BCZ02].

Theorem 1.2.1. *Let $S \subseteq M_{\mathbb{Q}}$ be a finite set of places, with $\infty \in S$ as to include the usual absolute value, and fix some integer $n \geq 1$. For each $v \in S$, take $L_{1,v}, \ldots, L_{n,v} : \mathbb{Q}^n \to \mathbb{Q}$ to be linearly independent set of linear forms. Fix some $\delta > 0$ and $C > 0$, and consider the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(x_1, \ldots, x_n)|_v < (\max_{1 \leq i \leq n} |x_i|)^{-\delta}.$$

Then the integer solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ with $\gcd(x_1, \ldots, x_n) = 1$ to the above inequality lie in finitely many hyperplanes of $\mathbb{Q}^n$.

Let's now go over the proof of the main result from [BCZ02].

Step 1: Setup

Let $a, b \in \mathbb{Z}$ be multiplicatively independent integers. For each $n \geq 1$, we may take $D_n = \gcd(a^n - 1, b^n - 1)$, and write

$$d_n = \frac{a^n - 1}{D_n}, \qquad c_n = \frac{b^n - 1}{D_n}.$$

With this, we clearly find for each $n \geq 1$

$$\frac{b^n - 1}{a^n - 1} = \frac{c_n}{d_n}.$$

Fixing some $\varepsilon > 0$, suppose for a contradiction that there is some infinite exceptional set E for which $n \in E$ implies that $D_n \geq a^{\epsilon n}$. Equivalently, note that this implies that $d_n \leq a^{(1-\varepsilon)n}$ for exceptional n, a fact that will be exploited by Diophantine approximation since our denominators will simply be too small for what we will ask of them.

To get this proof moving, we will need some extra variables to allow for more flexibility in our approach. For each $n, j \geq 1$, we also write

$$c_{n,j} = d_n \cdot \frac{b^{jn} - 1}{a^n - 1} = \frac{b^{jn} - 1}{D_n} = \frac{b^n - 1}{D_n} \sum_{i=0}^{j} b^{in} = c_n \sum_{i=0}^{j} b^{in}.$$

For the sake of convenience, we will write $z_{n,j} = c_{n,j}/d_n$.

Step 2: An initial bound

To lean us towards an approximation, we consider the series representation for each $n \geq 1$ as

$$\frac{1}{a^n - 1} = \frac{1}{a^n} \cdot \frac{1}{1 - (1/a)^n} = \frac{1}{a^n} \sum_{m=0}^{\infty} \frac{1}{a^{mn}} = \sum_{m=1}^{\infty} \frac{1}{a^{mn}}$$

We recall that for any $M \geq 1$, we have that the difference between the full series and the truncated series is

$$\begin{aligned} \frac{1}{a^n - 1} - \sum_{m=1}^{M} \frac{1}{a^{mn}} &= \sum_{m>M} \frac{1}{a^{mn}} \\ &= \frac{1}{a^{nM}} \sum_{m=1}^{\infty} \frac{1}{a^{mn}} \\ &= \frac{1}{a^{nM}(a^n - 1)} \\ &\ll \frac{1}{a^{n(M+1)}}. \end{aligned}$$

Multiplying this difference by $(b^{jn} - 1)$ for a given $j \geq 1$, we obtain an approximation for $z_{n,j}$ as

$$\left| \frac{b^{jn} - 1}{a^n - 1} - \sum_{m=1}^{M} \frac{b^{jn} - 1}{a^{mn}} \right| = \left| z_{n,j} - \sum_{m=1}^{M} \frac{b^{jn}}{a^{mn}} + \sum_{m=1}^{M} \frac{1}{a^{mn}} \right| \ll \frac{b^{jn}}{a^{n(M+1)}}.$$

Step 3: Trying Schmidt's Subspace Theorem

Moving towards the Subspace Theorem, notice that the previous approximation is a bound on a linear form in the variables $z_{n,j}$, b^{jn}/a^{mn}, and $1/a^{\ell n}$. Fixing a finite number J to only consider finitely many $1 \leq j \leq J$, consider the space $\mathbb{Q}^N$ for $N = J + M + JM$ and coordinates

$$\mathbb{Q}^N = \{(x_1, \ldots, x_N) = (z_1, \ldots, z_J, u_1, \ldots, u_M, v_{1,1}, \ldots, v_{J,M}) : z_j, u_m, v_{j,m}, x_i \in \mathbb{Q}\}.$$

For each $n \geq 1$, we consider the vector $\vec{x}_n \in \mathbb{Z}^N$ with coordinates

$$\vec{x}_n = d_n a^{Mn}(z_{n,1}, \ldots, z_{n,J}, \tfrac{1}{a^n}, \ldots, \tfrac{1}{a^{Mn}}, \tfrac{b^n}{a^n}, \ldots, \tfrac{b^{nJ}}{a^{Mn}}),$$

where precisely $z_j = z_{n,j}$, $u_m = 1/a^{mn}$, and $v_{j,m} = b^{jn}/a^{mn}$ for each $1 \leq j \leq J$ and $1 \leq m \leq M$. Note that the multiple of d_n clears the denominators of the first group of coordinates, and the multiple of a^{Mn} clears the denominators of the rest of the coordinates.

We may now also consider linear form for each $1 \leq j \leq J$

$$L_{j,\infty} = z_j + \sum_{m=1}^{M} u_M - \sum_{m=1}^{M} v_{j,m},$$

so that our bound form the previous step shows $|L_{j,\infty}(\vec{x}_n)|_\infty \ll d_n b^{jn}/a^n$ for any $n \geq 1$. Again towards the Subspace Theorem, it also follows that for any $n \geq 1$ we have

$$\prod_{1 \leq j \leq J} |L_{j,\infty}(\vec{x}_n)|_\infty \ll \frac{d_n^J b^{J^2 n}}{a^{Jn}}.$$

In order to apply our Subspace Theorem, note that we should have at least as many linear forms as the dimension of our input space. Just as in the case of Roth's Theorem as a special case, we will let the linear form $L_{i,\infty}$ for $i > J$ be given by $L_{i,\infty} = x_i$, accounting for the magnitude of the terms approximating $z_{n,j}$.

Clearly, all of our linear forms are linearly independent. But taking their product, we find for any $n \geq 1$ that

$$\begin{aligned}\prod_{1 \leq i \leq N} |L_{j,\infty}(\vec{x}_n)|_\infty &\ll \frac{d_n b^{J^2 n}}{a^{Jn}} \cdot \prod_{1 \leq m \leq M} |a^{n(M-m)}| \cdot \prod_{\substack{1 \leq m \leq M \\ 1 \leq j \leq J}} |b^{jn} a^{n(M-m)}| \\ &\ll \frac{d_n b^{J^2 n}}{a^{Jn}} \cdot a^{M^2 n} \cdot b^{J^2 M n} a^{JM^2 n} = d_n b^{J^2(M+1)n} a^{J(M^2-1)n}.\end{aligned}$$

Unfortunately, adding these extra linear forms shows that our approximation is not exceptional with respect to how large our inputs are, even once we apply our bound to d_n. However, this is only one norm for which our bound is not exceptional, but we will see that there are norms on which our approximation is very good.

Step 4: Applying Schlickewei's Subspace Theorem

With the previous shortcoming's in mind, let's consider the set of places $S \subseteq M_{\mathbb{Q}}$ containing the standard absolute value, but also containing the p-adic absolute values for each $p|ab$. For ease of notation, let's represent $S^0 \subseteq S$ as the set of places in S corresponding to a p-adic norm. For each $1 \leq i \leq N$ and $v \in S^0$, we will take $L_{i,v} = x_i$, which is clearly a linearly independent set of linear forms. Recall that exponents of a and b are very small under the p-adic norms for $p|ab$, so this will allow us to balance out our product relative to S.

Already, we may find that multiplying these linear forms balances out our product somewhat. Specifically, for $i > J$ and $n \geq 1$, we find that $L_{i,v}(\vec{x}_n) = d_n a^{mn} b^{jn}$ for some

$1 \leq m < M$ and $0 \leq j \leq J$ and so

$$\begin{aligned}\prod_{v \in S} |L_{i,v}(\vec{x}_n)|_v &= \prod_{v \in S} |d_n|_v \cdot |a^{mn} b^{jn}|_v \\ &= \left(\prod_{v \in S} |d_n|_v\right) \cdot \left(\prod_{v \in S} |a^{mn} b^{jn}|_v\right) \\ &= |d_n| \left(\prod_{p|ab} |d_n|_p\right) \cdot |a^{mn} b^{jn}| \left(\prod_{p|ab} |a^{mn} b^{jn}|_p\right) \\ &\leq d_n.\end{aligned}$$

Accounting for our remaining linear forms, for each $1 \leq j \leq J$, $v \in S^0$, and $n \geq 1$, we recall that $L_{j,v}(\vec{x}_n) = d_n z_{n,j} a^{Mn} = c_{n,j} a^{Mn}$, and so

$$\prod_{v \in S^0} |L_{j,v}(\vec{x})|_v = \prod_{p|ab} |c_{n,j}|_p |a^{Mn}|_p \leq \prod_{p|ab} |a^{Mn}|_p = \frac{1}{a^{Mn}}.$$

Putting each of these bounds of these products together, we obtain that our full product for $x \in E$, where we may assume $d_n \leq a^{(1-\varepsilon)n}$, is given by

$$\begin{aligned}\prod_{v \in S} \prod_{1 \leq i \leq N} |L_{i,v}(\vec{x}_n)|_v &= \prod_{1 \leq j \leq J} |L_{j,\infty}(\vec{x}_n)|_\infty \cdot \prod_{1 \leq j \leq J} \prod_{v \in S^0} |L_{j,v}(\vec{x}_n)|_v \cdot \prod_{J < i \leq N} \prod_{v \in S} |L_{i,v}(\vec{x}_n)|_v \\ &\ll \frac{d_n^J b^{J^2 n}}{a^{Jn}} \cdot \frac{1}{a^{JMn}} \cdot d_n^{N-J} \\ &\ll \frac{d_n^N b^{J^2 n}}{a^{J(M+1)n}} \\ &\ll \frac{a^{N(1-\varepsilon)n} b^{J^2 n}}{a^{(N-M)n}} \\ &\ll \left(b^{J^2} a^{M-\varepsilon N}\right)^n\end{aligned}$$

To keep simplifying, we are ready to fix choices of M and J. Ideally, we would like to choose J so that $M - \varepsilon N < J - M$, and then by choosing M for which $a^M > 2b^{J^2}a^J$ gives

$$\left(b^{J^2}a^{M-\varepsilon N}\right)^n < \left(b^{J^2}a^{J-M}\right)^n < \frac{1}{2^n}.$$

Fortunately, $J > \frac{2}{\varepsilon}$ will suffice since this gives

$$M - \varepsilon N < M + J - \varepsilon MJ < M + J - 2M = J - M.$$

To obtain a bound in the form of the Subspace Theorem, as the coordinates of $\vec{x}_n$ are given as rational polynomials in a^n, b^n, and d_n of degrees no more than $MJ+1$, and $d_n \leq a^n$ is true for $n \in E$, there is some constant $C > 1$ for which $\max_{1\leq i\leq N} |\vec{x}_n| < C^n$. Thus, by choosing $0 < \delta < \log 2/\log C$ we must have for all sufficiently large $n \in E$ that

$$\prod_{v\in S}\prod_{1\leq i\leq N} |L_{i,v}(\vec{x}_n)|_v < (\max_{1\leq i\leq N} |\vec{x}_n|)^{-\delta}.$$

Step 4: Too many integers, not enough hyperplanes

With the work of setting up the inequality from the Subspace Theorem completed, we may now reap the benefits of its conclusion. This means that the vectors $\vec{x}_n$ for $n \in E$ must lie in only finitely many hyperplanes of $\mathbb{Q}^N$. In particular, since E is infinite, there exists some infinite subset E' for which $\vec{x}_n$ all lie on some rational hyperplane H.

To derive a contradiction, we may explicitly write out our hyperplane as the equation

$$\sum_{j=1}^{J} \zeta_j z_j + \sum_{m=1}^{J} \alpha_1 u_1 + \sum_{j=1}^{J}\sum_{m=1}^{J} \beta_{j,m} v_{j,m} = 0,$$

with $\zeta_k, \alpha_m, \beta_{j,m} \in \mathbb{Q}$ for $1 \leq j \leq J$ and $1 \leq m \leq M$. Writing $\beta_{0,m} = \alpha_m$ for each $1 \leq m \leq M$, notice that we have for any $n \in E'$,

$$\sum_{j=1}^{J} \zeta_j \frac{b^{jn}-1}{a^n-1} + \sum_{\substack{0\leq j\leq J\\ 1\leq m\leq M}} \beta_{j,m} \frac{b^{jn}}{a^{mn}} = 0,$$

which follows easily by the coordinates of $\vec{x}_n$ and dividing out by $d_n a^{Mn}$. That is, the integer polynomial

$$F(x,y) = x^M \sum_{j=1}^{J} \zeta_j (y^j - 1) + (x-1) \sum_{\substack{0 \leq j \leq J \\ 0 \leq m < M}} \beta_{j,M-m} x^m y^j$$

has infinitely many roots along $\{(a^n, b^n) : n \in E'\}$. However, this must mean that $F(x,y) = 0$ since we'd otherwise find a finite set of coefficients $\alpha_{i,j} \in \mathbb{Q}$ for $1 \leq i, j \leq K$, such that for infinitely many $n \in E'$,

$$\sum_{1 \leq i,j, \leq K} \alpha_{i,j} a^{in} b^{jn} = 0.$$

Specifically, taking $1 \leq i_0, j_0 \leq k$ for which $\alpha i_0, j_0 \neq 0$ and $a^{i_0} b^{j_0} > a^i b^j$ for any $i_0 \neq i, j_0 \neq j$ and $\alpha_{i,j} \neq 0$, which may be done since we are assuming $a^i \neq b^j$ for all $i, j \geq 1$, we find

$$\lim_{n \to \infty} \frac{1}{(a^{i_0} b^{j_0})^n} \sum_{1 \leq i,j, \leq K} \alpha_{i,j} a^{in} b^{jn} = \alpha_{i_0, j_0},$$

contradicting the fact that we may always find some $n \in E'$ large enough for which the term is zero.

Using the fact that $F(x,y) = 0$, and $\gcd(x^M, x-1) = 1$, we must have

$$(x-1) | \sum_{j=1}^{J} \zeta_j (y^j - 1),$$

which is only possible if each coefficient is zero. Consequently, this must imply that $\beta_{j,M-m} = 0$ for each $0 \leq j \leq J$ and $0 \leq m < M$ as $(x-1) \neq 0$.

Finally, we have deduced a contradiction as our vectors $\vec{x}_n$ do not lie on the trivial hyperplane, granting us the desired result.

2 Geometry

2.1 Sheaves

We begin this section with the basic building block we will use for endowing the various geometrical spaces we will encounter with various rings of locally defined functions. We follow closely the work of [Har13] in their representation of the material.

Definition 2.1.1 (Presheaf)**.** A *presheaf* $\mathcal{F}$ on a topological space X is mapping on the open sets $U \mapsto \mathcal{F}(U)$, where the sets $\mathcal{F}(U)$ may either be groups, rings, modules, or objects in other categories. Importantly, given a containment of open sets $V \subseteq U$, there exists a restriction morphism $\rho_{V\to U} : \mathcal{F}(V) \to \mathcal{F}(U)$. As well, these groups (rings, modules, etc.) and restriction morphisms must satisfy:

1. $\mathcal{F}(\emptyset)$ is trivial,

2. $\rho_{U\to U}$ is the identity on $\mathcal{F}(U)$, and

3. Given the containment of open sets $W \subseteq V \subseteq U$, the restriction morphism from W to U is the composition of the other two restriction morphisms, captured by the diagram below.

$$\begin{tikzcd}
\mathcal{F}(W) \arrow[d, "\rho_{W\to V}"] \arrow[dr, bend left, "\rho_{W\to U}"] & \\
\mathcal{F}(V) \arrow[r, "\rho_{V\to U}"] & \mathcal{F}(U)
\end{tikzcd}$$

Some other notation we will encounter when dealing with presheaves is that the elements of each local group may be referred to as *sections* and we may alternatively use the notation $\Gamma(U, \mathcal{F})$ opposed to $\mathcal{F}(U)$. Also, with the idea of functions in mind, given a section $s \in \Gamma(U, \mathcal{F})$ and a containment of open sets $V \subseteq U \subseteq X$, we will almost always prefer to write $s|_V$ opposed to $\rho_{U\to V}(s)$ for the restriction of s.

Alongside this, we also want to consider maps between presheaves which, in some sense, respect the underlying algebra.

Definition 2.1.2 (Presheaf map)**.** Given two sheaves $\mathcal{F}$ and $\mathcal{G}$ on a space X, we may define a *map of presheaves* $\varphi : \mathcal{F} \to \mathcal{G}$ as a homomorphism $\varphi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ on each open set U which commutes with the restriction maps. This relationship is demonstrated with the diagram below for open sets $V \subseteq U \subseteq X$.

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\varphi(U)"] \arrow[d, "\rho_{\mathcal{F},U\to V}"] & \mathcal{G}(U) \arrow[d, "\rho_{\mathcal{G},U\to V}"] \\
\mathcal{F}(V) \arrow[r, "\varphi(V)"] & \mathcal{G}(V)
\end{tikzcd}$$

Composition of sheaf maps is given in the straightforward manner by composition on each underlying homomorphism. Such a mapping is considered an isomorphism when each homomorphism is itself an isomorphism. Also, when it is clear which open set a given section $s \in \mathcal{F}(U)$ belongs to, we may elect to write $\varphi(s)$ instead of the much more verbose $\varphi(U)(s)$.

While a presheaf satisfies the job of attaching local data to the various open subsets of our space, it doesn't have strong enough requirements to glue sections together or guarantee uniqueness.

Definition 2.1.3 (Sheaf)**.** A *sheaf* $\mathcal{F}$ on a topological space X is a presheaf which has certain local properties which mimic the usual notions of functions defined in an open neighbourhood. Specifically, these extra conditions are given as follows.

1. Given an open cover $\cup_{i\in I} U_i$ of some open subset $U \subseteq X$, if a section $s \in \mathcal{F}(U)$ satisfies $s|_{U_i} = 0 \in \mathcal{F}(U_i)$, then $s = 0$. That is, we may conclude that the local properties of each section uniquely determine the global properties.

2. Given an open cover $\cup_{i\in I} U_i$ of some open subset $U \subseteq X$, and some sections $s_i \in \mathcal{F}(U_i)$ for which $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$ for any $i, j \in I$, then there exists some section $s \in \mathcal{F}(U)$ such that $s_i = s|_{U_i}$. That is, given some sections defined on an open cover which agree on overlaps, we may always extend this to construct a section on the broader open subset.

One more key concept to keep in mind with a sheaf is the idea of the stalk. This is a set of local data to a particular point which is obtained by considering the sections on all open neighbourhoods of our point.

Definition 2.1.4 (Stalk)**.** Let $P \in X$ be some point and $\mathcal{F}$ a presheaf. We define the *stalk* $\mathcal{F}_P$ at the point P as the set of equivalence classes $\langle U, s\rangle$, with $U \subseteq X$ open containing P and $s \in \mathcal{F}(U)$. Two pairs $\langle U, s\rangle$ and $\langle V, t\rangle$ are said to be equivalent when there exists some open subset $W \subseteq U \cap V$ such that $s|_W = t|_W$.

Stalks are very useful tools since for a map of sheaves $\varphi : \mathcal{F} \to \mathcal{G}$ on a space X, we get an associated map of stalks $\varphi_P : \mathcal{F}_P \to \mathcal{G}_P$. With the associated maps, we find that φ is an isomorphism if and only if φ_P is an isomorphism for each $P \in X$. We will also say a sheaf morphism is injective (surjective) precisely when the associated map on the stalks is injective (surjective) for all $P \in X$. Note that our injectivity condition is equivalent to each map of sections being injective, but our surjectivity condition is not equivalent to each map of sections being surjective.

The power of sheaves is demonstrated with the following useful lemma. Note that sheaf restriction to an open set is done so in the obvious way.

Lemma 2.1.5 (Gluing sheaves)**.** *Consider an open cover $X = \cup_{i\in I} U_i$, with sheaves $\mathcal{F}_i$ on U_i for each $i \in I$. Suppose for each $i, j \in I$ there exists a sheaf isomorphism $\varphi_{ij} : \mathcal{F}_i|_{U_i \cap U_j} \to \mathcal{F}_j|_{U_i \cap U_j}$ which behaves nicely in the following ways for any indices $i, j, k \in I$:*

1. *φ_{ii} is the identity sheaf map.*

2. *$\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$ on the intersection $U_i \cap U_j \cap U_k$.*

Then there exists a sheaf $\mathcal{F}$ on X such that $\mathcal{F}_i = \mathcal{F}|_{U_i}$.

Proof. We may in fact show the sheaf in question directly. Given an open set $U \subseteq X$, we may define the sections as

$$\mathcal{F}(U) = \{(s_i)_{i\in I} \in \prod_{i\in I} \mathcal{F}_i(U_i \cap U) : \varphi_{i,j}(s_i|_{U_i\cap U_j \cap U}) = s_j|_{U_i \cap U_j \cap U} \forall i, j \in i\},$$

where the operations are done component wise. Clearly, by defining the restriction maps componentwise, we have a presheaf, so it remains is to validate the sheaf axioms.

Starting with our uniqueness axiom, let $V \subseteq X$ be arbitrary with open cover $V = \cup_{j \in J} V_j$. Suppose for some $s \in \mathcal{F}(V)$ that $s|_{V_j} = 0$ for each $j \in J$. To show that $s = (s_i)_{i \in I} = 0$, we notice that it suffices to show that each component of s is zero. For this, we recall that for each $i \in I$, that U_i and $\mathcal{F}_i$ form a sheaf and $U_i \cap V = \cup_{j \in J} U_i \cap V_j$ is an open cover. Thus, since $s|_{V_j} = 0$ for each $j \in J$, we find $s_i|_{U_i \cap V_j} = 0$ and so $s_i = 0$ by our sheaf axiom. Therefore, it must be that $s = 0$ as well.

