Universiteit Utrecht

Counting points of bounded height over global function fields

Mathematical sciences

Master thesis

Luke van de Kraats

Supervisor
Dr. M. Pieropan

Second reader
Prof. dr. G.L.M. Cornelissen

Academic year 2024

Abstract

In analytic number theory one can use the classical Riemann zeta function to solve certain counting problems, for example the Prime number theorem is equivalent to the fact that the Riemann zeta function is non-zero for some specific values. For the ring of polynomials over a finite field, we can define a similar zeta function which we can use to solve counting problems over global function fields. One may define a height function on global function fields, which gives a means of measuring the 'size' of a point. Using standard applications of Tauberian theorems we will show that the size of the set of points of bounded height is finite, and in particular how it behaves asymptotically, by computing the rightmost pole of the zeta function and its order. Later we will discuss how this asymptotic behavior changes when we require our points to satisfy certain arithmetic properties.

Contents

1 Introduction

1.1 Global function fields

In algebraic number theory one is interested in the study of integers, rational numbers and number fields and their properties. We can use this theory to resolve question, like the existence of solutions to Diophantine equations