Next, similarly take $V \subseteq X$ open with the same open cover as before. Suppose now that we are given some sections $s^{(j)} = (s_i^{(j)})_{i \in I} \in \mathcal{F}(V_j)$ for which $s^{(j)}|_{V_j \cap V_{j'}} = s^{(j')}|_{V_j \cap V_{j'}}$ for all $j, j' \in J$. As before, we wish to use our sheaf axioms to determine for each $i \in I$ some $s_i \in \mathcal{F}_i(U_i \cap V)$ so that for all $j \in J$,

$$(s_i)_{i \in I}|_{V_j} = s^{(j)} \iff s_i|_{U_i \cap V_j} = s_i^{(j)}.$$

As before, fixing $i \in I$, note that $\bigcup_{j \in J} U_i \cap V_j$ is an open cover of $U_i \cap V$. Thus, since for each $j, j' \in J$ we have $s^{(j)}|_{V_j \cap V_{j'}} = s^{(j')}|_{V_j \cap V_{j'}}$, we must then have

$$s_i^{(j)}|_{U_i \cap V_j \cap V_{j'}} = s_i^{(j')}|_{U_i \cap V_j \cap V_{j'}}.$$

Therefore, it follows that there exists some section $s_i \in \mathcal{F}(U_i \cap V)$ such that $s_i|_{U_i \cap V_j} = s_i^{(j)}$. Lastly, we also remark that for each $i, k \in I$ that $\varphi_{ik}(s_i|_{U_i \cap U_k \cap V}) = s_k|_{U_i \cap U_k \cap V})$. This is since $\cup_{j \in J} V_j \cap U_i \cap U_k$ is an open cover of $V \cap U_i \cap U_k$ and we have on each restriction $V_j \cap U_i \cap U_k$

that

$$\begin{aligned}\varphi_{ik}(s_i|_{U_i \cap U_k \cap V})|_{V_j \cap U_i \cap U_k} &= \varphi_{ik}(s_i^{(j)}|_{U_i \cap U_k \cap V_j}) \\ &= s_k^{(j)}|_{U_i \cap U_k \cap V_j} \\ &= (s_k|_{U_i \cap U_k \cap V})|_{V_j \cap U_i \cap U_k}.\end{aligned}$$

Finally, we also briefly mention why $\mathcal{F}_i \cong \mathcal{F}|_{U_i}$ for any particular $i \in I$. The isomorphism from $\mathcal{F}|_{U_i}$ to $\mathcal{F}_i$ is given by projection onto the corresponding coordinate. The mapping is clearly injective by the fact that the other components are given by isomorphisms on intersections. Also, the mapping is surjective since given $U \subseteq U_i$, if $s_i \in \mathcal{F}_i(U)$, then we can consider

$$(\varphi_{ik}(s_i|_{U \cap U_k}))_{k \in I} \in \mathcal{F}|_{U_i}(U),$$

which clearly projects onto our given section. □

While this clearly demonstrates the utility of the sheaf axioms, we are often left with only a presheaf. However, we may in fact uniquely extend any given presheaf to a sheaf by examining the stalks.

Theorem 2.1.6 (Sheaf associated to a presheaf)**.** *Let $\mathcal{F}$ be a presheaf on a topological space X. There exists a sheaf $\mathcal{F}^+$ and map $\theta : \mathcal{F} \to \mathcal{F}^+$, unique up to isomorphism, such that $\mathcal{F}_P \cong \mathcal{F}^+_P$ for any $P \in X$. Moreover, we have the following universal property.*

Given a sheaf $\mathcal{G}$ and a map $\varphi : \mathcal{F} \to \mathcal{G}$, there exists a unique morphism of sheaves $\psi : \mathcal{F}^+ \to \mathcal{G}$ such that the following diagram commutes.

$$\begin{tikzcd}\mathcal{F} \arrow[r, "\varphi"] \arrow[d, "\theta"] & \mathcal{G} \\ \mathcal{F}^+ \arrow[ur, "\psi"] & \end{tikzcd}$$

One way to view our associated sheaf is to define it as the gluing of sections from $\mathcal{F}$.

Fundamentally, we may represent our algebras as sets of the following form.

$$\mathcal{F}^+(U) = \{\{(U_i, s_i)\}_{i\in I} : U = \cup_{i\in I} U_i, s_i \in \mathcal{F}(U_i), s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}\}.$$

There is also an implicit equivalence relationship when two sets of pairs agree on all mutual overlaps. Note that restriction is done pairwise and we may simply discard any empty restrictions, while our algebra is done on intersection pairs between the two open covers. We also define our stalks to be given by taking any of the open set and section pairs. As they agree on overlaps, this is well-defined. For more details on the sheaf associated to the presheaf, we refer to Proposition-Definition II.1.2 of [Har13].

For one last important aspect of sheaves which we will make use of, consider two topological spaces X and Y with sheaves $\mathcal{F}$ and $\mathcal{G}$ respectively. Given a continuous map $f : X \to Y$, we are able to consider how $\mathcal{F}$ may act as a sheaf on Y and likewise for $\mathcal{G}$ on X.

We consider the *pushforward* $f_*\mathcal{F}$ on Y as for each $U \subseteq Y$, $(f_*\mathcal{F})(U) = \mathcal{F}(f^{-1}(U))$. Likewise, we are able to consider the *inverse image sheaf* $f^{-1}\mathcal{G}$ on X by the sheaf associated to the presheaf given below

$$U \mapsto \{(V, s) : f(U) \subseteq V, s \in \mathcal{G}(V)\}/\sim$$

with $(V, s) \sim (W, t)$ whenever there exists some open neighbourhood $O \subseteq V \cap W$ also containing $f(U)$ for which $s|_O = t|_O$.

2.2 Affine Schemes

Next, let's create a topological space for which a given ring will act like a space of functions. A natural place where functions and rings coincide are polynomial rings, and indeed this is a motivating example and basis for all of algebraic geometry with the so-called affine spaces.

Consider the polynomial ring $A = k[x_1, \ldots, x_n]$ for some algebraically closed field k and integer $n \geq 1$. Common sets of interest include the zero sets of some polynomials

$f_1, \dots, f_m \in A$. However, to speak of a zero set, it is not always clear what exactly this entails for general rings where the notion of "plugging-in" is not well-defined. For exactly these cases, it is convenient to note that a point $(a_1, \dots, a_n) \in \mathbb{A}_k^n$, where $\mathbb{A}_k^n$ can be regarded as k^n for now, is a common zero of our functions precisely when we have

$$f_1 \equiv \cdots \equiv f_m \equiv 0 \mod \langle x_1 - a_1, \dots, x_n - a_n \rangle.$$

In fact, even for the non-vanishing points of $\mathbb{A}_k^n$, it is easy to see that the value of a given polynomial $f(a_1, \dots, a_n)$ can be seen to be the unique representative in k modulo the ideal generated by the polynomials $a_1 - x_1, \dots, a_n - x_n \in A$. This can even be generalized to take an integer $n \in \mathbb{Z}$ and use it as a function on the primes of $\mathbb{Z}$ given by

$$p \mapsto n \mod p,$$

and n vanishes precisely at those p which divide it, or equivalently using ideals, when $(n) \subseteq (p)$.

We are now ready to define a topological space derived from a ring for which the ring itself will provide us a sheaf of functions.

Definition 2.2.1 (Zariski Topology)**.** Given a commutative ring A, we define the *spectrum of* A, written $\operatorname{Spec}(A)$, to be the set of all prime ideals of A. The *Zariski Topology* will be generated by open subsets given for $f \in A$ of the form

$$D_f = \{P \in \operatorname{Spec}(A) : f \notin P\},$$

or equivalently, with closed sets given by the ideals $I \subseteq A$ as

$$V(I) = \{P \in \operatorname{Spec}(A) : I \subseteq P\}.$$

Let's first explore our topology. Note that the sets D_f do in fact form a basis for a topology.

1. Given $P \in \operatorname{Spec}(A)$, we may find some $f \in A \setminus P$ so that $P \in D_f$.

2. For $f, g \in A$, we have $D_f \cap D_g = D_{fg}$ as for any $P \in \operatorname{Spec}(A)$, $fg \in P$ if and only if $f \in P$ or $g \in P$.

Examining our other topology, we see that the sets $V(I)$ do in fact form a system of closed sets since we may likewise check a few basic facts.

1. It is clear that $V(\langle 0 \rangle) = \operatorname{Spec}(A)$ and $V(A) = \emptyset$.

2. Given $I, J \subseteq A$, we find that $V(IJ) = V(I) \cup V(J)$, following from basic facts of prime ideals. Note that this implies $V(P)$ is an *irreducible closed set* in the topology as we cannot write $P = IJ$ non-trivially.

3. For a system of ideals I_j indexed by $j \in S$, $V(\sum_{j \in S} I_j) = \cap_{j \in S} V(I_j)$. This one is only slightly less obvious as clearly $\sum_{j \in S} I_j \subseteq P$ implies $V(I_j)$ contains P for all $j \in S$. Conversely, if $P \in V(I_j)$ for all $j \in S$, then as the smallest ideal containing each I_j, $\sum_{j \in S} I_j \subseteq P$.

We may also explain briefly why the two topologies given agree. Clearly, we have $D_f = \operatorname{Spec}(A) \setminus V((f))$ from reading definitions. Checking that the basis generates this topology as well, we may consider an arbitrary open subset $U = \operatorname{Spec}(A) \setminus V(I)$ from a given ideal $I \subseteq A$ and a point $P \in U$. We may then take any $f \in I \setminus P$ (non-empty or else $P \in V(I)$), such that $P \in D_f \subseteq U$.

In this case, we will refer to the closed sets as *algebraic sets* or *affine varieties.* Recall that $\operatorname{Spec}(A)$ is defined as the set of all prime ideals while $\mathbb{A}_k^n$ was originally defined by the tuples k^n. A *closed point* is some $P \in \operatorname{Spec}(A)$ such that $\overline{\{P\}} = \{P\}$. It is clear that the closed points of $\mathbb{A}_k^n$ will then be maximal ideals of A, and hence the following correspondence

$$(a_1, \ldots, a_n) \in k^n \rightleftharpoons \langle x_1 - a_1, \ldots, x_n - a_n \rangle \in \mathbb{A}_k^n.$$

For our other prime ideals which are not maximal, these will then correspond to irreducible algebraic sets as mentioned previously, such as curves or surfaces contained in $\mathbb{A}_k^n$ defined by algebraic equations. Under this correspondence, it is clear that our closed sets $V(I) \subseteq \mathbb{A}_k^n$ correspond to the points on which all polynomials in I vanish.

Next, we turn towards Hilbert's Nullstellensatz from Theorem 1.3A of [Har13].

Theorem 2.2.2 (Hilbert's Nullstellensatz)**.** *Consider the polynomial ring $A = k[x_1, \dots, x_n]$ over an algebraically closed field k. Let $I \subseteq A$ be an ideal and consider $V(I) \subseteq \mathbb{A}_k^n$. If $f \in A$ vanishes along $V(I)$, then $f^k \in I$ for some integer $k \geq 1$.*

In this context, if we find $g \in A$ vanishes only on a subset of $V(f)$, then f vanishes along $V(g)$ so $f^k \in \langle g \rangle$ for some $k \geq 1$. Therefore, we may write $f^k = gh$ for some $h \in A$ and

$$\frac{1}{g} = \frac{h}{gh} = \frac{h}{f^k}.$$

Hence, our ring of functions is exactly the functions whose denominators are powers of f. This may be expressed as the localization A_f of A by the multiplicative system $\{f^n\}_{n \geq 0}$.

This definition works well even on more general rings A. Thinking of restriction maps, consider $D_g \subseteq D_f \subseteq \operatorname{Spec}(A)$ for some $f, g \in A$. While it is obvious how to restrict $a \in A$ to $\frac{a}{1} \in A_f$, it is not as clear how to restrict A_f to A_g. Fortunately, we have the following chain of equivalences

$$D_g \subseteq D_f \iff V(f) \subseteq V(g) \iff \sqrt{\langle g \rangle} \subseteq \sqrt{\langle f \rangle},$$

where $\sqrt{I}$ is the radical of the ideal $I \subseteq A$, and we may use the following characterization from Corollary 2.21 of [Eis13],

$$\sqrt{I} = \bigcap_{\substack{P \in \operatorname{Spec}(A) \\ I \subseteq P}} P = \{a \in A : \exists n \geq 1, a^n \in I\}.$$

While the second equality is clear from the definition as an intersection of prime ideals, we also find from the other part of the definition that since $g \in \sqrt{\langle g \rangle}$, there must be some

$n \geq 1$ such that $g^n \in \langle f \rangle$. Writing $g^n = fh$, it is clear that $f \in A$ maps to a unit in A_g under the canonical ring homomorphism. Thus, we may use the universal property of localization to determine a unique ring homomorphism $A_f \to A_g$ such that the following diagram commutes.

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A_g \\
A_f \arrow[ur, dashed] &
\end{tikzcd}$$

Let's now examine what our expected stalks should be by considering the ring $\mathbb{Z}$. Taking $n \in \mathbb{Z}$ arbitrarily, we may consider n^{-1} defined as a function on the open set D_n since for any $(p) \in D_n$, n has a multiplicative inverse in the ring $\mathbb{Z}/p\mathbb{Z}$ by the fact $\gcd(n,p) = 1$. Thus, if we fix a prime p and examine all open basis sets D_n containing p, we find that the pair $\langle D_n, n^{-1} \rangle$ belongs to our stalk. After considering all such possibilities in this regard, we should expect our stalk to be

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus (p) \right\},$$

which is the localization of $\mathbb{Z}$ by the multiplicative system of integers not contained in (p).

With this, for an arbitrary ring A, we determine our sheaf of functions $\mathcal{O}_{\mathrm{Spec}(A)}$.

Theorem 2.2.3. *Given a ring A with $X = \mathrm{Spec}(A)$, there exists a unique sheaf of rings $\mathcal{O}_X$ referred to as the structure sheaf such that the following three properties hold.*

1. *Our global sections are the entire ring, given by $\mathcal{O}_X(X) \cong A$.*

2. *For any $f \in A$, $\mathcal{O}_X(D_f) \cong A_f$. The restriction map $\mathcal{O}_X(X) \to \mathcal{O}_X(D_f)$ is given by the canonical ring homomorphism $A \to A_f$, and likewise for $\mathcal{O}_X(D_f) \to \mathcal{O}_X(D_g)$ by $A_f \to A_g$ when $D_g \subseteq D_f$ for some $g \in A$.*

3. *For any $P \in X$, $\mathcal{O}_{X,P} \cong A_P$.*

Proof. Refer to Proposition II.2.2 of [Har13]. □

With the previous theorem from as the defining characteristics of our affine space, the best way to truly understand affine spaces is via maps between them. Indeed, there is a very natural way to interpret all the maps $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$, and this is through ring homomorphisms $B \to A$. Certainly, by following directly from the definition, if $\varphi : B \to A$ is a ring homomorphism, then $\varphi^{-1}(P) \subseteq B$ is a prime ideal whenever $P \subseteq A$ is a prime ideal. Moreover, for any distinguished open set $D_b \subseteq B$, it is clear that

$$\begin{aligned} P \in (\varphi^{-1})^{-1}(D_b) &\iff \varphi^{-1}(P) \in D_b \\ &\iff b \notin \varphi^{-1}(P) \\ &\iff \varphi(b) \notin P \\ &\iff P \in D_{\varphi(b)}, \end{aligned}$$

and hence $\varphi^{-1} : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ is continuous.

Let's consider a case that will be of interest and how these maps fit together with the geometry of the situation. Consider an algebraically closed field k and let A and B be finitely generated k-algebras with ring homomorphism $\varphi : B \to A$. Explicitly, for some integers $n, m \geq 1$, we consider surjective ring homomorphisms

$$\alpha : k[x_1, \ldots, x_n] \to A, \qquad \beta : k[y_1, \ldots, y_m] \to B.$$

Notice that we may understand the map φ entirely from how it acts on the images of $y_1, \ldots, y_m \in B$, where the quotient by the kernel of β is implicit. That is, for each $1 \leq i \leq m$, there is some function $f_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ for which

$$\varphi(y_i) = f_i(x_1, \ldots, x_n),$$

where again the quotient by the kernel of α is taken implicitly. Note that f_i may be taken equivalently up to the kernel of α and hence from the ring A under isomorphism, something we will note shortly.

Staying close to the geometry, let $P \in \mathrm{Spec} A$ be a maximal ideal, which corresponds to a maximal ideal of $k[x_1, \ldots, x_n]$ containing $\ker \alpha$. As discussed previously, this maximal ideal is generated by $x_i - a_i$ for $1 \leq i \leq n$. Therefore, we find that

$$\langle y_1 - f_1(a_1, \ldots, a_n), \ldots, y_m - f_m(a_1, \ldots, a_m) \rangle \subseteq \varphi^{-1}(P),$$

since $f_i(x_1, \ldots, x_n) - f_1(a_1, \ldots, a_n) \in P$. However, this containment is equality since the ideal on the left is a maximal ideal.

Therefore, we have seen in the fundamental case of maximal ideals of finitely generated k-algebras, that our functions $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ are actually given by the polynomial ring A, mapping

$$(a_1, \ldots, a_n) \in \mathrm{Spec}(A) \mapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)) \in \mathrm{Spec}(B).$$

Based on the previous example, we see that there is a good reason to believe that the spectrum of a quotient ring is a subspace. Consider the ring surjection $A \to A/I$, where $I \subseteq A$ is any ideal of the ring A. In this case, the map $\mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ is exactly the map which sends an ideal P/I to the ideal P, where $I \subseteq J \subseteq A$. It is an easy exercise to verify that all prime ideals of A/I are given in this form.

Note that this map is certainly injective as the ideal P/I is generated by the elements of P under the surjection $A \to A/I$, and hence $\mathrm{Spec}(A/I)$ can be viewed as a subspace of $\mathrm{Spec}(A)$. Furthermore, this subspace is also a closed set, as it is exactly $V(I) \subseteq \mathrm{Spec}(A)$. In this way, we see that we can recover all the closed subspaces of $\mathrm{Spec}(A)$, and we refer to the map $\mathrm{Spec}(A/I) \hookrightarrow \mathrm{Spec}(A)$ as a *closed immersion*.

Just as for closed sets, we too have inclusion for open sets defined by ring maps. Let $f \in A$ be arbitrary and consider the localization A_f with the canonical ring homomorphism $\varphi : A \to A_f$, which is the same as the restriction map $\mathcal{O}_X(X) \to \mathcal{O}_X(D_f)$ Since we know

$\mathcal{O}_X(D_f) \cong A_f$, we should expect $\operatorname{Spec}(A_f)$ to be bijective correspondence to $D_f \subseteq \operatorname{Spec}(A)$. Let $P \in \operatorname{Spec}(A_f)$ be a prime ideal. Immediately, we find $f^n \notin \varphi^{-1}(P)$ for any $n \geq 1$, or else P generates all of A_f by $\frac{1}{f^n} \cdot \frac{f^n}{1} = \frac{1}{1}$. From this, we may conclude that not only is $\varphi^{-1}(P) \in D_f$, but also that the for any element $\frac{a}{f^n} \in A_f$ represented by some $a \in A$ and $n \geq 1$, it is equivalent for $\frac{a}{f^n}$ to belong to P as it is for $\frac{a}{1}$ to belong to P, where the latter is also equivalent to the condition that a belongs to $\varphi^{-1}(P)$.

Thus, prime ideals of A_f are generated by elements in the image of the map $A \to A_f$, and so it is clear that $\operatorname{Spec}(A_f)$ is precisely D_f. The map $\operatorname{Spec}(A_f) \to \operatorname{Spec}(A)$ is therefore able to be seen as the inclusion, or specifically the *open immersion*, of $D_f \subseteq \operatorname{Spec}(A)$. In fact, for any open subset $U \subseteq \operatorname{Spec}(A)$, we may define the inclusion along U by restricting to distinguished open sets as these maps are certainly compatible on overlap.

Let's look at some further cases as to how these ring maps induce maps between the structure sheaves of our affine spaces. Let $f : X \to Y$ be given by a ring map $\varphi : B \to A$, where $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$. Take $U \subseteq \operatorname{Spec}(B)$ to be the distinguished open subset D_b for some $b \in B$, and recall from previous discussion that $f^{-1}(U) = D_{\varphi(b)}$. What we wish to consider is a map $f^{\#}(U) : \mathcal{O}_Y(U) \to f_*\mathcal{O}_X(U)$, so that we may ultimately construct a sheaf map $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$.

In this case, it is easy since $\mathcal{O}_Y(U) = B_b$ and $f_*\mathcal{O}_X(U) = A_{\varphi(b)}$ and we may define the map of rings $B_b \to A_{\varphi(b)}$ as simply

$$\frac{s}{b^k} \mapsto \frac{\varphi(s)}{\varphi(b)^k},$$

which is well-defined and injective when $\ker \varphi = 0$ by checking on equivalent fractions. Importantly, this definition agrees when you restrict to overlapping distinguished open subsets, and so we may indeed glue these maps together to form a sheaf map $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$.

Lastly, we may consider the stalks. Let $(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be as above and fix some prime $P \in \operatorname{Spec}(A)$. Just as before on distinguished open subsets, we obtain a map $f^{\#}_P : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ by applying φ to the numerator and denominator of the fractions in $B_{f(P)}$. Moreover, this is a *local homomorphism* since $(f^{\#}_P)^{-1}(PA_P) = f(P)B_{f(P)}$, sending the unique maximal ideal on one local ring to the unique maximal ideal of the other.

2.3 Schemes and Properties

With some sense to the geometry of the fundamental affine spaces, we are ready to consider the generalized concept of a scheme.

Definition 2.3.1 (Scheme)**.** An *affine scheme* is a space X with structure sheaf $\mathcal{O}_X$ which is isomorphic to $\operatorname{Spec}(A)$ and structure sheaf $\mathcal{O}_{\operatorname{Spec}(A)}$, in the sense that $\operatorname{Spec}(A)$ is homeomorphic to X and $\mathcal{O}_X$ is isomorphic to the pushforward of $\mathcal{O}_{\operatorname{Spec}(A)}$ as sheaves on X.

A *scheme* is a topological space X with sheaf of rings $\mathcal{O}_X$ such that for any point $P \in X$, there exists some open neighbourhood $U \subseteq X$ of P such that $(U, \mathcal{O}_X|_U)$ is an affine scheme.

A morphism of schemes $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $f : X \to Y$ and sheaf map $f^\# : \mathcal{O}_Y \to f_*\mathcal{O}_X$. Additionally, we require that when restricted to affine open subschemes $(U, \mathcal{O}_X|_U)$ and $(V, \mathcal{O}_Y|_V)$ such that $U \subseteq f^{-1}(V)$, that the restricted map $(f|_U, f^\#|_U) : (U, \mathcal{O}_X|_U) \to (V, \mathcal{O}_Y|_V)$ is given by a ring homomorphism $\Gamma(V, \mathcal{O}_Y|_V) \to \Gamma(U, \mathcal{O}_X|_U)$.

Let's consider our first fundamental example of a scheme which is not necessarily affine. Consider a graded ring $S = \bigoplus_{d\in\mathbb{Z}} S_d$, where for $d \in \mathbb{Z}$, S_d denotes an additive group of *homogeneous* elements of the same degree, and we require that $S_d \cdot S_e \subseteq S_{d+e}$ for any integers $d, e \in \mathbb{Z}$. We will also denote S_+ to be all elements of positive degree in S. Lastly, we will say that an ideal is a *homogeneous ideal* when it is generated by homogeneous elements.

With this, we define $\operatorname{Proj}(S)$ to be the space of all homogeneous prime ideals which do not contain all of S_+. To induce a topology on $\operatorname{Proj}(S)$, our closed sets will be given for each homogeneous ideal $I \subseteq S$ as

$$V_+(I) = \{P \in \operatorname{Proj}(S) : I \subseteq P\}.$$

Just as in the affine case, we have same familiar rules of arbitrary intersections and finite unions of these closed sets. Similarly, we also have distinguished open subsets given for each homogeneous element $f \in S_+$ as $D_+(f) = \mathrm{Proj}(S) \setminus V_+((f))$.

Let's now put a sheaf of rings on $\mathrm{Proj}(S)$ to define a scheme.

Theorem 2.3.2. *Let S be a graded ring and denote $\mathrm{Proj}(S)$. There exists a sheaf of rings $\mathcal{O}$ on $\mathrm{Proj}(S)$ satisfying the following:*

1. *$(\mathrm{Proj}(S), \mathcal{O})$ defines a scheme.*

2. *For any $P \in \mathrm{Proj}(S)$, $\mathcal{O}_{X,P} \cong S_{(P)}$, where $S_{(P)}$ is the subring of elements of degree zero in the localized graded ring S_P.*

3. *For any $f \in S_+$, we have $(D_+(f), \mathcal{O}_X|_{D_+(f)})$ is an affine scheme isomorphic to $\mathrm{Spec}(S_{(f)})$, where $S_{(f)}$ is the subring of S_f of elements of degree zero.*

Proof. Refer to Proposition II.2.5 of [Har13]. □

A very important example following from the previous theorem is projective space. Given some ring A, we define *projective n-space over A* to simply be

$$\mathbb{P}^n_A = \mathrm{Proj}(A[x_0, \ldots, x_n]).$$

Over our projective space, notice that for each $0 \leq i \leq n$, we may cover the entire space with affine patches

$$D_+(x_i) = \mathrm{Spec}(A[\tfrac{x_0}{x_i}, \ldots, \tfrac{x_n}{x_i}]).$$

Moreover, when considering $\mathbb{P}^n_k$ for an algebraically closed field k, the closed points of $\mathbb{P}^n_k$ are given by *homogeneous coordinates* $(a_0 : \cdots : a_n)$ corresponding to the maximal ideals

$$\langle a_i x_j - a_j x_i \rangle_{0 \leq i,j \leq n} \subseteq k[x_0, \ldots, x_n],$$

which is described locally on $D_+(x_i)$ for $0 \leq i \leq n$ as $(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}) \in \mathbb{A}^n_k$. Notice that in both cases our homogeneous coordinates are invariant to scaling by $\alpha \in k^*$. With the latter property, $\mathbb{P}^n_k$ is sometimes thought of as the space of lines through the origin in $\mathbb{A}^{n+1}_k$, and the open affine sets $D_+(x_i) \cong \mathbb{A}^n_k$ is the projection of each line onto the plane $\{x_i = 1\}$. Also under this interpretation, the lines contained within $\{x_i = 0\}$ that never intersect the plane are thought of as being contained in the hyperplane at infinity. This inspires an obvious interpretation, at least for the closed points, that for any $n \geq 1$,

$$\mathbb{P}^n_k = \mathbb{A}^n_k \cup \mathbb{P}^{n-1}_k = \mathbb{A}^n_k \cup \mathbb{A}^{n-1}_k \cup \cdots \cup \mathbb{A}^1_k \cup \mathbb{A}^0_k.$$

Moving on from projective space for now, let's consider the closed subschemes of $\text{Proj}(S)$ for a graded ring S. As before, consider a map $\varphi : S \to T$ which is surjective and preserves degree. Clearly, the preimage of homogeneous prime ideals in $\text{Proj}(T)$ will likewise be homogeneous prime ideals, and by surjectivity and degree preservation, any homogeneous prime ideal whose preimage contains all of S_+ must therefore contain all of T_+. Thus, we obtain a map $f : \text{Proj}(T) \to \text{Proj}(S)$ which is injective for the same reason as the affine case. We also obtain surjective maps on local rings and open affine pieces defined by ϕ, and so we see that $\text{Proj}(T) \cong \text{Proj}(S/\ker\varphi)$ is a closed subscheme identified with $V_+(\ker\varphi)$. These facts follow from Exercise II.2.14 and Exercise II.3.12 of [Har13].

So far, we've kept our schemes and rings quite general in our setup, but our examples are often finitely generated k-algebras for an algebraically closed field k. While these rings provide very nice geometric intuition in the ways we've just described, we can take some caution and state which properties of our rings and spaces we would like or require.

Another type of scheme we will look towards will be integral schemes. A scheme X, with structure sheaf $\mathcal{O}_X$, is said to be *integral* when $\mathcal{O}_X(U)$ is an integral domain for all open subsets $U \subseteq X$. We also note that $\text{Spec}A$ is integral if and only if A is an integral domain. To understand this further, let's take a quick look at some consequences of this.

The first deduction we can make is that an integral scheme X is *irreducible*, and not the union of any two proper closed subsets. Otherwise, we would be able to find the complements of these closed subsets, which we will denote as U and V, would necessarily have trivial intersection. Following the diagram below resulting from the open cover $X = U \cup V$,

$$\begin{tikzcd}
 & \mathcal{O}_X(U) \arrow[dr] & \\
\mathcal{O}_X(X) \arrow[ur] \arrow[dr] & & \mathcal{O}_X(U \cap V) = 0 \\
 & \mathcal{O}_X(V) \arrow[ur] &
\end{tikzcd}$$

we must have that $\mathcal{O}_X(X) \cong \mathcal{O}_X(U) \times \mathcal{O}_X(V)$, which is certainly not an integral domain, with the restriction maps granting the isomorphism $s \mapsto (s|_U, s|_V)$. By applying our sheaf axiom regarding the vanishing of a global section with respect to vanishing of local sections this open cover, it is clear why the proposed map is injective. Likewise, using the sheaf axiom regarding the existence of a global section from local sections, this open cover with trivial overlap also explains why the map is surjective.

Note that irreducibility of a closed subset $Z \subseteq X$ implies that it has a *generic point*. By taking $U \cong \operatorname{Spec}(A) \subseteq Z$ which is open affine, we may consider the nilpotent elements of the ring $\eta = \sqrt{(0)}$. This ideal must be prime as $ab \in \eta$ means $U = V(a) \cup V(b)$, and so one of a or b is an element of every prime ideal of A by irreducibility. By definition, the set $\{\eta\}$ is dense in U. Going one step further, since we know $U \cap V \neq \emptyset$ for all open subsets $V \subseteq X$, it follows that $\{\eta\}$ is dense in X as well. This point is also unique since being dense in U necessitates being the radical of A.

Resuming our discussion on integral schemes, another deduction we can make is that X is *reduced*. That is, for any $P \in X$, $\mathcal{O}_{X,P}$ has no nilpotent elements. By taking an affine neighbourhood of any point, we can immediately see this holds. Additionally, when X is both reduced and irreducible, we notice that the generic point corresponds to just the trivial ideal of each open affine subset, or else we would be able to find some $P \in X$ for which $\mathcal{O}_{X,P}$ has nilpotent elements. As this holds over any affine open subscheme of X, for any $U \subseteq X$, $fg = 0$ over $\mathcal{O}_X(U)$ grants the same relationship on every affine subset of U. Therefore, by partitioning our open cover $\mathcal{V}$ of open affine subsets of V, we find

$$\left(\bigcup_{\substack{V\in\mathcal{V}\\ f|_V=0}} V\right)\cap\left(\bigcup_{\substack{V\in\mathcal{V}\\ f|_V\neq 0}} V\right)=\emptyset$$

and so it follows by irreducibility one of the two must be the empty set and the other all of U. When the condition $f|_V = 0$ holds for all $V \in \mathcal{V}$, then $f = 0$ and we are done. Otherwise, since $V \in \mathcal{V}$ is integral, $g|_V = 0$ for every open affine subset, and then $g = 0$ as desired.

We summarize this discussion in the following proposition.

Proposition 2.3.3. *A scheme X is integral if and only X is both reduced and irreducible. Moreover, an affine scheme is integral if and only if the defining ring is an integral domain.*

Proof. See previous discussion above, as well as Proposition II.3.1 of [Har13] □

One last aspect of integrality we will enjoy is the notion of a fraction field for the entire scheme. Indeed, taking an affine subset $U \cong \text{Spec}A$ of an integral scheme X, which is necessarily an integral domain, we may localize at the prime ideal (0) and obtain a field of fractions. As before, this ideal corresponds to the generic point $\eta \in X$, we obtain the same field $\mathcal{O}_{X,\eta}$ regardless of choice of affine subset.

Next, let's consider the property of being noetherian, which applies both to spaces and to rings. For our space X, a *noetherian topological space* is defined by the descending chain condition. That is, for any family closed subsets $(Y_n)_{n\geq 1}$, satisfying the following descending chain condition,

$$Y_1 \supseteq Y_2 \supseteq \cdots,$$

then it must be the case that there is some sufficiently large N for which $Y_N = Y_n$ for all $n \geq N$ thereafter. An interesting consequence is that any closed subset of a noetherian topological space can be covered uniquely by a finite number of irreducible closed subsets.

We may also define the *dimension* of X as a topological space as the supremum of such chains with distinct closed sets strictly contained in X by

$$\dim X = \sup\{n : X \supsetneq Y_1 \supsetneq \cdots \supsetneq Y_n\}.$$

If we fix some closed subset $Z \subseteq X$, then the *codimension* is defined by the supremum of lengths of descending chains strictly contained in X, ending with Z, and no two closed subsets are equal. This definition can be extended to any other subset $Y \subseteq X$ by considering the infimum of $\operatorname{codim}(Z, X)$ for all closed subsets $Z \subseteq Y$.

For our rings, a *noetherian ring* is one for which all ideals are finitely generated. Equivalently, it is a ring that satisfies an ascending chain condition (section 1.4 of [Eis13]). Specifically, for a noetherian ring A, that for a family of ideals $(I_n)_{n\geq 1}$ such that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

then it must be the case that there is some sufficiently large N for which $I_N = I_n$ for all $n \geq N$ thereafter.

For any prime ideal $P \in \operatorname{Spec}(A)$, we may take its *height* as the supremum of the lengths of chains strictly contained within P. We also define the *Krull dimension* of A by the supremum of all heights of prime ideals.

With so many similarities, it does not come across as a surprise that these notions coincide. We summarize the relationships between our terminology in the following proposition.

Proposition 2.3.4. *Let $X = \operatorname{Spec} A$ be an affine scheme.*

1. *The dimension of X as a topological space is the same as the Krull dimension of A.*

2. *X is noetherian if and only if A is noetherian.*

3. *If we suppose further that A is an integral domain, which is also a finitely generated*

k-algebra, then for any closed irreducible subset $V(P) \cong \operatorname{Spec}(A/P)$,

$$\dim V(P) + \operatorname{codim}(X, V(P)) = \dim(A/P) + \operatorname{ht}(P) = \dim X,$$

where the two sums are equal term wise.

Proof. We refer to Propostion II.3.2 of [Har13], Corollary 13.4 of [Eis13], and our characterization of the irreducible closed subsets of an affine space as the closures of prime ideals. □

To explain some further properties, we will examine relative schemes and relatively valued points.

Definition 2.3.5. A scheme X is said to be a *scheme over* Y when there exists a morphism $X \to Y$. We will often write X/Y to denote this, or X/A when $Y = \operatorname{Spec}(A)$ for some ring A.

This generally captures the notion that the defining equations and algebras of our scheme are drawn from the rings associated to Y. Notably, since there is a canonical map $\mathbb{Z} \to A$ for any ring A, any affine scheme is over $\mathbb{Z}$ and thus all schemes when gluing is accounted for. This follows from exercise 7.3.G of [Vak22].

Definition 2.3.6. Given schemes X and Z, a Z*-valued* point on X is a morphism $Z \to X$. The space of Z-valued points on X is denoted $X(Z)$. Moreover, when $Z = \operatorname{Spec}(k)$ for a field k, we refer these points as k*-rational* (or rational when $k = \mathbb{Q}$), and write $X(k)$.

To make sense of this, for a k-rational point $f : \operatorname{Spec}(k) \to X$, the unique prime ideal of $\operatorname{Spec}(k)$ is sent to some point $P \in X$, so we would like to think of P as the rational point itself. However, the image in X is not enough to characterize our rational point, as we also have an associated map of sheaves $\mathcal{O}_X \to f_*\mathcal{O}_k$.

To understand this sheaf map, for any $U \subseteq X$, it is clear that $f_*\mathcal{O}_k(U) = k$ when $P \in U$, and $f_*\mathcal{O}_k(U) = 0$ otherwise. Moreover, this map is characterized by the map $\mathcal{O}_{X,P} \to k$ since sheaf maps commute with restriction homomorphisms.

To further dive into this map on the local ring $\mathcal{O}_{X,P}$, we recall that the local ring $\mathcal{O}_{X,P}$ has a unique maximal ideal denoted $\mathfrak{m}_P$. And so we may define the *residue field* $\kappa(P) = \mathcal{O}_{X,P}/\mathfrak{m}_P$. Since we require this to be a local homomorphism, it should be immediate that the kernel of $\mathcal{O}_{X,P} \to k$ is exactly $\mathfrak{m}_P$, and so the map $\kappa(P) \to k$ is an inclusion. This therefore characterizes our rational points.

Examining the residue field for a given point $P \in X$, consider the $\mathcal{O}_{X,P}$ module $\mathfrak{m}_P/\mathfrak{m}_P^2$. As the elements of $\mathfrak{m}_P$ vanish under multiplication, we in-fact have a well-defined $\kappa(P)$-vector space. For the affine variety $V(f_1, \ldots, f_n) \subseteq \mathbb{A}_k^n$, notice that there is a correspondence between the Jacobian $(\partial f_i/\partial x_j)_{i,j}$ and the vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$.

Definition 2.3.7. Given a connected scheme X and a point $P \in X$, we say that P is *regular* if

$$\dim_{\kappa(P)} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim X.$$

If all the points of X are regular, we that X is a *regular scheme*, or X is *non-singular*.

For one last construction essential to our geometry, we come to the product of schemes. Consider for example some ring homomorphisms $f : C \to A$ and $g : C \to A$ for some rings A, B, and C. With these, note that we may also define morphisms $A \to A \otimes_C B$ and $B \to A \otimes_C B$ by

$$a \in A \mapsto a \otimes 1 \qquad b \in B \mapsto 1 \otimes b.$$

With these ring maps, suppose for a fourth ring R that we have homomorphisms $\alpha : A \to R$ and $\beta : A \to R$ for which $\alpha \circ f = \beta \circ g$ as maps $C \to R$. Then there is a ring homomorphism $A \otimes_C B \to R$ given by

$$a \otimes b \mapsto \alpha(a)\beta(b),$$

which is well-defined by our requirements on α and β, such that the maps α and β may be factored through $A \otimes_C B$. Moreover, it is clearly unique since the images of $a \otimes 1$ and $1 \otimes b$ for $a \in A$ and $b \in B$ determine the map on the rest of the ring. With this in mind, note that the same must be true for the associated affine schemes with the arrows reversed. More generally, by taking affine covers, we may construct a product over general schemes.

Theorem 2.3.8. *Let X, Y, and Z be schemes with morphisms $A \to Z$ and $Y \to Z$. Then there exists a scheme $X \times_Z Y$, referred to as the fibred product, such that there are projection maps $\pi_1 : X \times_Z Y \to X$ and $\pi_2 : X \times_Z Y \to Y$ such that, for any scheme W with morphisms to A and B, there is a morphism $W \to X \times_Z Y$ such that the following diagram commutes*

$$\begin{tikzcd}
W \arrow[rrd, dashed] \arrow[rdd] \arrow[rrrdd, bend left] & & & \\
& & X \times_Y Z \arrow[ld] \arrow[rd] & \\
& X \arrow[rd] & & Y \arrow[ld] \\
& & Z &
\end{tikzcd}$$

The projection morphisms also satisfy that the preimage $\pi_1^{-}(U)$ for an open subset $U \subseteq A$ is the product $U \times_Z B$. Moreover, if $U \subseteq Z$ is affine, with $V_1 \subseteq X$ and $V_2 \subseteq Y$ affine contained in preimages of U, then $V_1 \times_U \times V_2$ is an open affine subset of $X \times_Z Y$ given by the ring tensor.

Proof. See Theorem II.3.3 of [Har13]. □

With fiber products, we uncover our last general properties of schemes which helps us describe varieties as schemes.

Definition 2.3.9. A map $X \to Y$ is said to be *separated* if the diagonal map $\Delta : X \to X \times_Y X$, which is derived from the identity $X \to X$ and the morphism $X \to Y$, is a closed immersion. If the canonical map $X \to \mathbb{Z}$ is separated, we say that X is separated.

Definition 2.3.10. Let X and Y be schemes. Defining *projective n-space* over Y as $\mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} Y$, we say that a map $f : X \to Y$ is *projective* if it is factored by a closed immersion $X \to \mathbb{P}^n_Y$.

More generally, the map $f : X \to Y$ is *quasi-projective* if we may factor first by some open immersion into a projective map. If A is a ring and $f : X \to \operatorname{Spec}(A)$ is a (quasi) projective map, we say that X is (quasi) projective over A.

Finally, we come to our very nice schemes referred to as *varieties.* These are exactly the quasi-projective integral schemes over k, where k is an algebraically closed field.

2.4 Divisors and Sheaves of Modules

While schemes and the rings associated to them have proven to be very useful, there is no reason we cannot examine other sheaves on our topological spaces. A natural step to obtaining further algebras is to go from sheaves of rings to sheaves of modules.

Definition 2.4.1. Let X be a scheme with sheaf of rings $\mathcal{O}_X$. A *sheaf of $\mathcal{O}_X$-modules* is a sheaf of modules $\mathcal{M}$ such that for any $U \subseteq X$, $\mathcal{M}(U)$ is an $\mathcal{O}_X(U)$-module. Moreover, for an inclusion $V \subseteq U$ of open sets, for any $a \in \mathcal{O}_X(U)$ and $m_1, m_2 \in \mathcal{M}(U)$, we have

$$(am_1 + m_2)|_V = a|_v m_1|_v + m_2|_v.$$

The morphisms of such sheaves also preserve the structure as a $\mathcal{O}_X$-module.

Example. Consider a closed immersion $\iota : Y \hookrightarrow X$. We may consider the *ideal sheaf* $\mathcal{I}_Y$ associated to Y by

$$\mathcal{I}_Y = \ker(\mathcal{O}_X \to \iota_* \mathcal{O}_Y).$$

Clearly, $\mathcal{I}_Y(U) = \ker(\mathcal{O}_X(U) \to \iota_* \mathcal{O}_Y)$ is an ideal of $\mathcal{O}_X(U)$, and thus an $\mathcal{O}_X(U)$-module, for any $U \subseteq X$ open. Moreover, the restriction map preserves the module structure since it's just a ring homomorphism on $\mathcal{O}_X$ elements.

Just as we may associate a structure sheaf $\mathcal{O}_X$ to a ring A, we may also associate a sheaf of $\mathcal{O}_X$-modules to an A-module M. In fact, one may do so in the following obvious way.

Proposition 2.4.2. *Fix a ring A and an A-module M. If $(X, \mathcal{O}_X) = \mathrm{Spec}A$, there exists an $\mathcal{O}_X$-module $\widetilde{M}$ on X associated M which satisfies the following properties.*

1. $\Gamma(X, \widetilde{M}) = M$.

2. *Given $f \in A$, $\Gamma(D_f, \widetilde{M}) \cong M_f$.*

3. *For any $P \in X$, $\widetilde{M}_P \cong M_P$.*

Proof. See Proposition II.5.1 of [Har13]. □

Although the affine case is quite useful, we are more interested in how it applies to projective cases. In order to do so, however, we must first discuss graded modules.

Definition 2.4.3. Let $S = \bigoplus_{d \in \mathbb{Z}} S_d$ be a graded ring. A *graded S-module* $M = \bigoplus_{d \in \mathbb{Z}} M_d$ is such that M_d is an S_0-module and $S_e \cdot M_d \subseteq M_{d+e}$ for any $e, d \in \mathbb{Z}$. We also define the *twisted module* $M(n)$ for each $n \in \mathbb{Z}$ as $M(n)_d = M_{n+d}$ for any $d \in \mathbb{Z}$.

With this, we may describe how the affine case generalizes to our projective case.

Proposition 2.4.4. *Let S be a graded ring and M a graded S-module. Writing $(X, \mathcal{O}_X) =$ $\mathrm{Proj}(S)$, there exists a sheaf of $\mathcal{O}_X$-modules $\widetilde{M}$ which has the following characteristics.*

1. *For any $f \in S_+$, we have $\widetilde{M}|_{D_+(f)} \cong \widetilde{M_{(f)}}$, where $M_{(f)}$ is the submodule of M_f that contains only degree zero elements.*

2. *For any $P \in X$, $(\widetilde{M})_P \cong M_{(p)}$, where the module $M_{(p)}$ is again the submodule of M_p of elements of degree zero.*

Proof. See Proposition II.5.11 of [Har13]. □

Example. As a perfect example, let $S = k[x_0, \dots, x_n]$ and $X = \mathrm{Proj}(S) = \mathbb{P}^n$. For each $n \geq 1$, we write $\mathcal{O}_X(n)$ to denote the sheaf of $\mathcal{O}_X$-modules associated to the graded module $\widetilde{S(n)}$. We also specifically refer to $\mathcal{O}_X(1)$ as the *twisting sheaf of Serre*.

To understand the sheaf $\mathcal{O}_X(1)$, we can look locally on each piece $D_+(x_i)$ for each $0 \leq i \leq n$. Specifically, note that

$$S(n)_{(x_i)} = \bigcup_{d\geq 0} \{x_i^{-d} f(x_0, \ldots, x_n) : \deg f(x) = n + d\} = x_i^n k[\tfrac{x_0}{x_i}, \ldots, \tfrac{x_n}{x_i}].$$

Thus, we see that $\mathcal{O}_X(n)|_{D_+(x_i)} = x_i^n \mathcal{O}_X$. Moreover, the global sections have the form

$$\Gamma(X, \mathcal{O}_X(n)) = \mathrm{Span}_k\{x_0^{a_0} \cdots x_n^{a_n} : a_0 + \cdots + a_n = d\}.$$

From the previous example, which may be generalized to other graded rings S generated by S_1 as an S_0 algebra (see Proposition II.5.12 of [Har13]), we note a few properties that make this sheaf nice. To start, we note that our open cover revealed $\mathcal{O}_X(n)$ to be *free* on the subsets $U_i = D_+(x_i)$, in the sense that it is isomorphic to $\bigoplus_{i=1}^m \mathcal{O}_x|_{U_i}$ with $m = 1$. We refer to the exact integer on which our module is the direct sum copies of as the *rank*, which must be constant on connected components. When the rank is one, we refer to our sheaf of modules as an *invertible sheaf* for reasons which will become apparent.

Additionally, we refer to $\mathcal{O}_X(n)$ as *coherent*, which means that we may cover X with open affine patches upon which $\mathcal{O}_X|_U$ is the sheaf associated to a finitely generated module. More generally, we may say that a sheaf of modules is *quasi-coherent* when this condition holds without the module necessarily being finitely generated.

Examining the invertible sheaves further, suppose that $\mathcal{M}$ is an invertible sheaf on an integral scheme X. In this case, let $\cup_{i\in I} U_i$ be an open cover of X for which $\mathcal{M}|_{U_i} \cong \mathcal{O}_X|_{U_i}$ for all $i \in I$. We notice that for any $i \in I$, we may take some $s_i \in \Gamma(U_i, \mathcal{M})$ such that $\mathcal{M}|_{U_i} = s_i \mathcal{O}_X|_{U_i}$ since s_i cannot restrict to 0 on any open subset of U_i without changing the entire structure of $\mathcal{M}|_{U_i}$. With this in mind, let's consider a pair $i, j \in I$ and the intersection $U_i \cap U_j$. On $\Gamma(U_i \cap U_j)$, we find that both s_i and s_j generate the module, and so there is some $f_{i,j}, f_{j,i} \in \mathcal{O}_X(U_i \cap U_j)$ for which

$$s_i f_{i,j} = s_j, \qquad s_j f_{j,i} = s_i.$$

In fact, we must have that $f_{i,j} = f_{j,i}^{-1}$ in the ring $\mathcal{O}_X(U_i \cap U_j)$. Fixing some $i_0 \in I$, and denoting $f_{i_0,i} = f_i$, we may identify $\mathcal{M}$ with a sub-$\mathcal{O}_X$-module $\mathcal{L}$ of $K(X)$, now referring to $K(X)$ as the constant sheaf as a $\mathcal{O}_X$-module, by $\mathcal{L}|_{U_i} = f_i \mathcal{O}_X|_{U_i}$.

Interestingly, this in-fact takes us back to our previous discussion of ideal sheaves associated to closed subschemes, specifically in the case where $f_i \in \mathcal{O}_X(U_i)$, where identification is done through localizing at the generic point. In this case, our sheaf of ideals is locally principal, but we can speak more generally to this.

As an illustrative example, let's take $\mathcal{O}_X(1)$ with $X = \mathbb{P}^2$. Following the same procedure, we have the following association of open subsets to $K(X)$ as

$$D_+(x) \mapsto 1 \qquad D_+(y) \mapsto \frac{x}{y},$$

so that $\mathcal{O}(1)|_{D_+(x)} \cong \mathcal{O}_X$ and $\mathcal{O}(1)|_{D_+(y)} \cong \frac{x}{y}\mathcal{O}_X|_{D_+(y)}$ under this isomorphism. More generally, however, we may multiply the functions $1, \frac{x}{y} \in K(X)$ by any other $g \in K(X)^*$, and we would still obtain an isomorphism. Looking at the associated ideal sheaf, it is quite clear that we have described $(0:1) \in \mathbb{P}^n$ as a closed subscheme. And if we do take the liberty of using the functions g and $g\frac{x}{y}$ for $g = \frac{y}{x} \in K(X)^*$, we may move from $(0:1)$ to the point $(1:0)$.

Without knowing yet whether a given ideal sheaf of $K(X)$ corresponds to a closed subscheme, there may be two distinct ideas we are looking at. Namely, closed subschemes of codimension one, sub-$\mathcal{O}_X$-modules of $K(X)$, and invertible sheaves.

Definition 2.4.5. Let X be an integral separated scheme such that for every $x \in X$, if $\dim \mathcal{O}_x = 1$, then $\dim_{\kappa(x)} \mathfrak{m}/\mathfrak{m}^2 = \dim \mathcal{O}_x = 1$. We refer to a closed integral subscheme Y of X as a *prime divisor*. A *Weil divisor* is a formal sum $D = \sum_{i=1}^n a_i Y_i$, with $a_i \in \mathbb{Z}$ and Y_i a prime divisor for each $1 \leq i \leq n$.

The support of a Weil divisor D is the union of prime divisors Y for which the associated coefficient in D is non-zero. We say that a divisor D is *effective*, and write $D \geq 0$, if the integers may be taken to be non-negative, and we identify such divisors with their support.

As we may add and subtract these formal sums, the Weil divisors form a group, which we will denote as $\mathrm{Div}(X)$.

To make sense as to how the group of Weil divisors operates, consider the fact that a prime divisor Y of X has a generic point $\eta \in Y$. By the codimension of Y, we find $\dim \mathcal{O}_{X,\eta} = 1$, and so by our regularity proposition, $\mathcal{O}_{X,\eta}$ is principal and thus a discrete valuation ring. Therefore, on the units of our field of fractions of $K(X)$, we may define an order of vanishing at the prime divisor Y, denoted $v_Y : K(X)^* \to \mathbb{Z}$. For a prime divisor Y, $f \in K(X)^*$, and an integer $m > 0$, we say that f has a *zero of order m at Y* if $v_Y(f) = m$, and that f has a *pole of order m at Y* if $v_Y(f) = -m$.

Definition 2.4.6. Given X as before and $f \in K(X)^*$, we may define the *principal divisor* $\mathrm{div}(f) \in \mathrm{Div}(X)$ as

$$\mathrm{div}(f) = \sum_{\mathrm{codim}(Y,X)=1} v_Y(f)Y.$$

If $D_1, D_2 \in \mathrm{Div}(X)$ are such that $D_1 - D_2 = \mathrm{div}(f)$ for some $f \in K(X)^*$, we say that D_1 and D_2 are *linearly equivalent* and may write $D_1 \sim D_2$.

Just as we had noticed before in our example derived from invertible sheaves, we see that there is some notion of equivalence by the elements of $K(X)^*$.

For another example, let $k/\mathbb{Q}$ be a finite extension with ring of integers R_k. Since R_k is a Dedekind domain, it is clear that $X = \mathrm{Spec}(R_k)$ satisfies all the defining properties required to describe $\mathrm{Div}(X)$. Indeed, our principal divisors are just elements of k^* and our prime divisors are prime ideals $P \subseteq R_k$. We recall from Corollary 3.9 of [Neu13] that given some finitely generated sub-R_k-module of k^*, we may associate a unique factorization as prime ideals, and this corresponds to the valuation along our prime divisors as before. As expected, when we consider $\mathrm{Div}(X)$ under linear equivalence, we have described the class group of R_k which describes how far R_k is from being a principal ideal domain.

Definition 2.4.7. Let X be such that we may define $\mathrm{Div}(X)$ as above. Then we may define the *class group of divisors on* X, denoted $\mathrm{Cl}(X)$, as the quotient of $\mathrm{Div}(X)$ by the subgroup of principal divisors.

To obtain a more geometric picture of our class group of divisors, consider an open subset $U \subseteq X$, with $\mathrm{Cl}(X)$ well-defined. In the case where $\mathrm{codim}(X \setminus U, X) \geq 2$, notice that the prime divisors of U will be given exactly as the restriction of a prime divisor from X, and we likewise haven't removed any prime divisors in this process, up to at least what may be permuted by the principal divisors. However, if $\mathrm{codim}(X \setminus U, X) = 1$, we have the following proposition.

Proposition 2.4.8. *Let X be such that $\mathrm{Cl}(X)$ is well-defined, and suppose that $U \subseteq X$ is open with complement Y. Then $\mathrm{Cl}(U)$ is well-defined, and the restriction of the prime divisors of X to U grants a map $D \mapsto D|_U$ which is surjective. If $\mathrm{codim}(Y, X) \geq 2$, we have $\mathrm{Cl}(X) \cong \mathrm{Cl}(U)$. However, if $\mathrm{codim}(Y, X) = 1$, we have the following exact sequence,*

$$\langle Y \rangle \to \mathrm{Cl}(X) \to \mathrm{Cl}(U) \to 0,$$

where the first map is just the inclusion as a subgroup.

Proof. Refer to Proposition II.6.5 of [Har13]. □

As another hint in the direction towards unification of these ideas, let X be such that the class group is well-defined and take any $D \in \mathrm{Div}(X)$. For each $U \subseteq X$, we may define a subgroup of $K(X)^*/\mathcal{O}_X(U)^*$ as

$$L(D)(U) = \{f \in K(X)^*/\mathcal{O}_X(U)^* : D|_U + \mathrm{div}(f|_U) \geq 0\}$$

where we note the quotient may be taken as units of $\mathcal{O}_X(U)$ certainly have no poles or zeroes on U. Notice that linear equivalence, whether globally or locally on just the open set of interest, induces an isomorphism between these subgroups by simply performing the group action of multiplication by the principal divisor on $K(X)^*/\mathcal{O}_X(U)^*$

Also, we see that $L(D)(U) \cup \{0\}$ is an $\mathcal{O}_X(U)$-module. For any prime divisor Y, $f_1, f_2 \in L(D)(U)$, and $c_1 \in \mathcal{O}_X(U)$ non-zero,

$$v_Y(c_1 f_1 + f_2) \geq \min(v_Y(c_1 f_1), v_Y(f_2)) = \min(v_Y(f_1) \cdot v_Y(f_1), v_Y(f_2)) \geq \min(v_Y(f_1), v_Y(f_2)).$$

If $\mathcal{O}_X(U)$ were to contain a field, this would then be a vector space, as is the case with varieties.

While this may appear to be a sheaf, in general this is not. However, this may be easily accounted for.

Definition 2.4.9. Let X be an integral scheme. We recall that $K(X)$ acts as a constant sheaf on X. Taking $\mathcal{O}_X^*$ to be the sheaf defined by the group of multiplicative units of $\mathcal{O}$, a *Cartier divisor* D is a global section of $\Gamma(X, K(X)^*/\mathcal{O}_X^*)$, where the quotient sheaf is defined as the sheaf associated to the presheaf $U \mapsto K(X)^*/\mathcal{O}_X(U)^*$. The group $\Gamma(X, K(X)^*/\mathcal{O}_X^*)$ is denoted $\mathrm{CaDiv}(X)$ and referred to as the group of Cartier divisors.

Moreover, if a section lies in the image $K(X)^* \to K(X)^*/\mathcal{O}_X^*$, we say that the Cartier divisor is *principal.* Using additive language, when the difference between two Cartier divisors is principal, we say that they are *linearly equivalent.* We denote the quotient of $\mathrm{CaDiv}(X)$ by the principal Cartier divisors as $\mathrm{CaCl}(X)$.

By our explanation of a sheaf associated to a presheaf, a Cartier divisor $D \in \mathrm{CaDiv}(X)$ may be represented by a set of pairs

$$D = \{(U_i, f_i) : f_i \in K(X)/\mathcal{O}_X(U_i)^*, i \in I\}$$

for which $\bigcup_{i\in I} U_i = X$, and $f_i f_j^{-1} \in \mathcal{O}_X(U_i \cap U_j)^*$ for any $i, j \in I$. The group action on such sets is simply done by pairwise multiplication on intersections.

Just as with the Weil divisors, the Cartier divisors as well have a similarly notated and similarly behaving associated group. Taking $D = \{(U_i, f_i)\}_{i\in I} \in \mathrm{CaDiv}(X)$ for an integral scheme X, we define the *sheaf associated to* D, notated $\mathcal{L}(D)$, to be the sub-$\mathcal{O}_X$-module of $K(X)^*$ which is defined locally as

$$\mathcal{L}(D)|_{U_i} = \frac{1}{f_i}\mathcal{O}_X|_{U_i},$$

which may be glued together since $f_i/f_j^{-1} \in \mathcal{O}_X(U_i \cap U_j)^*$ for any $i, j \in I$. Furthermore, notice that $\mathcal{L}(D + \mathrm{div}(f)) \cong \mathcal{L}(D)$ by multiplication by $f \in K(X)^*$, so it this sheaf is well-defined on $\mathrm{CaDiv}(X)$.

Notice for the case of

$$D_W = (1:0) \in \mathrm{Div}(\mathbb{P}^1), \qquad D_C = \{(D_+(x), 1), (D_+(y), \tfrac{x}{y})\} \in \mathrm{CaDiv}(\mathbb{P}^1),$$

we immediately find a correspondence between $L(D_W)(U) \cong \Gamma(U, \mathcal{L}(D_C)) \cong \Gamma(U, \mathcal{O}(1))$ for any open $U \subseteq \mathbb{P}^1$.

Definition 2.4.10. The *Picard group* of X, denoted $\mathrm{Pic}(X)$, is the group of invertible sheaves of $\mathcal{O}_X$-modules up to isomorphism. The group operation is given by $\mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$ for $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Pic}(X)$, where $\mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$ is the sheaf associated to the presheaf

$$U \mapsto cL_1(U) \otimes_{\mathcal{O}_X(U)} \mathcal{L}_2(U).$$

Theorem 2.4.11. *Suppose that X is a non-singular, integral, separated, noetherian scheme. Then there are group isomorphisms between* $\mathrm{Cl}(X)$, $\mathrm{CaCl}(X)$, *and* $\mathrm{Pic}(X)$.

With our concepts joined together, we may see how these groups allow us to understand a given non-singular variety X/k. Take $D \in \mathrm{Div}(X)$ arbitrarily and consider the global sections of $\Gamma(X, \mathcal{L}(D))$. In the projective case, as $\Gamma(X, \mathcal{O}_X) = k$, we may consider a basis

$$\Gamma(X, \mathcal{L}(D)) = \mathrm{Span}_k\{f_0, \ldots, f_n\},$$

which is finite by A.3.2.7 of [HS13]. Next, define a map $\varphi : X \to \mathbb{P}^n$ by

$$\varphi(P) = (f_0(P) : \cdots : f_n(P)).$$

The first issue which might be encountered is that one of our maps has a pole. We may be able to move a pole around by multiplying through by $g \in K(X)^*$, and clearly this will not change the value of φ away from $\mathrm{supp}(\mathrm{div}(g))$. However, we may encounter the issue as well that we could have a *base point* of D on which all global sections vanish. If this does not occur, and the resulting map is a closed immersion, then we say that D is *very ample*, while D being *ample* refers to the property that some multiple mD is very ample for $m \geq 1$.

For an alternative picture, consider a map $\varphi : X/k \to Y/k$ of non-singular varieties. Fixing $D \in \mathrm{Pic}(Y)$, represented as $\{(U_i, f_i)\}_{i \in I}$, we would like to define

$$\varphi^* D = \{(\varphi^{-1}(U_i), f_i \circ \varphi)\}_{i \in I},$$

where $f_i \circ \varphi$ is understood by considering $\eta \in X$ as the generic point and the map

$$\kappa(\varphi(\eta)) \to \kappa(\eta) = K(X)^*.$$

However, $\kappa(\varphi(\eta))$ may be a proper subset of $K(Y)^*$ in the case where $\varphi(X)$ is not dense in Y. Fortunately, if all defining functions belong to $\kappa(\varphi(\eta))$, this map makes sense, and this is the condition that $\varphi(X)$ is not contained in the support of D. It is known that for varieties by Lemma A.2.2.5 of [HS13], we may always determine a representative D' of the class of D

for which the pullback is defined. Alternatively, we have for the associated sheaves,

$$\varphi^* \mathcal{L}(D) = \varphi^{-1} \mathcal{L}(D) \otimes_{\mathcal{O}_Y} \mathcal{O}_X.$$

This allows us to express the following.

Definition 2.4.12. Let X be a scheme and $\mathcal{M}$ a sheaf of $\mathcal{O}_X$-modules. We say that $\mathcal{M}$ is *generated by global sections* if there exists an indexed set $\{s_i\}_{i \in I}$ of global sections of $\Gamma(X, \mathcal{M})$ such that

$$\mathcal{M}_x = \sum_{i \in I} s_i|_x \mathcal{O}_{X,x},$$

for any $x \in X$.

Theorem 2.4.13. *Let X/k be a non-singular variety.*

1. *If $\varphi : X \to \mathbb{P}^n_k$ is a morphism, then $\varphi^* \mathcal{O}(1)$ is an invertible sheaf generated by the global sections $\{x_i \circ \varphi\}_{i=0}^n$.*

2. *For any $D \in \operatorname{Pic}(X)$, if $\mathcal{L}(D)$ is generated by global sections $s_0, \ldots, s_n \in \Gamma(X, \mathcal{L}(D))$, then the map*

$$\varphi(x) = (s_0(x) : \cdots : s_n(x))$$

is a morphism such that $\varphi^* \mathcal{O}(1) \cong \mathcal{L}(D)$ with $x_i \circ \varphi = s_i$ for each $0 \leq i \leq n$.

Proof. See Theorem II.7.1 of [Har13]. □

2.5 Blowups

One of the advantages of algebraic geometry is the ability to analyze a space regardless of coordinates or embedding. As such, we often look towards birational maps which capture the geometry of a given space but may transform into an easier to understand or better behaved space. One such way of constructing these birational maps comes from the idea of a blow up. We capture blow ups unique up to isomorphism using the following universal property definition.

Definition 2.5.1 (Blow up)**.** Let $Y \subseteq X$ be a closed subscheme. The *blowup of* X *along* Y, with *centre* Y, is a space $\widetilde{X}$ and a map $\pi : \widetilde{X} \to X$ which is an isomorphism on $X \setminus Y$. We denote $E = \pi^{-1}(Y)$ as the *exceptional divisor*, which is an effective Cartier divisor.

Finally, for any space W with closed subscheme Z for which the ideal sheaf is locally invertible, along with a map $\varphi : W \to X$ satisfying $Z = \varphi^{-1}(Y)$, then there exists a unique map $\psi : W \to \widetilde{X}$ which satisfies $\pi \circ \psi = \varphi$. This is captured by the following commutative diagram.

$$\begin{tikzcd}
Z \arrow[r, hook] \arrow[drr, dashed] \arrow[ddr] & W \arrow[drr, dashed] \arrow[ddr] & & \\
& & E \arrow[r, hook] \arrow[dl] & \widetilde{X} \arrow[dl] \\
& Y \arrow[r, hook] & X &
\end{tikzcd}$$

Let's investigate this definition by examining the example on the affine case $X = \text{Spec}(A)$, where our closed subscheme Y is described by an ideal $I = \langle f_1, \ldots, f_r \rangle$. We claim that a good candidate for $\widetilde{X}$ is $\text{Proj}(\bigoplus_{d \geq 0} I^d t^d)$, where $I^d = A$ and the parameter t is kept to account for the degree in our graded ring. We may write $A[It]$ as a shorthand for the graded module in question.

A natural place to start is by first establishing a map $\pi : \widetilde{X} \to X$. In this case, we have a very simple and natural map by taking $P \in \text{Proj}(A[It])$ and considering $P \cap A$, which simply follows from the inclusion $A \hookrightarrow A[It]$. Under such a mapping, let's consider our exceptional divisor $E = \pi^{-1}(Y)$. Following the inclusion $Y \hookrightarrow X$ by prime ideals containing I, we have the equivalence below.

$$P = \bigoplus_{d\geq 0} P_d t^d \in \pi^{-1}(Y) \iff I \subseteq \pi(P) = P_0$$

$$\iff \forall d \geq 0, I^{d+1}t^d = I \cdot I^d t^d \subseteq P_0 \cdot I^d t^d \subseteq P_d t^d.$$

Therefore, as $P \in E$ contains $I^{d+1}t^d$ for the degree d components of the homogeneous prime ideal P, our exceptional divisor E may be thought of as cut out by the ideal sheaf $\mathcal{I}_E = (\bigoplus_{d\geq 0} I^{d+1}t^d)^{\sim}$.

We check as well that this ideal sheaf is indeed invertible. To do so, consider for some $1 \leq j \leq r$ the section $f_j t \in A[It](1)$. On the open set $D_+(f_j t) \cong \operatorname{Spec}(A[It])_{(f_j t)}$, note we have

$$A[It]_{(f_j t)} = A + \frac{1}{f_j} I + \frac{1}{f_j^2} I^2 + \cdots$$

Note as well that since $f_j^k \in I^k$ for all $k \geq 1$, it follows that we may cut off arbitrarily many terms from the start as $A \subseteq \frac{1}{f_j} I \subseteq \frac{1}{f_j^2} I^2$ and so forth. Likewise, taking the ideal sheaf associated to E and localizing to $D_+(f_j t)$, we have from definition that

$$\mathcal{I}_E|_{D_+(f_j t)} = \left(\bigoplus_{d\geq 0} I^{d+1} t^d \right)_{(f_j t)} = I + \frac{1}{f_j} I^2 + \frac{1}{f_j^2} I^3 \cdots$$

demonstrating that $\mathcal{I}_E|_{D_+(f_j t)} \cong f_j \mathcal{O}_{\widetilde{X}}|_{D_+(f_j t)}$. Note as well the parallels of $\mathcal{I}_E$ to $\mathcal{O}_{\widetilde{X}}(1)$ as they are the same invertible sheaf.

Next, consider a pair $Z \hookrightarrow W$ with $\mathcal{I}_Z$ invertible, and a map $\varphi : W \to X$ such that $Z = \varphi^{-1}(Y)$. With our map φ, it is easy to construct a map $\psi : W \to \widetilde{X}$ which factors through $\pi : \widetilde{X} \to X$ as for any $Q \in W$,

$$\psi(Q) = \bigoplus_{d\geq 0} (\varphi(Q) \cap I^d) t^d.$$

A full verification of our universal property follows from Proposition II.7.14 [Har13], and shows we have indeed constructed the blow up $\pi : \widetilde{X} \to X$.

In fact, we have indeed shown that the blow up exists in general. We explore this and some consequences in the following propositions and corollaries.

Proposition 2.5.2. *Blow ups are locally defined. That is, given $U \subseteq X$ and a blow up $\pi : \widetilde{X} \to X$ with centre Y and exceptional divisor E, $\pi^{-1}(U)$ is the blow up of U along $Y \cap U$ with exceptional divisor $E \cap \pi^{-1}(U)$.*

Proof. To show this, we need only demonstrate the universal property. For this, consider $Z \hookrightarrow W$ satisfying all necessary conditions. We may immediately draw the following diagram.

$$\begin{tikzcd}
Z \arrow[r, hook] \arrow[d] & W \arrow[d] & E \cap \pi^{-1}(U) \arrow[r, hook] \arrow[d] \arrow[dll] & \pi^{-1}(U) \arrow[d] \arrow[dll] \\
Y \cap U \arrow[r, hook] \arrow[d] & U \arrow[d] & E \arrow[r, hook] \arrow[dll] & \widetilde{X} \arrow[dll] \\
Y & X & &
\end{tikzcd}$$

Following our maps $Z \to Y$ and $W \to X$, we may use our universal property to determine a map $W \to \widetilde{X}$. However, since it must commute with the map $W \to X$ which has image contained in U, we see that we in-fact have a map $W \to \pi^{-1}(U)$, which satisfies all requirements. □

Corollary 2.5.3. *Let $\pi : \widetilde{X} \to X$ be a blow up along Y with exceptional divisor E. Then $\pi : \widetilde{X} \setminus E \to X \setminus Y$ is an isomorphism, and hence π is birational.*

Proof. For this, we simply consider that $\pi^{-1}(X \setminus Y)$ is the blow up of $X \setminus Y$ along the empty set. However, the empty set is already cut out by the ideal sheaf generated by 1 on any open subset. Therefore $X \setminus Y$ satisfies the universal property and hence is isomorphic to $\pi^{-1}(X \setminus Y) = \widetilde{X} \setminus E$. □

We also cite Exercise 23.2.A of [Vak22] in the following proposition.

Proposition 2.5.4. *Blow ups may be glued together. That is, if $\cup_{i\in I} U_i$ is an open cover of X, and there exists blow ups $\pi_i : \widetilde{U}_i \to U_i$ along center $Y \cap U_i$, then there exists a blow up $\pi : \widetilde{X} \to X$ along center Y.*

With the basics of construction covered, let's examine some notable properties of blow ups. For our first example, let's see how blow ups separate crossing lines and hence could resolve singularities, though we will not dive further into this as it is unnecessary for our cases. We first take a quick detour to define the *strict transform.*

Lemma 2.5.5. *Let $Y, Z \subseteq X$ be closed subschemes. If $\widetilde{Z}$ is the blow up of Z along $Y \cap Z$ and $\widetilde{X}$ is the blow up of X along Y, then there exists a closed immersion $\widetilde{Z} \hookrightarrow \widetilde{X}$. Moreover, we may draw the following commutative diagram.*

$$\begin{tikzcd}
\widetilde{Z} \arrow[r, hook] \arrow[d] & \widetilde{X} \arrow[d] \\
Z \arrow[r, hook] & X
\end{tikzcd}$$

Proof. See Corollary II.7.15 of [Har13]. □

Definition 2.5.6 (strict/proper transform)**.** Taking X, Y, Z and $\widetilde{Z}$ as above, we refer to $\widetilde{Z}$ as the *strict transform* of Z.

Proposition 2.5.7. *Let $Y \subseteq X$ be the intersection $Y = \cap_{i=1}^r Y_i$ such that $\mathcal{I}_Y = \sum_{i=1}^r \mathcal{I}_{Y_i}$. Then if $\pi : \widetilde{X} \to X$ is the blow up of X along Y, then the intersection of the strict transforms of Y_i is empty in $\widetilde{X}$.*

Proof. To begin, we note that this suffices to prove locally since any intersection would lie in the preimage of some open subset of X. Therefore, we may assume $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(A/I)$ for some ideal $I \subseteq A$, and $Y_i = \mathrm{Spec}(A/J_i)$ for some ideal $J_i \subseteq A$ for each $1 \leq i \leq r$. Next, note that $Y \cap Y_i$ is then given as $V(I/J_i) \subseteq Y_i$, so we may write each strict transform and our blow up $\widetilde{X}$ as

$$\widetilde{Y_i} = \operatorname{Proj}\left(\bigoplus_{d\geq 0}(I/J_i)^d t^d\right), \qquad \widetilde{X} = \operatorname{Proj}\left(\bigoplus_{d\geq 0} I^d t^d\right).$$

With this, we may proceed by noting that there is a clear surjective graded ring homomorphism $A[It] \to A[(I/J_i)t]$ which gives each closed immersion. Therefore, any prime ideal in the image of a given closed immersion must contain the kernel of this graded ring homomorphism. Hence, if $P \in \cap_{i=1}^r \widetilde{Y_i}$, then by examining the degree one terms in each kernel, it follows that $J_i t \subseteq P$ for each $1 \leq i \leq r$. However, since $I = \sum_{i=1}^r J_i$ by hypothesis, we must have $It \subseteq P$ and so P contains all of $A[It]_+$, which is a contradiction. □

Another useful way strict transforms and blow ups come together is in the pullback of an effective Cartier divisor. Let $\pi : \widetilde{X} \to X$ be a blow up of a non-singular variety with irreducible, non-singular center Y of codimension at least 2 and exceptional divisor E. We will also assume that $\widetilde{X}$ is non-singular as well. The first objective is to determine the relation between $\operatorname{Pic}(\widetilde{X})$ and $\operatorname{Pic}(X)$.

To explore this further, recall that we have the exact sequence

$$\mathbb{Z} \to \operatorname{Pic}(\widetilde{X}) \to \operatorname{Pic}(\widetilde{X} \setminus E) \to 0.$$

In fact, this is a short exact sequence. Consider the fact that $\pi^* : K(X) \to K(\widetilde{X})$ is an isomorphism as it is the pullback of a birational map. Thus, if $mE = \operatorname{div}(f)$ for some $m \in \mathbb{Z}$ and $f \in K(\widetilde{X})$, then we may write $mE = \pi^*\operatorname{div}(g) = \operatorname{div}(g \circ \pi)$ for some $g \in K(X)$. However, this implies that g may not vanish outside Y, but because $\operatorname{codim}(Y, X) \geq 2$, this is only possible if g is a non-vanishing constant and $m = 0$.

Next, we also have isomorphisms between $\operatorname{Pic}(\widetilde{X} \setminus E)$, $\operatorname{Pic}(X \setminus Y)$, and $\operatorname{Pic}(X)$, where the last isomorphism is due to the fact $\operatorname{codim}(Y, X) \geq 2$. Therefore, we may now write a short exact sequence as

$$0 \to \mathbb{Z} \to \mathrm{Pic}(\widetilde{X}) \to \mathrm{Pic}(X) \to 0$$

Lastly, we also have a section $\pi^* : \mathrm{Pic}(X) \to \mathrm{Pic}(\widetilde{X})$ which composes with the previous morphism as the identity. To confirm this, fix some Cartier divisor $D = \{(U_i, f_i)\}_{i=1}^r \in \mathrm{Pic}(X)$. We then find that

$$\begin{aligned}(\pi^* D)|_{\pi^{-1}(X \setminus Y)} &= \{(\pi^{-1}(U_i), f_i \circ \pi)\}|_{\widetilde{X} \setminus E} \\ &= \{(\pi^{-1}(U_i) \cap \widetilde{X} \setminus E, f_i \circ \pi|_{\widetilde{X} \setminus E})\} \\ &= \{(\pi|_{\widetilde{X} \setminus E}^{-1}(U_i \cap X \setminus Y), f_i|_{X \setminus Y} \circ \pi|_{\widetilde{X} \setminus E})\} \\ &= \pi|_{\widetilde{X} \setminus E}^{*} D|_{X \setminus Y}.\end{aligned}$$

As the map $\mathrm{Pic}(\widetilde{X}) \to \mathrm{Pic}(X)$ follows by restricting to $\mathrm{Pic}(\widetilde{X} \setminus E)$, and then following $\pi|_{\widetilde{X} \setminus E}*$ to $\mathrm{Pic}(X \setminus Y)$, we see that this composition is indeed the identity on $\mathrm{Pic}(X)$. Therefore, we may write $\mathrm{Pic}(\widetilde{X}) \cong \mathrm{Pic}(X) \oplus \mathbb{Z}$.

Since an effective Cartier divisor D on X corresponds to ideal sheaf of a closed subscheme via $\mathcal{L}(-D)$, it is natural for us to associate a strict transform $\widetilde{D}$ to this divisor. As such, locally writing out $D = \{(U_i, f_i)\}_{i=1}^r$, we also consider the pullback

$$\pi^* D = \{(\pi^{-1}(U_i), f \circ \pi)\}_{i=1}^r.$$

In the case where Y is a point, we find that $\pi^* D = \widetilde{D} + \mathrm{ord}_Y(D)E$, where $E = \pi^{-1}(Y)$ is the exceptional divisor, following from Exercise 23.4.P of [Vak22]. To clarify, $\mathrm{ord}_Y(D) \geq 0$ is defined such that if $\eta \in Y$ is the generic point, and $D|_U = \mathrm{div}(f)$ for some neighbourhood $U \subseteq X$ of η, then $f \in \mathfrak{m}_\eta^{\mathrm{ord}_Y(D)} \setminus \mathfrak{m}_\eta^{\mathrm{ord}_Y(D)+1}$. This is well-defined regardless of neighbourhood for the same reason the usual mapping from Cartier divisors to Weil divisors is.

2.6 Canonical Divisor Class

To tie our geometry together, we take a page from differential geometry and consider the derivatives of our functions. Following from the operations familiar to us for derivatives in ordinary calculus, let's examine the generalization of Kähler differentials.

Definition 2.6.1 (Relative Derivation)**.** Let A be a commutative ring, B and A-algebra, and M some B-module. An A-*derivation* $d : B \to M$ is a map satisfying for all $b_1, b_2 \in B$ and $a \in A$:

1. (Additivity) $d(b_1 + b_2) = d(b_1) + d(b_2)$.
2. (Leibniz Rule) $d(b_1 b_2) = b_1 d(b_2) + b_2 d(b_1)$.
3. (Constant Rule) $d(a) = 0$.

Note that the Leibniz rule, constant rule, and additivity pair together to mean that a k-derivation over a k-vector space is indeed linear.

Paired with our relative derivations, we also have an associated module which satisfies a certain universal property. The most straightforward way to go about constructing such a module is by taking

$$M = \frac{\langle db \rangle_{b \in B}}{\langle d(b_1 + db_2) - db_1 - db_2, d(b_1 b_2) - b_1 db_2 - b_2 db_1, da \rangle_{b_1, b_2 \in B, a \in A}},$$

where we imply the free B-modules generated by such symbols. However, another such way we may do so is by considering the ring $B \otimes_A B$.

Following a construction familiar if you have worked with differential forms, suppose we have the map $D : B \otimes_A B \to B$ given on the pure tensors as $D(b_1 \otimes b_2) = b_1 b_2$. Using the kernel $I = \ker D$, we may determine an A-derivation $d : B \to I/I^2$ by

$$db = b \otimes 1 - 1 \otimes b + I^2,$$

where I/I^2 inherits B-multiplication from $B \otimes_A B$ defined by $b_1(b_2 \otimes b_3) = b_1b_2 \otimes b_3$. Clearly, without even considering B-multiplication, we immediately see this derivation satisfies additivity and the constant rule. Additionally, we do also find for $b_1, b_2 \in B$ that

$$d(b_1b_2) = b_1b_2 \otimes 1 - 1 \otimes b_1b_2 + I^2, \tag{1}$$

$$b_1db_2 + b_2db_1 = b_1b_2 \otimes 1 - b_1 \otimes b_2 + b_2b_1 \otimes 1 - b_2 \otimes b_1 + I^2, \tag{2}$$

$$db_1 \cdot db_2 = b_1b_2 \otimes 1 - b_2 \otimes b_1 - b_1 \otimes b_2 + 1 \otimes b_1b_2 + I^2. \tag{3}$$

However, since the representative for $db_1 \cdot db_2$ is necessarily an element of I^2, it follows that

$$b_1db_2 + b_2db_1 = d(b_1b_2) + db_1 \cdot db_2 = d(b_1b_2).$$

This discussion is summarized in the following proposition.

Proposition 2.6.2. *Let B be an A-algebra, both commutative rings. There exists a module of relative differential forms, denoted $\Omega_{B/A}$ with an A-derivation $d : B \to \Omega_{B/A}$ and unique up to isomorphism, such that if $d_2 : B \to M$ is another A-derivation, there there exists a unique map $\varphi : \Omega_{B/A} \to M$ such that the following diagram commutes.*

$$\begin{tikzcd}
B \arrow[r, "d_2"] \arrow[d, "d"] & M \\
\Omega_{B/A} \arrow[ur, dashed, "\varphi"] &
\end{tikzcd}$$

Proof. See Proposition 26.1 of [Mat70]. □

Example. Let $A = k$ and $B = k[x_1, \ldots, x_n]$ for a number field k. Then $\Omega_{B/k} = \text{Span}_k\{dx_1, \ldots, dx_n\}$, and the derivation map $d : B \to \Omega_{B/k}$ corresponds to the derivative of a given polynomial as a complex function.

Let's now construct a sheaf which corresponds to our module of relative differentials. Suppose that X and Y are schemes and we are given a map $f : X \to Y$. Consider first the case where $X = \operatorname{Spec}(B)$ and $Y = \operatorname{Spec}(A)$. We recall that $X \times_Y X \cong \operatorname{Spec}(B \otimes_A B)$, and there is a map $X \to X \times_Y X$ which comes from the map $D : B \otimes_A B \to B$ as defined above. As this ring map is surjective, we have identified X as a closed subscheme of $X \times_Y X$ whose ideal sheaf is generated by the kernel of D.

With this setup, we may now impose that $\Omega_{X/Y}$ be defined as $(\Omega_{B/A})^\sim$, where we now obtain a derivation $d : \mathcal{O}_X \to \Omega_{X/Y}$. It should be noted that the localization of a module of relative differential forms is precisely the differential forms of the localized ring, so our derivation map remains well defined as a sheaf map. For more general schemes X and Y, it suffices to patch both with affine open subsets and glue these modules together to define the sheaf $\Omega_{X/Y}$.

Example. Let $X = \mathbb{P}^1_k$ with projective coordinates $(x : y)$, and take $Y = \operatorname{Spec}(k)$ for an algebraically closed field k. We may compute $\Omega_{\mathbb{P}^1_k/k}$ as isomorphic to the sheaf $\mathcal{O}(-2)$. To see why, fix an affine patch $U = D_+(x)$. On this patch, we know that $\Omega_{U/k}$ is a free sheaf of rank 1 generated by the global section $d\left(\frac{y}{x}\right)$. By using a similar argument on $V = D_+(y)$, we have on the open cover $\mathbb{P}^1_k = U \cup V$

$$\Omega_{\mathbb{P}^1_k/k}|_U \cong d\left(\frac{y}{x}\right)\mathcal{O}_{\mathbb{P}^1_k}|_U \qquad \Omega_{\mathbb{P}^1_k/k}|_V \cong d\left(\frac{x}{y}\right)\mathcal{O}_{\mathbb{P}^1_k}|_V.$$

On the intersection $U \cap V$, it follows from our rules of derivation (or by standard calculus rules) that

$$\frac{x}{y} \cdot d\left(\frac{y}{x}\right) = -\frac{y}{x} \cdot d\left(\frac{x}{y}\right).$$

Therefore, by comparing local generators, $\Omega_{\mathbb{P}^1_k/k}$ is isomorphic to the sheaf generated by the Cartier divisor $\{(U, \frac{x}{y}), (V, \frac{y}{x})\}$. Since this divisor has a pole at $\{y = 0\}$ and a pole at $\{x = 0\}$, and no zeroes or poles anywhere else, it must be isomorphic to $\mathcal{O}(-2)$.

An interesting fact of the sheaf of relative differentials is that it encodes the information regarding whether a particular scheme is non-singular by its rank should it be a free sheaf. Unfortunately, this also means that for surfaces and beyond, we no longer have an invertible sheaf and cannot connect it to the Picard group. However, we may recover this via the exterior algebra.

Definition 2.6.3. Let X/k be non-singular. The *canonical divisor sheaf* on X, is $\omega_X = \bigwedge^n \Omega_{X/k}$, where $\bigwedge^n \Omega_{X/k}$ is the sheaf associated to the presheaf

$$U \mapsto \bigwedge^n \Omega_{X/k}(U).$$

We often write K_X as the canonical divisor associated to $\omega_{X/k}$ when we have all divisor groups isomorphic.

We refer to such a sheaf as canonical since it has been defined without any choices. Notably, each of our previous divisors which granted us maps to projective space each came with some choice of coordinates or hyperplanes. Now, however, we have a purely geometric way to examine non-singular schemes. Let's investigate a few propositions which help give a sense for how this sheaf behaves.

Proposition 2.6.4. *Let $X = \mathbb{P}^n$. Then $\omega_X \cong \mathcal{O}(-n-1)$.*

Proof. While a similar argument follows for $n \geq 2$ as it did for $\mathbb{P}^1$, this also follows from Theorem II.8.13 of [Har13]. □

We also recall Exercise II.8.3 and Exercise II.8.5 of [Har13] in the following two propositions.

Proposition 2.6.5. *Let X and Y be non-singular schemes over k. Then if $\pi_1 : X \times_k Y \to X$ and $\pi_2 : X \times_k Y \to Y$ are the projection maps, we have*

$$K_{X \times_k Y} \sim \pi_1^* K_X + \pi_2^* K_Y.$$

Proposition 2.6.6. *Let X be a non-singular scheme, with $Y \subseteq X$ a non-singular closed subscheme with* $\operatorname{codim}(Y, X) = r \geq 2$. *If $\pi : \widetilde{X} \to X$ is the blow up of X along Y, with* *exceptional divisor E. Then*

$$K_{\widetilde{X}} = \pi^* K_X + (r-1)E.$$

2.7 Elliptic Curves

With much of the geometry behind us, let's turn to another interesting curve, which encodes a similar level of novel arithmetic information on a level comparable to $\mathbb{P}^1$. To understand *elliptic curves*, we begin with a famous result of projective curves.

Theorem 2.7.1 (Riemann-Roch for Curves)**.** *Let C be a non-singular projective curve with canonical sheaf K_C. For any $D \in \operatorname{Div}(C)$, we denote*

$$\ell(D) = \dim_k L(D).$$

Then there exists an integer $g \geq 0$, referred to as the genus, such that for any $D \in \operatorname{Div}(C)$,

$$\ell(D) - \ell(K_C) = \deg(D) - g + 1$$

Proof. Refer to Theorem IV.1.3 of [Har13]. □

Note that when $D = 0$, we have $\deg(D) = 0$ and $\ell(D) = 1$, so that $\ell(K_C) = g$ after re-arrangement.

Proposition 2.7.2. *Let C/k be a smooth projective curve of genus 1, then there exists $a_1, \ldots, a_6 \in k$ such that we may embed C into $\mathbb{P}^3_k$ by*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Proof. To begin, notice by Riemann-Roch that the canonical divisor is trivial as it must have dimension 1. Next, choose a point $O \in E$, consider $\ell(nO)$ for $n \geq 0$. Since nO is effective, there is certainly no $f \in K(C)^*$ for which $\operatorname{div}(f) - nC$ has no poles anywhere, and so $\ell(-nO) = 0$. Therefore, now applying Riemann-Roch again, we may conclude $\ell(nO) = n$ for all $n \geq 1$

Next, let's go through the construction of $L(nO)$ for each $n \geq 0$.

When $n = 1$, we simply have $L(nO) = \mathrm{Span}_k\{1\}$.

For $n = 2$, we may then obtain some $x \in K(C)^*$ such that $2O + \mathrm{div}(x) \geq 0$. From this point, we also note that $2mO + \mathrm{div}(x^m) \geq 0$. Now our space is $L(2O) = \mathrm{Span}_k\{1, x\}$.

For $n = 3$, we may necessarily obtain an additional $y \in K(C)^*$ such that $3O + \mathrm{div}(y) \geq 0$. From this point, we also note that $3mO + \mathrm{div}(y^m) \geq 0$. Now our space is $L(3O) = \mathrm{Span}_k\{1, x, y\}$.

At $n = 4$, we finally may obtain a new rational function from our previous basis. It then suffices to take $L(4D) = \mathrm{Span}_k\{1, x, y, x^2\}$.

Likewise, at $n = 5$, the section $xy \in K(C)^*$ will suffice, bringing us up to $L(5D) = \mathrm{Span}_k\{1, x, y, x^2, xy\}$.

Finally, for $n = 6$, we have reached a conflict since we know of seven sections in $K(C)^*$ which belong to $L(6O)$, but $\ell(6O) = 6$. Thus, we may obtain some $a_1, \ldots, a_6 \in k$ such that

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

With these rational functions, we take $\varphi : C \to \mathbb{P}^2$ to be the rational map given as

$$\varphi(P) = (x(P) : y(P) : 1).$$

It can be deduced from Theorem A.4.2.4 of [HS13] that $3O$ is very ample, and hence we obtain our desired result.

□

Assuming the defining field is not of characteristic 2 or 3, by following the proof of

Theorem A.4.4.1 in [HS13], We may also write our defining equation in *Weierstrass form* by

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

The fact that C is non-singular is equivalent to the condition that $4a^3 + 27b^2 \neq 0$, an assumption we will often make. We may also use this form of the equation to analyze a rational point $P = (x_P : y_P : 1) \in C(\mathbb{Q})$. By substituting into our Weierstrass equation and clearing denominators, we may determine that we can write $x_P = A_P/D_P^2$ and $y_P = B_P/E_P^3$ in reduced form.

Fix a point $O \in C$ and consider a mapping on the closed points of C to $\mathrm{Pic}^0(C)$, divisors of degree zero in the equivalence class, by $P \mapsto P - O$. Note that for any pair of points $P, Q \in C$, by Bézout's Theorem (Corollary I.7.8 of [Har13]), the line through P and Q passes through a third point R, up to multiplicity. If we take L to be the rational function associated to this line, then by dividing by the line T which vanishes to order 3 at O, we obtain in our Picard group that

$$\mathrm{div}(L/T) + 3O = P + Q + R.$$

Therefore, as $(P - O) + (Q - O) + (R - O)$ is the identity in $\mathrm{Pic}^0(P)$, this grants us a group law that $P + Q = -R$.

3 Height Functions

3.1 Projective Height Functions

As with our initial result from [BCZ02], a key element to characterizing our result was the arithmetic complexity of a given integer. While it is simple in the case of integers, we note that we may easily and naturally extend our notion of arithmetic complexity. We follow closely the work of [HS13] throughout the next few sections.

As an example, consider Roth's theorem, as cited from [HS13], mentioned previously.

Theorem 3.1.1 (Roth's Theorem). *Given an algebraic number $\alpha \in \mathbb{R}$, for any $\varepsilon > 0$, there exist at most finitely many co-prime integers $p, q \in \mathbb{Z}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{|q|^{2+\varepsilon}}.$$

In this example, we have a notion on the arithmetic complexity of a fraction p/q by taking its denominator. It should be noted that only the denominator is considered in this expression of Roth's theorem due to the common analysis of reals in the interval $[0, 1)$. For completeness, we may more symmetrically examine $\max(|p|, |q|)$.

However, looking at only this norm on the rationals is only half of the picture. We recall that for each prime $p \in \mathbb{Z}$, that $\mathbb{Z}_{(p)}$ is a discrete valuation ring with $p\mathbb{Z}_{(p)}$ the unique maximal ideal. From this, we obtain a function

$$\mathrm{ord}_p : \mathbb{Z}_{(p)} \setminus \{0\} \to \mathbb{N}$$

such that $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$, $\mathrm{ord}_p(p) = 1$, and $\mathrm{ord}_p(x) = 0$ for any $x \notin p\mathbb{Z}_{(p)}$. Clearly, this corresponds to our notion of the unique power of p in the unique prime factorization of a given integer.

Extending this to the field of fractions by preserving our additive rule, we obtain a new *p-adic norm* on our rational numbers given for $a \in \mathbb{Q} \setminus \{0\}$ as $|a|_p = p^{-\mathrm{ord}_p(a)}$ and $|0|_p = 0$. We may also note one interesting quirk when verifying our triangle inequality that we rather find an *ultrametric inequality.* For any $a, b \in \mathbb{Q}$, we may show that $|a+b|_p \leq \max\{|a|_p, |b|_p\}$, which easily follows as a result of unique prime factorization. Due to this, the natural numbers are obviously bounded, and hence we refer to such absolute values as *non-archimedean* while our usual absolute value is *archimedean.* We refer to the collection of norms on $\mathbb{Q}$ by the set $M_{\mathbb{Q}}$ and use the notation $|\cdot|_v$ to represent the v-norm.

With this, we are ready to define the height of a rational number $r \in \mathbb{Q}$. Looking instead at the rational point $(r : 1) \in \mathbb{P}^1$, which can be re-expressed with co-prime integer coordinates $(a : b)$, we set

$$H_{\mathbb{Q}}(a : b) = \prod_{v \in M_{\mathbb{Q}}} \max\{|a|_v, |b|_v\}.$$

While this perfectly coincides with our original definition for $\gcd(a, b) = 1$, we also note that this norm is perfectly invariant to the scaling of coordinates as we'd expect for $\mathbb{P}^1$. This definition can be easily extended to higher dimensional projective spaces by taking a maximum over more coordinates.

Next, let's mention how we can extend our notion of algebraic complexity to finite field extensions $k/\mathbb{Q}$. We begin with our non-archimedean norms, denoted M_k^0. Setting R_k as our ring of integers and fixing a prime ideal $P \in \operatorname{Spec}(R)$, note that $R_{k,P}$ is likewise a local ring with a valuation. Therefore, we may similarly obtain a homomorphism $\operatorname{ord}_P : k^* \to \mathbb{Z}$.

In order to now find an exponential base, we will use $N_{k/\mathbb{Q}}(\mathfrak{p}) = |R_k/\mathfrak{p}|$. With this, we take for $x \in k^*$,

$$\|x\|_{\mathfrak{p}} = N_{k/\mathbb{Q}}(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(x)},$$

and of course $\|0\|_{\mathfrak{p}} = 0$. In this way, as $R_k/\mathfrak{p}$ is a finite field and $\operatorname{Spec}(R_k) \to \operatorname{Spec}(\mathbb{Z})$ puts R_k over some prime $p \in \mathbb{Z}$, we may define all of our p-adic norms on k. Pay special attention to this case as if $p \in \mathbb{Z}$ is still prime in R_k, then $N_{k/\mathbb{Q}}(pR_k) = p^{[k:\mathbb{Q}]}$, so it is not the case that $\|x\|_{pR_k} = |x|_p$ for $x \in \mathbb{Q}$.

However, we also usually have more than one archimedean norm on k as well. In fact, we obtain one for each real embedding of $k \to \mathbb{R}$, as well as one for each pair of conjugate complex embeddings $k \to \mathbb{C}$. Once a particular embedding $\rho : k \to \mathbb{C}$ is chosen, we simply take for $x \in k$

$$\|x\|_\rho = |\rho(x)|^{n_\rho},$$

where $n_\rho = [\mathbb{F} : \mathbb{R}]$ with $\mathbb{F} = \mathbb{C}$ for a complex embedding and $\mathbb{F} = \mathbb{R}$ for a real embedding. We commonly denote the archimedean norms on k as M_k^∞.

Finally, with an understanding of the set of places M_k of a finite field extension $k/\mathbb{Q}$, we may define our relative heights with respect to a choice of coordinates on $\mathbb{P}^n$. Note that k-rational points in $\mathbb{P}^n$ may be thought of as any point who has some choice of coordinates all lying k.

Definition 3.1.2. Let $k/\mathbb{Q}$ be a finite field extension. For a point $P = (a_0, \ldots, a_n) \in \mathbb{P}^n(k)$, we define the *multiplicative height* as

$$H_k(P) = \prod_{v \in M_k} \max\{\|a_0\|_v, \ldots, \|a_n\|_v\}.$$

We also define the *logarithmic hieght* as $h_k(P) = H_k(P)$.

We also attribute a more general height on our projective space.

Definition 3.1.3. The *absolute multiplicative height* $H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [1, \infty)$ is given by

$$H(P) = H_k(P)^{\frac{1}{[k:\mathbb{Q}]}},$$

where $P \in \mathbb{P}(k)$ and choice of finite extension $k/\mathbb{Q}$ is arbitrary. We similarly define the *absolute logarithmic height* $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty)$ as $h(P) = \log H(P)$.

Let's show that these height functions are well-defined irrespective of homogeneous coordinates or choice of field for our absolute heights. First, we recount an important fact regarding absolute values.

Lemma 3.1.4 (Product formula)**.** *Let $k/\mathbb{Q}$ be a finite field extension. For any $x \in k^*$, we have*

$$\prod_{v \in M_k} \|x\|_v = 1.$$

Proof. We note that this is clearly true for $k = \mathbb{Q}$ as each p-adic norm will divide out by the part of a rational lying over p. To verify for a field extension $k/\mathbb{Q}$ with ring of integers R_k, consider by the fact that R_k is a Dedekind domain (Theorem 3.1 in [Neu13]) that for any $x \in k^*$,

$$xR_k = \prod_{i=1}^{r} \mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}(x)}.$$

By taking norms, we find

$$|N_{k/\mathbb{Q}}(x)| = N_{k/\mathbb{Q}}(xR_k) = \prod_{i=1}^{r} N_{k/\mathbb{Q}}(\mathfrak{p}_i)^{\mathrm{ord}_{\mathfrak{p}_i}(x)}.$$

Therefore, once we consider a particular prime $p \in \mathbb{Z}$, as each p-adic norm corresponds to the primes lying over p, we must have

$$\begin{aligned}
|N_{k/\mathbb{Q}}(x)|_p &= \prod_{i=1}^{r} |N_{k/\mathbb{Q}}(\mathfrak{p}_i)^{\mathrm{ord}_{\mathfrak{p}_i}(x)}|_p \\
&= \prod_{\substack{P \in \mathrm{Spec}(R_k) \\ x, p \in \mathfrak{p}}} N_{k/\mathbb{Q}}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)} \\
&= \prod_{\substack{v \in M_k \\ v \mid p}} \|x\|_v.
\end{aligned}$$

This similarly holds for archimedean extensions of the usual absolute value on $\mathbb{Q}$ as well. In the following calculation, note that the squaring of absolute values associated to complex embeddings can be accounted for as a product of the embedding and its conjugate, and that the norm of an algebraic number of $\mathbb{Q}$ is often defined as the product of all embeddings.

Putting this together with Proposition 2.6 of [Neu13] grants us

$$\prod_{v|\infty} \|x\|_v = \prod_{\sigma:k\to\mathbb{C}} |\sigma(x)|_\infty = |N_{k/\mathbb{Q}}(x)|_\infty.$$

With our identity true for all places $M_{\mathbb{Q}}$, we conclude

$$\begin{aligned}\prod_{v\in M_k} \|x\|_v &= \prod_{v_0\in\mathbb{Q}} \prod_{\substack{v\in M_k \\ v|v_0}} \|x\|_v \\ &= \prod_{v_0\in\mathbb{Q}} |N_{k/\mathbb{Q}}(x)|_{v_0} \\ &= 1.\end{aligned}$$

□

Also, we recall the fundamental identity found in Proposition 8.2 of [Neu13].

Lemma 3.1.5. *Let k'/k be a finite extension of number fields with rings of integers $R_{k'}$ and R_k. Suppose that $\mathfrak{p} \in \operatorname{Spec}(R_k)$ has the following unique decomposition over $R_{k'}$*

$$\mathfrak{p}R_{k'} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

Moreover, for each $1 \le i \le r$, as $R_k/\mathfrak{p}$ may be regarded as a subfield of $R_{k'}/\mathfrak{p}_i$, take

$$f_i = [R_{k'}/\mathfrak{p}_i : R_k/\mathfrak{p}].$$

Then the following fundamental identity holds

$$\sum_{i=1}^{r} e_i f_i = [k' : k].$$

Now, we may confirm that our height functions are well-defined.

Proposition 3.1.6. *Fix a finite field extended $k/\mathbb{Q}$ and fix some point $P \in \mathbb{P}^n(k)$. Then the height $H_k(P)$ is independent of choice of homogeneous coordinates. Moreover, if k'/k is an additional finite extension, then $H_{k'}(P) = H_k(P)^{[k':k]}$ and hence our absolute height is well-defined.*

Proof. We begin by verifying our first claim. Choose some coordinate $P = (a_0, \ldots, a_n)$ and consider some non-zero scalar $c \in k^*$. Then, using our product formula,

$$\begin{aligned}\prod_{v \in M_k} \max\{\|ca_0\|_v, \ldots, \|ca_n\|_v\} &= \prod_{v \in M_k} \|c\|_v \max\{\|a_0\|_v, \ldots, \|a_n\|_n\} \\ &= \left(\prod_{v \in M_k} \|c\|_v\right)\left(\prod_{v \in M_k} \max\{\|a_0\|_v, \ldots, \|a_n\|_v\}\right) \\ &= \prod_{v \in M_k} \max\{\|a_0\|_v, \ldots, \|a_n\|_v\}.\end{aligned}$$

Next, let's inspect $H_{k'}(P)$ given below as

$$H_{k'}(P) = \prod_{v \in M_{k'}} \max\{\|a_0\|_v, \ldots, \|a_n\|_v\}.$$

To analyze this with respect to the absolute values on our base field, let's break down this product by absolute values on k' which lie over a particular absolute value on k,

$$H_{k'}(P) = \prod_{v \in M_k} \prod_{\substack{w \in M_{k'} \\ w|v}} \max\{\|a_0\|_w, \ldots, \|a_n\|_w\}.$$

To proceed, let's consider the cases of an archimedean or non-archimedean absolute value. If $w \in M_{k'}$ extending $v \in M_k$ corresponds to some embedding $\sigma' : k' \to k'_w$, then v would correspond to $\sigma : k \to k_v$, where $k'_w, k_v = \mathbb{C}$ or $\mathbb{R}$ and $k_v \subseteq k'_w$. Hence, for any $x \in k$,

$$\|x\|_w = |\sigma'(x)|^{[k'_w:\mathbb{R}]} = |\sigma(x)|^{[k'_w:k_v]\cdot[k_v:\mathbb{R}]} = \|x\|_v^{[k'_w:k_v]}.$$

With this, we find for the component of our product extending the archimedean values that

$$\begin{aligned}\prod_{v\in M_k^\infty}\prod_{\substack{w\in M_{k'}\\ w|v}}\max\{\|a_0\|_w,\dots,\|a_n\|_w\} &= \prod_{v\in M_k^\infty}\prod_{\substack{w\in M_{k'}\\ w|v}}\max\{\|a_0\|_v,\dots,\|a_n\|_v\}^{[k'_w:k_v]}\\ &= \prod_{v\in M_k^\infty}\max\{\|a_0\|_v,\dots,\|a_n\|_v\}^{[k':k]},\end{aligned}$$

following simply from the fact that $[k':k]$ is the number of embeddings $k'\to\mathbb{C}$ which extend an embedding of $k\to\mathbb{C}$, and $[k'_w:k_v]$ ensures we count twice for each complex embedding and its conjugate when extending a real embedding by a complex one.

Next, let $P'\in\operatorname{Spec}(R_{k'})$ lie over $P\in\operatorname{Spec}(R_k)$. Then, as we may view R_k/P as a subfield of $R_{k'}/P'$, we may calculate

$$\begin{aligned}N_{k'/\mathbb{Q}}(\mathfrak{p}') &= |R_{k'}/\mathfrak{p}'|\\ &= |R_k/\mathfrak{p}|^{[R_{k'}/\mathfrak{p}':R_k/\mathfrak{p}]}\\ &= N_{k/\mathbb{Q}}(P)^{[R_{k'}/\mathfrak{p}':R_k/\mathfrak{p}]},\end{aligned}$$

where $f=[R_{k'}/\mathfrak{p}':R_k/\mathfrak{p}]$ is the inertia degree of $\mathfrak{p}'$ over $\mathfrak{p}$. Moreover, if e is the ramification index of $\mathfrak{p}'$ over $\mathfrak{p}$ in the factorization of $\mathfrak{p}R_{k'}$, then it is clear that $\operatorname{ord}_{\mathfrak{p}'}(x)=e\operatorname{ord}_{\mathfrak{p}}(x)$ for any $x\in k^*$. Therefore,

$$\|x\|_w = N_{k'/\mathbb{Q}}(P')^{-\operatorname{ord}_{\mathfrak{p}'}(x)} = N_{k/\mathbb{Q}}(P)^{-ef\operatorname{ord}_{\mathfrak{p}}(x)} = \|x\|_v^{ef}.$$

With this line of reasoning, using e_w and f_w to correspond to the ramification index and inertia degree of the primes associated to $w|v$, we may use our earlier fundamental identity to show

$$\prod_{v \in M_k^0} \prod_{\substack{w \in M_{k'} \\ w|v}} \max\{\|a_0\|_w, \dots, \|a_n\|_w\} = \prod_{v \in M_k^0} \prod_{\substack{w \in M_{k'} \\ w|v}} \max\{\|a_0\|_v, \dots, \|a_n\|_v\}^{e_w f_w}$$

$$= \prod_{v \in M_k^0} \max\{\|a_0\|_v, \dots, \|a_n\|_v\}^{[k':k]}.$$

Finally, putting these two cases together

$$H_{k'}(P) = \prod_{v \in M_k} \max\{\|a_0\|_v, \dots, \|a_n\|_v\}^{[k':k]} = H_k(P)^{[k':k]}.$$

□

As one more note, we also find that our projective heights don't change significantly by change of coordinates. Indeed, if $A : k^{n+1} \to k^{m+1}$ is an injective linear map, then for any $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$, we may define a constant $M > 0$ such that

$$\max_{0 \leq j \leq m} \left\| \sum_{i=0}^{n} A_{i,j} a_i \right\|_v \leq M \max_{0 \leq i \leq n} \|a_i\|_v.$$

Indeed, we may simply take

$$M = \max_{v \in M_k} \sum_{i=0}^{n} \sum_{j=0}^{m} \|A_{i,j}\|_v,$$

which makes sense over all places since there's only finitely many which don't evaluate to $(n+1)(m+1)$. Also, because our map was invertible on its image, there is some $N > 0$ which satisfies for all $(a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$ that

$$\max_{0 \leq j \leq m} \left\| \sum_{i=0}^{n} A_{i,j} a_i \right\|_v \geq N \max_{0 \leq i \leq n} \|a_i\|_v.$$

Using our product rule on these two bounds, it is immediate that we find $h(A(P)) = h(P) + O(1)$ for all $P \in \mathbb{P}^n$, with the implied constant independent of P.

3.2 Weil's Height Machine

With a notion for the arithmetic complexity of a point in projective space established, we are now ready to extend this definition considerably. Indeed, there exists a very natural method to extend to a much wider class of geometries.

Definition 3.2.1. Let $\varphi : X/k \to \mathbb{P}^n$ be a morphism. We may take the *(absolute logarithmic) height on X relative to φ* as $h : V(\overline{\mathbb{Q}}) \to [0, \infty)$ defined by $h_\varphi(P) = h(\varphi(P))$.

One should note that for a given quasi-projective variety over $\overline{\mathbb{Q}}$, there are always many maps which one can construct to projective space. This does make sense, however, since arithmetic complexity will naturally depend on the choices we are using to analyze our space, just as much as it matters where we fix the origin on the number line when setting up height functions for the abstract curve $\mathbb{P}^1(\mathbb{Q})$ itself. Fortunately, when our choices of maps are similar with respect to the underlying geometry, there is a strong relationship between the resulting height functions.

Indeed, for a projective variety X/k, when $\varphi : X \to \mathbb{P}^n$ and $\psi : X \to \mathbb{P}^m$ are morphisms for which $\mathcal{L}_1 = \phi^*\mathcal{O}_{\mathbb{P}^n}(1)$ and $\mathcal{L}_2 = \psi^*\mathcal{O}_{\mathbb{P}^m}(1)$ are isomorphic, we in particular have $\Gamma(X, \mathcal{L}_1) \cong \Gamma(X, \mathcal{L}_2)$ as a $k = \Gamma(X, \mathcal{O}_X)$ module. Thus, we may express the generating global sections of one module as a linear combination of global sections from another. Then regarding these sheaves of modules as a $\mathcal{O}_X$-module of $K(X)$, the associated maps to projective space may be composed with a k-linear map to obtain the other. As a result, we may state the following theorem.

Theorem 3.2.2. *Let X/k be a projective variety and k a number field, and consider two morphisms $\varphi : X \to \mathbb{P}^n$ and $\psi : X \to \mathbb{P}^m$. Suppose as well that $\phi^*\mathcal{O}_{\mathbb{P}^n}(1) \cong \psi^*\mathcal{O}_{\mathbb{P}^m}(1)$. Then there exists some constant $C > 0$ such that for any $P \in X(k)$,*

$$|h_\varphi(P) - h_\psi(P)| \leq C.$$

Proof. In addition to the discussion above, we refer to Theorem B.3.1 of [HS13]. □

Using this fact, let's consider the maps associated to the base point free divisors on some variety X/k. Immediately, we note that the choice of basis for $L(D)$ does not matter up to an $O(1)$ constant by the previous proposition. Also, when $D_1 \sim D_2$ for $D_1, D_2 \in \mathrm{Div}(X)$, it is also immediate that a basis $\{f_0, \dots, f_n\}$ of $L(D_1)$ grants a basis $\{f_0 g, \dots, f_2 g\}$ of $L(D_2)$ provided $D_1 = D_2 + \mathrm{div}(g)$, so these maps agree away from the support of $\mathrm{div}(g)$ since

$$\varphi_D(x) = (f_0(x) : \cdots : f_n(x)) = (f_0(x)g(x) : \cdots : f_n(x)g(x)).$$

Thus, we have a well-defined notion of heights associated to base point divisors in our Picard group up to $O(1)$, which we denote as h_D for any $D \in \mathrm{Div}(X)$.

To extend this a bit, note that for any base point free divisors $D_1, D_2 \in \mathrm{Div}(X)$, if we have $L(D_1) = \mathrm{Span}_k\{f_i\}_{i=0}^n$ and $L(D_2) = \mathrm{Span}_k\{g_j\}_{0=1}^m$, then there is some subset $I \subseteq \{(i,j) : 0 \leq i \leq n, 0 \leq j \leq m\}$ such that $L(D_1 + D_2) = \mathrm{Span}_k\{f_i g_j\}_{(i,j)\in I}$. Using this, and the fact that there is some linear map $A : k^{|I|} \to k^{nm+n+m}$ such that $A((f_i g_j)_{(i,j)\in I}) = (f_i g_j)_{0\leq i\leq n, 0\leq j\leq m}$, for any $P \in X(k)$,

$$\begin{aligned}
[k:\mathbb{Q}]h_{D_1+D_2}(P) &= [k:\mathbb{Q}]h(\phi_{D_1+D_2}(P))(P) \\
&= h(A(\phi_{D_1+D_2}(P))) + O(1) \\
&= \sum_{v\in M_k} \max_{\substack{0\leq i\leq n \\ 0\leq j\leq m}} \log \|f_i(P)g_j(P)\|_v + O(1) \\
&= \sum_{v\in M_k} \max_{0\leq i\leq n} \log \|f_i(P)\|_v + \sum_{v\in M_k} \max_{0\leq j\leq m} \log \|g_j(P)\|_v + O(1) \\
&= [k:\mathbb{Q}](h_{D_1}(P) + h_{D_2}(P)) + O(1),
\end{aligned}$$

implying $h_{D_1+D_2} = h_{D_1} + h_{D_2}$. Therefore, since we find that for any $D \in \mathrm{Div}(X)$, we may always find base point free divisors $D_1, D_2 \in \mathrm{Div}(X)$ for which $D = D_1 - D_2$, we may extend our notion to all such divisors in this additive way, which is well-defined up to $O(1)$. This map is referred to as *Weil's Height Machine*, and we will explore how the geometric and algebraic way the divisor class group behaves on our space correspondingly affects the arithmetic of rational points.

While we have explored additivity, linear equivalence, and some aspects of uniqueness, there are a few other properties which make our height machine very useful.

Theorem 3.2.3. *Let the map $D \mapsto h_D$ be the association of height functions to divisors described above. Letting X and Y be a variety over a number field k and $D_1, D_2 \in \mathrm{Div}(X)$, we have the following properties.*

1. *(Uniqueness) The properties described here force a unique choice of height functions, as constructed above, up to $O(1)$ equivalence. It is in fact possible as well to give effective bounds with respect to the defining equations of varieties, divisors, and morphisms.*

2. *(Normalization) Let $H \subseteq \mathbb{P}^n$ be a hyperplane. Then $h_H = h + O(1)$, where $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty)$ is the absolute logarithmic height.*

3. *(Functiorality) Let $\varphi : X \to Y$ be a morphism of varieties and fix $D \in \mathrm{Div}(Y)$, then $h_{\varphi^* D} = h_D \circ \varphi + O(1)$.*

4. *(Additivity) $h_{D_1 + D_2} = h_{D_1} + h_{D_2} + O(1)$.*

5. *(Linear Equivalence) If D_1 is linearly equivalent to D_2, then $h_{D_1} = h_{D_2} + O(1)$.*

6. *(Positivity) If D_1 is effective and U is an open subset on which none of the global sections of $\mathcal{L}(D)$ vanish then $h_{D_1}|_U \geq O(1)$.*

7. *(Northcott Property) Suppose that D_1 is ample. Then for any finite extension k_2/k and $M > 0$, there are only finitely many $P \in V(k')$ for which $h_D(P) \leq B$.*

Proof. We refer to the proof of Theorem B.3.2 of [HS13] for more details. □

3.3 Local Height Functions

We begin this section by recalling our projective height definition on $\mathbb{P}^1$. Fixing $(x:1) \in \mathbb{P}(k) \setminus \{(0:1)\}$ for some finite extension $k/\mathbb{Q}$, we recall

$$h(x:1) = h(1:x^{-1}) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} \max\{-\log \|x\|_v, 0\}.$$

To simplify things, we may consider for each $v \in M_k$ an associated function $v^+ : k_v^* \to \mathbb{R}_{\geq 0}$ given by $v^+(x) = \frac{1}{[k:\mathbb{Q}]} \max\{-\log \|x\|_v, 0\}$. From here, it is clear that v^+ is morally behaving as minus the logarithm of v-adic distance function from $x \in k_v^*$ to $0 \in k_v$.

In particular, we see that the height $h(x:1)$ is broken down as the v-adic distances from $(x:1)$ to the point $(0:1)$. Fundamentally, this is an interesting example since the divisor given by $(0:1)$ corresponds to the invertible sheaf $\mathcal{O}(1)$, which is exactly the identity embedding on $\mathbb{P}^1$ as we would hope. Overall, we would like to show that we could think of our height functions as the sum of v-adic distances to the divisor in question.

To explore local heights further, fix a base field k which is a finite extension of $\mathbb{Q}$, and let X/k be a projective variety. For each $v \in M_k$, writing k_v as the completion of k with respect to this place and $v : k^\times \to \mathbb{R}$ as the function $v(x) = -\frac{1}{[k_v:\mathbb{Q}_v]} \log \|x\|_v$, we may endow $X(k_v)$ with a minimal topology containing the Zariski open sets, and such that $P \mapsto \log v(f(P))$ is continuous away from the poles and zeroes of $f \in K(x)$.

With this topology, for a given divisor D, we would like to describe a family of functions $(\lambda_v)_{v \in M_k}$ such that

$$\lambda_v : (X \setminus \operatorname{supp}(D))(k_v) \to \mathbb{R}$$

is continuous and roughly approximates the negative logarithm of v-adic distance to D in the sense that if $D|_U$ is given by $\operatorname{div}(f)$, we have

$$\sum_{v \in M_k} |\lambda_v(P) - v(f(P))| = O(1).$$

Definition 3.3.1. Let X/k be a projective variety with k a number field. A family of functions $(\gamma_v)_{v\in M_k}$, with $\gamma_v : X(k_v) \to \mathbb{R}$, is an *$M_k$-constant* when each γ_v is constant and $\gamma_v \neq 0$ for only finitely many $v \in M_k$. If we are given a similar family of functions $(\alpha_v)_{v\in M_K}$ and $(\beta_v)_{v\in M_k}$, we write $\alpha_v = \beta_v + O_v(1)$ if their difference is an M_k-constant.

We also speak towards bounded regions.

Definition 3.3.2. Let X/k be a variety and consider a family of subset $S = (S_v)_{v\in M_k}$ for which $S_v \subseteq X(k_v)$. We say that the family S is *affine M_k-bounded* when there exists some affine open subset $U \subseteq X$ and M_k constant γ, with coordinates $(x_1, \dots, x_n)$, such that for any $v \in M_k$ and $(x_1, \dots, x_n) \in S_v \cap U(k_v)$,

$$\min_{1\leq i\leq n} v(x_i) \geq -\gamma_v.$$

We say that a family S is *M_k-bounded* when we may cover our family with finitely many affine M_k-bounded families.

Proposition 3.3.3. *Let X/k be a projective variety. Then the family $(X(k_v))_{v\in M_k}$ is M_k-bounded.*

Proof. See Proposition 10.1.2 of [Lan13]. □

With the above in mind, we would like to be able to write for a Cartier divisor $D = \{(U_i, f_i)\}$, and associated family $\lambda = (\lambda_v)_{v\in M_k}$ for which we have for all $P \in U_i(k_v)$ which is neither a pole nor zero of f_i,

$$\lambda_v(P) - v(f(P))$$

is continuous and bounded above and below by a predetermined M_k constant on all M_k-bounded families of U_i. This condition simplifies in projective space as we just require that we are bounded by an M_k-constant. We often attribute a family of functions $\alpha_i = (\alpha_{i,v})_{v\in M_k}$ to represent this difference

$$\lambda_v = v \circ f_i + \alpha_{i,v},$$

and would then require that $v \circ f_i f_j^{-1} = \alpha_{j,v} - \alpha_{i,v}$ on the intersections $U_i \cap U_j$. Such functions are referred to as *Weil functions*, or *local height functions*, and we consequently obtain the following properties.

Theorem 3.3.4. *Let X/k be a non-singular projective variety and D a Cartier divisor. A Weil function λ_D associated to D satisfies the following properties.*

1. *(Uniqueness) If λ'_D satisfies the same difference requirement as above, then $\lambda_{D,v} = \lambda'_{D,v} + O_v(1)$.*
2. *(Additivity) For another divisor $E \in \mathrm{Div}(X)$, we have $\lambda_{D_1+D_2,v} = \lambda_{D_1,v} + \lambda_{D_2,v} + O_v(1)$.*
3. *(Functiorality) Given a morphism $\varphi : X \to Y$ of non-singular projective varieties and $E \in \mathrm{Div}(Y)$, we find that $\lambda_{\varphi^* E,v} = \lambda_{E,v} \circ \varphi + O_v(1)$*

Proof. The above properties are given in Proposition 10.2.1, Proposition 10.2.2, and Proposition 10.2.5 of [Lan13]. □

To explore this relationship further, consider the following proposition.

Proposition 3.3.5. *Let X/k be a non-singular projective variety, and let $D, D_1, \dots, D_n \in \mathrm{Div}(X)$ a family of divisors such that $\cap_{1\leq i\leq n}\mathrm{supp}(D_i) = \emptyset$. Then we may calculate for any $v \in M_k$ and $P \in (X \setminus \mathrm{supp}(D))(k_v)$ that*

$$\lambda_{D,v} = \min_{1\leq i\leq n} \lambda_{D+D_i,v}(P),$$

where the minima only takes into account $1 \leq i \leq n$ for which $P \notin \mathrm{supp}(D_i)$.

Proof. See Proposition 10.3.2 in [Lan13]. □

As a consequence, we may construct a Weil function for any divisor. To do so, fix some $D \in \mathrm{Div}(X)$ and choose $E_1, \dots, E_n$ and $F_1, \dots, F_m \in \mathrm{Div}(X)$ such that

$$\bigcap_{1\leq i\leq n} \mathrm{supp}(E_i) = \bigcap_{1\leq j\leq m} \mathrm{supp}(F_i) = \emptyset,$$

and $D+E_i = F_j$ by Lemma 10.3.4 of [Lan13]. Next, taking $f_{i,j} \in K(X)$ such that $\operatorname{div}(f_{i,j}) = F_j - D - E_i$ for each $1 \leq i \leq n$ and $1 \leq j \leq m$, we may use the following proposition to determine that for all $v \in M_k$, $1 \leq i \leq n$, and $P \in (X \setminus \operatorname{supp}(D+E_i))(k)$,

$$\lambda_{-D-E_i,v}(P) = \min_{1\leq j\leq m} \lambda_{F_j-D-E_i,v}(P) = \min_{1\leq j\leq m} v(f_{i,j}(P)),$$

or $\lambda_{D+E_i} = \max_{1\leq j\leq m} -v(f_{i,j}(P))$. With one more application of our proposition, we arrive at

$$\lambda_{D,v}(P) = \max_{1\leq j\leq m} \min_{1\leq i\leq n} -v(f_{i,j}(P)).$$

This is indeed a very useful way to compute local heights. In particular, if we have a hypersurface of $\mathbb{P}^n$ defined by a single equation $F(x_0, \ldots, x_n) = 0$ of degree d, note that we have for each $0 \leq i \leq n$ that

$$d\{x_i = 0\} - \{F(x) = 0\} = \operatorname{div}(x_i^d / F(x)).$$

Since $\cap_{0\leq i\leq n}\{x_i = 0\} = \emptyset$, we then have

$$\lambda_{\{F(x)=0\}}(x) = \max_{0\leq j\leq m} v(F(x)/x_i^d).$$

This very nice computational aspect aside, we also have a few other properties which allow local height functions to apply quite generally. Referring to Theorem B.8.1 of [HS13], we write the following.

Theorem 3.3.6. *Consider a non-singular projective variety X/k with divisor D. Let $D \mapsto \lambda_D$ be the local height machine as described above. We also have the following two properties.*

1. *(Positivity) If D is effective, then $\lambda_{D,v} \geq O_v(1)$.*

2. *(Local to Global Property) We may determine the Weil height h_D by the local heights*

as

$$h_D(P) = \sum_{v \in M_k} \frac{[k_v : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \lambda_{D,v}(P) + O(1).$$

4 Vojta's Conjecture

At the heart of this paper's conclusion lies a conjecture of Vojta. To explore this conjecture further, let's re-examine the Subspace Theorem.

Fix a number field k, with algebraic closure $\overline{k}$ and ring of integers R_k, and let $S \subseteq M_k$ be a finite set of places containing all the archimedean places. Let's also consider a set of linearly independent linear forms $L_0, \ldots, L_n \in \overline{k}[x_0, \ldots, x_n]$. Taking $\delta > 0$, our inequality of the Subspace Theorem is

$$\prod_{i=0}^{n} \prod_{v \in S} \|L_n(x_0, \ldots, x_n)\|_v \geq (\max_{0 \leq i \leq n, v \in M_k^\infty} \|x_i\|_v)^{-\delta},$$

for all $x_0, \ldots, x_k \in R_k$ except for those solutions contained in finitely many hyperplanes. However, notice that through scaling both sides of the inequality by the same constant, this inequality may be viewed for points of $\mathbb{P}^n(k)$ except for an exceptional union of hyperplanes denoted Z.

To proceed, we note by Lemma 2.2.2 of [Voj06] that

$$\max_{0 \leq i \leq j, v \in M_K^\infty} \|x_i\|_v \ll H_k(x)$$

So we may generally write that outside of Z we have for $\varepsilon > 0$ sufficiently small that

$$\prod_{i=0}^{n} \prod_{v \in S} \|L_n(x)\|_v \geq H(x)^{-\varepsilon}.$$

Notice as well that this reformulation is independent of our base field k, so long as it is still a finite extension of $\mathbb{Q}$.

Next, consider the divisor $D = \{L_0 \cdots L_n = 0\}$. We know for each $v \in M_k$ that our corresponding local height function can be written out as

$$\lambda_{D,v}(x) = \log \max_{1 \leq j \leq n} \left\| \frac{x_j^{n+1}}{L_0(x) \cdots L_n(x)} \right\|_v = \log \max_{1 \leq j \leq n} \prod_{0 \leq i \leq n} \left\| \frac{x_j}{L_i(x)} \right\|_v .$$

Rearranging our main inequality and taking logarithms, we may now write that

$$\sum_{v \in S} \lambda_{D,s}(x) \leq \varepsilon h(x) + (n+1) \sum_{v \in S} \log \max_{0 \leq j \leq n} \|x_j\|_v.$$

To simplify this, note that $\log \max_{0 \leq j \leq n} \|x_j\|_v \geq O(1)$ for any $v \in M_k^0$. To see why, recall that the class group of R_k is finite, and so we may fix a subset of small primes to which we scale our coordinates to having potentially positive division at. Therefore, we may replace the sum over the places in S with the full sum over all of M_k while preserving inequality.

Lastly, note that on $\mathbb{P}^n$, our canonical divisor $K_{\mathbb{P}^n}$ is given by the invertible sheaf $\mathcal{O}(-n-1)$, and so we may replace $-(n+1)h(x) = h_{K_{\mathbb{P}^n}}(x) + O(1)$ to obtain

$$\sum_{v \in S} \lambda_{D,s}(x) + h_{K_{\mathbb{P}^n}}(x) \leq \varepsilon h(x) + O(1).$$

With the above, we have found that the Subspace Theorem is actually a geometrical result on the space $\mathbb{P}^n$. To explore this relationship in more generality, let's go over some terminology.

Definition 4.0.1 (Proximity Function and Counting Function)**.** Given a divisor D and a finite set of places $S \subseteq M_k$ for a number field k, we denote the *proximity function* $m_S(D, P)$ for each $P \notin \operatorname{supp}(D)$ as

$$m_S(D, P) = \sum_{v \in S} \lambda_{D,s}(x).$$

Intuitively, this is minus the logarithm of the distance from P to D on the places S of interest.

We similarly define the complimentary *counting function* $N_S(D, P)$ for each $P \notin \operatorname{supp}(D)$

as

$$N_S(D,P) = \sum_{v \notin S} \lambda_{D,s}(x) = h_D(P) - m_S(D,P)$$

Definition 4.0.2 (Normal Crossings Divisor)**.** A *strict normal crossings divisor* D on a non-singular scheme X is an effective Cartier divisor D, such that for any $P \in D$ as a closed subscheme, there is a $\kappa(P)$ basis for $\mathfrak{m}_P/\mathfrak{m}_P^2$ with representatives $f_1, \dots, f_d \in \mathfrak{m}_P \setminus \mathfrak{m}_P^2$ for which D is cut out by $f_1, \dots f_r$ in $\mathcal{O}_{X,P}$ for some $1 \leq r \leq d$.

Remark. Normal crossings divisors generalize the concept of hyperplanes in general position. Indeed, for a projective non-singular variety X, we may take a choice of coordinates of the surrounding projective space for which each hyperplane is some coordinate vanishing, and then these coordinates also generate any particular maximal ideal $\mathfrak{m}_P$ for $P \in X$.

Definition 4.0.3. (Big Divisor) A divisor L is said to be *big* if nL is the sum of an effective divisor and ample divisor for sufficiently large n.

Let's now state Vojta's conjecture in more generality.

Conjecture 4.0.4. *(Vojta's Conjecture) Let X/k be a non-singular projective variety and k a number field. We will also take A to be a big divisor on X, D a normal crossings divisor on X, and K the canonical divisor class on X. Then for any $\varepsilon > 0$, there exists a proper closed subset Z, depending on all choices made, such that for any $P \notin Z$*

$$m_S(D,P) + h_K(P) \leq \varepsilon h_A(P) + O(1).$$

While not much is known with respect to particular cases of Vojta's conjecture, we have the following result from [McK03] which is applicable to our next section.

Theorem 4.0.5. *Let C/k be a smooth elliptic curve where the group $C(\mathbb{Q})$ is rank one. Suppose that there exists a birational k-morphism $f : X \to C \times C$, where X is a non-singular, projective k-scheme. Moreover, suppose that the image of the exceptional set is* *contained in a finite subset of $(C \times C)(k)$. If L is a big divisor on X, D is the zero divisor with trivial height function, and K_X is the canonical divisor, then for any $\varepsilon > 0$, there exists an effectively computable proper closed subset $Z \subseteq X$ for which $P \in (X \setminus Z)(k)$ implies that*

$$h_K(P) \leq \varepsilon h_L(P) + O(1).$$

5 Application to GCD Problems

5.1 Generalized GCD

With our toolkit in place, let's now dive into some generalizations of the GCD. Consider two integers $a, b \in \mathbb{Z}$. We recall that

$$\gcd(a,b) = \prod_{p \text{ prime}} p^{\min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}}.$$

Re-arranging the above expression, and recalling some notation from the section on local heights, we have

$$\log \gcd(a,b) = \sum_{v \in M_{\mathbb{Q}}^0} \min\{v^+(a), v^+(b)\}.$$

Notice as well that for the usual archimedean absolute value on $\mathbb{Q}$ that for $x \in \mathbb{Z}$

$$v_\infty^+(x) = \max(-\log |x|_v, 0) = 0,$$

so our sum may as well be over all places of $M_{\mathbb{Q}}$.

This strongly suggests that the GCD could be generalized by considering the minus logarithm of the v-adic distance to $(0,0)$ (abusing notation for an affine piece of $\mathbb{P}^1$), using the tools of local heights. However, we run into the immediate pitfall that if we are considering $(a,b) \in (\mathbb{P}^1 \times \mathbb{P}^1)(\mathbb{Q})$, then $(0,0)$ is of co-dimension 2 and not a divisor.

Fortunately, the situation can still be recovered and generalized easily. The key idea is that blowing up $\mathbb{P}^1 \times \mathbb{P}^1$ at the point $(0,0)$ yields an exceptional divisor, which we can use for constructing local heights.

Definition 5.1.1 (Generalized GCD)**.** Suppose X/k is a smooth variety, with a closed subvariety Y of co-dimension at least 2. Let $\pi : \widetilde{X} \to X$ be the blowup of X along Y, and take $E = \pi^{-1}(Y)$ to be the exceptional divisor. We may then define the *generalized* *logarithmic greatest common divisor* for a point $P \in (X \setminus Y)(k)$ as

$$h_{\mathrm{gcd},Y}(P) = h_{\widetilde{X},E}(\pi^{-1}(P)).$$

Let's re-examine our motivating example to see how this definition plays out. Consider the following special case of Lemma 2.5.2 of [Voj06].

Lemma 5.1.2. *Let X/k be a non-singular variety of dimension at least 2 and consider a closed point $Y \in X(\overline{k})$. Suppose as well that Y is given as the intersection of finitely many effective divisors $\{D_i\}_{i=1}^m$ in the sense that $\mathcal{I}_P \cong \sum_{i=1}^m \mathcal{L}(-D_i)$. If $\pi : \widetilde{X} \to X$ is the blowing up of X with respect to Y with exceptional divisor $E = \pi^{-1}(Y)$, then the local Weil height for any $P \in X \setminus Y$ with respect to the divisor E and place $v \in M_k$ is given by*

$$\lambda_{E,v}(\pi^{-1}(P)) = \min\{\lambda_{D_i,v}(P)\}_{i=1}^m.$$

Proof. This is rather intuitive that the v-adic distance to the exceptional divisor could be determined by determining the v-adic distance to the closest divisor containing Y on X. For this, note that $\pi^*D_i = \widetilde{D}_i + E$ with $\cap_{i=1}^m \widetilde{D}_i = \emptyset$, where $\widetilde{D}_i$ is the strict transform of the closed subvariety associated to D_i. Hence, for any $P \in X \setminus Y$ and $v \in M_k$,

$$\lambda_E, v(\pi^{-1}(P)) = \min_{1 \leq i \leq m} \lambda_{\pi^* D}(\pi^{-1}(P)) = \min_{1 \leq i \leq m} \lambda_{D,v}(P).$$

□

We also require one more tool to assist in computation on products of curves.

Lemma 5.1.3. *Let X and Y be curves over an algebraically closed field k. Let $Z = X \times_k Y$ be the product surface with projections $p_1 : Z \to X$ and $p_2 : Z \to Y$. If $p_1(R) = P$ and $p_2(R) = Q$ for closed points $P \in X$, $Q \in Y$, and $R \in Z$, then the ideal sheaf associated to R on Z is isomorphic to $\mathcal{L}(-p_1^*P) + \mathcal{L}(-p_2^*Q)$, where P and Q are effective Cartier divisors.*

Proof. For this, we can work locally and assume that $U = \operatorname{Spec}(A) \subseteq X$, $V = \operatorname{Spec}(B) \subseteq Y$, P is the zero of some $f \in A$ locally, and Q is the zero of some $g \in B$ locally. For ease of variables, we identify each closed point with the associated maximal ideal. As our open neighbourhood of R is $U \times V = \operatorname{Spec}(A \otimes_k B)$, we will determine R as associated to some maximal ideal $A \otimes B$. As $p_1(R) = P$, it should be noted that R contains $f \otimes 1$, and likewise that R contains $1 \otimes g$.

However, we may stop here as for any pure element $a \otimes b \in A \otimes B$, we can determine some $u \in A$ and $v \in B$ for which $au - 1 \in fA$ and $bv - 1 \in gB$, allowing us to write

$$(a \otimes b) \cdot (u \otimes v) = au \otimes bv = (1 + As) \otimes (1 + gB) = 1 \otimes 1 + 1 \otimes gB + fA \otimes 1 + fA \otimes gB.$$

As the sets on the right are contained in $\langle f \otimes 1, 1 \otimes g \rangle$ by closure, we see that $A \otimes B/(f \otimes 1, 1 \otimes g)$ is a field. Consequently, $\langle f \otimes 1, 1 \otimes g \rangle$ is maximal and thus all of R.

With this description, let's now consider what p_1^*P and p_2^*Q are as ideals of $A \otimes_k B$. Fortunately, as these are principal subschemes, we may simply note that they are the vanishing of $f \circ p_1 = f \otimes 1$ and $g \circ p_2 = 1 \otimes g$. Therefore, we obtain that $R = p_1^*P + p_2^*Q$. Moreover, since we may cover X, Y, and Z with patches in this way and the construction agrees on overlaps, it must be the case that $\mathcal{I}_R \cong \mathcal{L}(-p_1^*P) + \mathcal{L}(-p_2^*Q)$. □

Let's go over some examples, ignoring error terms which may be taken as zero by choice of local height functions.

Example. Consider the point $Y = ((0 : 1), (0 : 1))$ in $X = \mathbb{P}^1 \times \mathbb{P}^1$. Let $\pi : \widetilde{X} \to X$ be the blowing up of X along our point Y with exceptional divisor E. Let's also denote $p_1, p_2 : X \to \mathbb{P}^1$ to be our projection maps from our product. From our previous lemmas, we may determine that for any place $v \in M_{\mathbb{Q}}$, we have for any closed point $(a, b) \in (X \setminus Y)(\mathbb{Q})$

that

$$\begin{aligned}\lambda_{E,v}(\pi^{-1}(a,b)) &= \min(\lambda_{p_1^*(0:1),v}(a,b), \lambda_{p_2^*(0:1),v}(a,b)) \\ &= \min(\lambda_{(0:1),v}(a), \lambda_{(0:1),v}(b)) \\ &= \min(v^+(a), v^+(b)).\end{aligned}$$

Therefore, using our local to global property, we find that

$$h_{\text{gcd}}((a,b);Y) = \sum_{v \in M_{\mathbb{Q}}} \min(v^+(a), v^+(b)) = \log \gcd(a,b),$$

exactly as desired.

Example. Take some $f_1, \ldots, f_m \in \mathbb{Z}[x_0, \ldots, x_n]$ to simultaneously vanish at a smooth subvariety $V \subseteq \mathbb{P}^n$ of co-dimension at least 2. We will aim to determine $h_{\text{gcd}}(P;V)$ for a given $P = (a_0 : \cdots : a_n) \in (\mathbb{P}^n \setminus V)(\mathbb{Q})$, where we are assuming that the coordinates have been chosen to be coprime integers. As before, we may write $V = \cap_{1 \le i \le m}\{f_i = 0\}$, and so we find with the full generality of Lemma 2.5.2 from [Voj06] that $h_{\text{gcd}}(P;Q)$ is given by a local height function, for each $v \in M_{\mathbb{Q}}$, as $\min_{1 \le i \le m} \lambda_{\{f_i=0\},v}(P)$.

To analyze these local heights, note that for any $v \in M_{\mathbb{Q}}$ and $1 \le i \le m$ we have

$$\lambda_{\{f_i=0\},v}(P) = \log \max_{0 \le j \le n} \left| \frac{a_j^{d_i}}{f_i(P)} \right|_v = d_i \log \max_{0 \le j \le n} |a_j|_v - \log |f_i(P)|_v,$$

where $d_i = \deg(f_i)$. To simplify this calculation, we find for any rational prime $p \in \mathbb{Z}$, $\max_{0 \le j \le n} |a_j|_p = 1$ by our coprime assumption and so $\lambda_{\{f_i=0\},p}(P) = -\log |f_i(P)|_p$.

Applying our local to global principle and summing over all places $M_{\mathbb{Q}}$, and performing some rearrangements on our local height functions, we may now see that

$$h_{\text{gcd}}(P;V) = \log \left(\min_{1 \le i \le m} \frac{(\max_{0 \le j \le m} |a_j|)^{d_i}}{|f_i(P)|} \right) - \log \left(\prod_{p \in M_{\mathbb{Q}}^0} \max_{1 \le i \le m} |f_i(P)|_p \right).$$

Clearly, the product on the right is simply $\gcd(f_1(P),\ldots,f_m(P))^{-1}$. Referring to Example 4 of [Sil04], we may then write $h_{\gcd}(P;V) = \log\gcd(f_1(P),\ldots,f_m(P)) + O(1)$.

Notation. Let $C/\mathbb{Q}$ be an elliptic curve, with rational point $P = (x_P, y_P) \in C(\mathbb{Q})$. We may then write x_P as A_P/D_P^2, with $\gcd(A_P, D_P) = 1$ and $D_P > 0$.

Example. Consider an elliptic curve C/k with identity $O \in C$. Assume without loss of generality C is given in $\mathbb{P}^2$ as the curve $y^2z = x^3 + Axz^2 + Bz^3$, with $4A^3 + 27B^2 \neq 0$, and our identity point is the intersection with $z = 0$ at $(0:1:0)$. To examine $O \in C$ as an effective Cartier divisor, let's specialize to the affine subspace $y = 1$ on $D_+(y)$ with coordinates $u = x/y$ and $v = z/y$. Therefore, we are equivalently looking for the vanishing $(0,0) \in \operatorname{Spec}(k[u,v]/\langle u^3 + Auv^2 + Bv^3 - v\rangle)$.

The maximal ideal associated to $(0,0)$ is simply $\langle u, v\rangle$. Writing in our function field

$$v = u\frac{u^2 + Av^2}{Bv^2 - 1},$$

since $Bv^2 - 1$ does not vanish at $(0,0)$, we find that u is an uniformizer for the unique maximal ideal of our local ring. Therefore, u vanishes to order 1, and we may similarly show (as expected) that v vanishes to order 3.

With this, on the affine subspace we are interested in of $z = 1$, we see that the function $\frac{z}{x} = x^{-1}$ vanishes to order 2 at O and $2O = \operatorname{div}(x^{-1})$. Using the additivity of our local height functions, for any $v \in M_{\mathbb{Q}}$ and $P \in C(\mathbb{Q})$,

$$\lambda_{O,v}(P) = \frac{1}{2}v^+(x_P^{-1}) = v(D_P).$$

Now, with this calculation and our lemma for heights on blowups, we may show that for any $P, Q \in C(\mathbb{Q})$ not the identity and $v \in M_{\mathbb{Q}}$ that

$$\begin{aligned}\lambda_{E,v}(\pi^{-1}(P,Q)) &= \min(\lambda_{p_1^*O,v}(P,Q), \lambda_{p_2^*O,v}(P,Q))\\ &= \min(\lambda_{O,v}(P), \lambda_{O,v}(Q))\\ &= \min(v(D_P), v(D_Q)),\end{aligned}$$

where $\pi : \widetilde{X} \to C \times C$ is the blowup along (O, O) with exceptional divisor $E = \pi^{-1}(O, O)$. Combined with our local to global principal, we may state that

$$h_{\mathrm{gcd}}((P,Q); (O,O)) = \sum_{v \in M_{\mathbb{Q}}} \min(v(D_P), v(D_Q)) = \log \gcd(D_P, D_Q).$$

5.2 Main Result

We are now ready to go over our main result from [Sil04].

Theorem 5.2.1. *Let X/k be smooth with $Y \subseteq X$ a smooth subvariety of co-dimension $r \geq 2$. Let A be some ample divisor on X, and assume that $-K_X$ is a normal crossings anti canonical divisor such that* $\mathrm{supp}(-K_X) \cap Y = \emptyset$.

Assuming Vojta's conjecture, then for every finite set $S \subseteq M_k$ and any $0 < \varepsilon < r - 1$, there is a closed subvariety $Z \subsetneq X$ and a constant $\delta \in \mathbb{R}$, with δ only depending only on X, Y, and A, such that for any $P \in (X \setminus Z)(k)$

$$h_{\mathrm{gcd}}(P; Y) \leq \varepsilon h_A(P) + \frac{1}{r - 1 + \delta\varepsilon} N_S(-K_X, P) + O(1).$$

Proof. Let $\pi : \widetilde{X} \to X$ be the blow up of X with centre Y and exceptional divisor $\pi^{-1}(Y) = E$. We begin by recalling that the canonical bundle $K_{\widetilde{X}}$ may be described with the given codimension as

$$K_{\widetilde{X}} = \pi^* K_X + (r-1)E,$$

up to linear equivalence. Next, since A is an ample divisor, we may find some $m \geq 1$ and

$\widetilde{A} \in \operatorname{Pic}(\widetilde{X})$ that is ample such that

$$\pi^* A = \widetilde{A} + mE.$$

As $\operatorname{supp}(K_X) \cap Y = \emptyset$, it is clear as well that $-\pi^* K_X$ is a normal crossings divisor as π is an isomorphism at relevant points. Thus, we are ready to apply Vojta's conjecture to $-\pi^* K_X$ and $\widetilde{A}$.

Taking $\varepsilon > 0$ and $S \subseteq M_k$ as above, we may assume that away from some exceptional proper closed subset W, for any $\widetilde{P} \in \widetilde{X} \setminus W$,

$$\begin{aligned} &m_S(-\pi^* K_X, \widetilde{P}) + h_{K_{\widetilde{X}}}(\widetilde{P}) \leq \varepsilon h_{\widetilde{A}}(\widetilde{P}) + O(1) \\ \Rightarrow &- m_S(K_X, \pi(\widetilde{P})) + h_{K_X}(\pi(\widetilde{P})) + (r-1)h_E(\widetilde{P}) \leq \varepsilon h_A(\pi(\widetilde{P})) - \varepsilon m h_E(\widetilde{P}) + O(1) \end{aligned}$$

Next, we may as well assume that $E \subseteq W$, and so there is some $P \in (X \setminus Y)(k)$ such that $\pi(P) = \widetilde{P}$. Recalling our definition of the generalized GCD, and simplifying using the counting function $N_S(-K_X, P)$, we may then write

$$N_S(K_X, P) + (r-1)h_{\mathrm{gcd}}(P; Y) \leq \varepsilon h_A(P) - \varepsilon m h_{\mathrm{gcd}}(P; Y) + O(1).$$

After just one more re-arrangement by grouping terms, and setting $\delta = m$, we finally arrive at

$$h_{\mathrm{gcd}}(P; Y) \leq \frac{\varepsilon}{r - 1 + \delta\varepsilon} h_A(P) + \frac{1}{r - 1 + \delta\varepsilon} N_S(K_X, P) + O(1).$$

□

Notice that the above theorem is indeed a general case of the special result on Vojta's conjecture mentioned in a previous section. Indeed, let C/k be an elliptic curve with identity $O \in C$, and choose any ample A divisor on $X = C \times C$. Notice that since C is an elliptic curve that $K_X = 0$, satisfying our necessary conditions and simplifying our inequality. Moreover, if K is the canonical divisor on $\pi : \widetilde{X} \to X$ blown up at Y, then K is linearly equivalent to the exceptional divisor by our co-dimension and that the canonical sheaf is trivial on X. Thus, we may write for $P \in (X \setminus Y)(k)$

$$h_K(\pi^{-1}(P)) = h_{\mathrm{gcd}}(P; Y) \leq \varepsilon h_A(P) + O(1) = \varepsilon h_{\pi^* A}(\pi^{-1}(P)) + O(1).$$

5.3 Applications of Main Result

Definition 5.3.1. Let S be a finite set of rational primes. For any integer $x \in \mathbb{Z} \setminus \{0\}$, The "prime-to S" part of x, denoted $|x|'_S$, is the unique multiplicative component of x which does not lie over the primes of S. That is,

$$|x|'_S = |x| \cdot \prod_{p \in S} |x|_p = \left(\prod_{p \notin S} |x|_p \right)^{-1}$$

Theorem 5.3.2. *Let $V \subset \mathbb{P}^n$ be a smooth variety of co-dimension $r = n - \dim(V)$ not intersecting any of the hyperplanes $\{x_i = 0\}$ for $0 \leq i \leq n$. Suppose as well that V is given as the vanishing set of some homogeneous polynomials $f_1, \ldots, f_m \in \mathbb{Z}[x_0, \ldots, x_n]$. We will also fix some $0 < \varepsilon$ arbitrarily.*

Suppose that Vojta's conjecture is true in the case of $\mathbb{P}^n$ blown up along V. Then we may determine some non-zero homogeneous polynomial $g \in \mathbb{Z}[x_0, \ldots, x_n]$ depending on the polynomials defining V and ε, as well as a constant δ only depending on $f_1, \ldots, f_m$, so that every coprime integer tuple $(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}$ is either a root of g or

$$\gcd(f_1(a_0, \ldots, a_n), \ldots, f_k(a_0, \ldots, a_n)) \leq \max\{|a_0|, \ldots, |a_n|\}^{\varepsilon} \cdot (|a_0 \cdots a_n|'_S)^{\frac{1}{r-1+\delta\varepsilon}}.$$

Proof. Let $S \subseteq M^0_{\mathbb{Q}}$ be a finite set of rational primes and $\varepsilon > 0$ taken arbitrarily. Note that showing it for $\varepsilon < r - 1$ suffices to prove for $\varepsilon \geq r - 1$, so we also assume this without loss of generality. Using our main result with $X = \mathbb{P}^n$, $Y = V$, and $A = \{x_0 = 0\}$, we may find some proper closed subset $Z \subsetneq \mathbb{P}^n$ and δ depending only on V (assuming $\mathbb{P}^n$ and $\{x_0 = 0\}$ fixed), for which any $P \in (X \setminus Z)(k)$ satisfies

$$h_{\mathrm{gcd}}(P; V) \leq \varepsilon h_A(P) + \frac{1}{r - 1 + \delta\varepsilon} N_{S\cup\{\infty\}}(-K_{\mathbb{P}^n}, P) + O(1).$$

Note we may take some homogeneous $g' \in \mathbb{Z}[x_0, \ldots, x_n]$ for which $D_+(g) \subseteq X \setminus Z$, we may assume that Z is contained in the vanishing of g'. Additionally, as V does not intersect any hyperplane of the form $\{x_i = 0\}$ for $0 \leq i \leq n$, we will assume $g = x_0 \cdots x_n g'$.

To begin, we must consider local height functions for the anti-canonical divisor class $-K_{\mathbb{P}^n} \cong \mathcal{O}(n + 1)$. To do so, for each $0 \leq j \leq m$ we may define local height functions for the divisor $\{x_j = 0\}$ for each $v \in M_k$ and $P \in (\mathbb{P}^n \setminus \{x_j = 0\})(\mathbb{Q})$ as

$$\lambda_{\{x_j=0\},v}(P) = \log\max(|\tfrac{x_0}{x_j}|_v, \ldots, |\tfrac{x_n}{x_0}|_v, 1).$$

By additivity, we may take $\lambda_{-K_{\mathbb{P}^n},v}(P) = \lambda_{\{x_j=0\},v}(P) + \cdots + \lambda_{\{x_n=0\},v}(P)$ away from the set $\{x_0 \cdots x_n = 0\}$, ignoring any $O_v(1)$ terms by this choice of local height function. Note this divisor representative for the anti canonical class is a normal crossings divisor.

If we are given that $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathbb{Q})$ not vanishing on $x_0 \cdots x_n$, assuming without loss of generality that $\gcd(a_0, \ldots, a_n) = 1$, we obtain

$$\begin{aligned} N_{S\cup\{\infty\}}(-K_{\mathbb{P}^n}, P) &= \sum_{p\notin S}\sum_{j=0}^{n} \log\max(|\tfrac{a_0}{a_j}|_p, \ldots, |\tfrac{a_n}{a_j}|_p, 1) \\ &= \sum_{p\notin S}\sum_{j=0}^{n} \big(\log\max(|a_0|_p, \ldots, |a_n|_p) - \log|a_j|_p\big) \\ &= -\log\prod_{p\notin S} |a_0 \cdots a_n|_p \\ &= \log|a_0 \cdots a_n|'_S. \end{aligned}$$

Next, we will take our ample divisor A to be given as the hyperplane $\{x_0 = 0\}$. As the map $\mathbb{P}^n \to \mathbb{P}^n$ given by A may be taken as the identity, we may simply write the formula for projective heights with co-prime integer coordinates as

$$h_A(a_0 : \cdots : a_n) = \log\max(|a_0|, \ldots, |a_n|).$$

Finally, with our result on $h_{\mathrm{gcd}}(P; V)$ as shown in a previous section, we have deduced that for any $(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}$ coprime and not vanishing on g,

$$\begin{aligned} &\log\gcd(f_1(a_0, \ldots, a_n), \ldots, f_m(a_0, \ldots, a_n)) \\ &\qquad\qquad \le \varepsilon\log\max(|a_0|, \ldots, |a_n|) + \frac{1}{r - 1 + \delta\varepsilon}\log|a_0 \cdots a_n|'_S + O(1), \end{aligned}$$

which is a logarithmic version of our desired inequality. □

Remark. It should be noted that this theorem gives a conditional proof of [BCZ02]. Indeed, fix integers $a, b \in \mathbb{Z}$ multiplicatively independent and let $\varepsilon > 0$ be arbitrary. Using $f(x, y, z) = x - z$, $g(x, y, z) = y - z$, and $S = \{p \in M_k^0 : p|ab\}$, we obtain some polynomial $h(x, y, z)$ such that for all $n \ge 1$, either $h(a^n, b^n, 1) = 0$, or

$$\gcd(a^n - 1, b^n - 1) \le \max\{|a|, |b|\}^{\varepsilon n}.$$

Since we have already shown that a polynomial $h(x, y, z)$ may vanish at only finitely many triples $(a^n, b^n, 1)$ without being trivial, the result follows.

Theorem 5.3.3. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation. Assuming Vojta's conjecture for E^2 blown up at (O, O), we then find that for any $\varepsilon > 0$ that there is a proper closed subvariety $Z \subsetneq E^2$ such that for any points $P, Q \in E(\mathbb{Q}) \setminus Z$,*

$$\gcd(D_P, D_Q) \le (H(P) \cdot H(Q))^{\varepsilon},$$

Proof. As before, we begin by using our main result. Set $X = E \times E$, $A = p_1^*O + p_2^*O$,

$Y = (O, O)$, and $S = M_{\mathbb{Q}}^{\infty}$, where $p_1, p_2 : E \times E \to E$ are the projection maps. Since $K_E = 0$ for an elliptic curve, it follows that $K_X = 0$ as well. Therefore, for any $\varepsilon > 0$, there exists some closed subset $Z \subsetneq X$ such that for all $(P, Q) \in (X \setminus Z)(\mathbb{Q})$,

$$h_{\text{gcd}}((P, Q); (O, O)) \leq \varepsilon h_A(P, Q) + O(1).$$

To make a quick understanding this, we start on the left as

$$h_{\text{gcd}}((P, Q); (O, O)) = \log \gcd(D_P, D_Q).$$

On the right, we may use additivity and linearity to find

$$h_A(P, Q) = h_O(P) + h_O(Q) + O(1).$$

Putting these results together, and rephrasing the result exponentially, we obtain our desired result. □

6 Conclusion

While there were many technicalities, we find overall there is particular relationship between the geometry of our spaces and the arithmetic of their rational points. Indeed, while [BCZ02] does initially focus on Diophantine approximation, a reinterpretation of the result under the geometry of $\mathbb{P}^n$ provides a generalization and even conjectures a result when you expand the set of places of $M_{\mathbb{Q}}$ of interest. In a similar vein, McKinnon's theorem ([McK03]) on products of elliptic curves was able to prove a similar result on elliptic curve groups.

When we then generalize to Vojta's conjecture, provided computation of the generalized GCD is available, we have a reliable way of creating such conjectures on the GCD of arithmetic sequences and the geometry which gives rise to them. In these cases, we note that the sequences $(x_n)_{n\geq 1}$, either given as $x_n = a^n - 1$ for some $a \in \mathbb{Z}$, or $x_n = D_{nP}$ with P a rational point of infinite order on an elliptic curve, follow a pattern that if $n|m$, then $x_n|x_m$. Such sequences are referred to as *divisibility sequences*, and Silverman conjectures in [Sil04] that sequences which arise from group schemes in the way of the previous two, should have that the GCD returns to small values infinitely often. However, the question over the integers whether the inequality, stated as

$$\gcd(a^n - 1, b^n - 1) \leq C,$$

holds true for infinitely many $n \geq 1$, assuming a and b multiplicatively independent and $C \geq 1$ arbitrary, is currently a conjecture and not much is known.

A natural improvement on many of these results will be to first convert them into effective arguments, and in this way, more could be concluded from computation alone. However, the cases which are still conditional on unproven cases of Vojta's conjecture remain elusive. If we look to the future with an optimistic lens, we may hope that the relationship between geometry and arithmetic continues to act as both a compass for navigating which results should hold, as well a tool which permits their conclusion.

References

[BCZ02] Yann Bugeud, Pietro Corvaja, and Umberto Zannier. "An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$". In: (2002).

[Eis13] David Eisenbud. *Commutative Algebra. with a View Towards Algebraic Geometry.* Springer, 2013. URL: `https://link.springer.com/book/10.1007/978-1-4612-5350-1`.

[Har13] Robin Hartshorne. *Algebraic geometry.* Springer, 2013. URL: `https://link.springer.com/book/10.1007/978-1-4757-3849-0`.

[HS13] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry. An Introduction.* Springer, 2013. URL: `https://link.springer.com/book/10.1007/978-1-4612-1210-2`.

[Lan13] Serge Lang. *Fundamentals of Diophantine Geometry.* Springer, 2013. URL: `https://link.springer.com/book/10.1007/978-1-4757-1810-2`.

[Mat70] Hideyuki Matsumura. *Commutative Algebra.* W. A. Benjamin Advanced Bk Program, 1970.

[McK03] David McKinnon. "Vojta's Main Conjecture for Blowup Surfaces". In: *Proceedings of the American Mathematical Society* 131.1 (2003), pp. 1–12.

[Neu13] Jürgen Neukirch. *Algebraic Number Theorty.* Springer, 2013. URL: `https://link.springer.com/book/10.1007/978-3-662-03983-0`.

[Sch77] H. P. Schlickewei. "The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt Theorem". In: *Arch. Math.* 29 (1977), pp. 267–270.

[Sil04] Joseph H. Silverman. "Generalized Greatest Common Divisors, Divisibility Sequences, and Vojta's Conjecture for Blowups". In: (2004). arXiv: `math/0407415 [math.NT]`.

[Vak22] Ravi Vakil. *The Rising Sea. Foundations of Algebraic Geometry*. 2022. URL: `https://math.stanford.edu/~vakil/216blog/FOAGaug2922public.pdf`.

[Voj06] Paul Vojta. *Diophantine Approximations and Value Distribution Theory*. Springer, 2006. URL: `https://link.springer.com/book/10.1007/BFb0072989`.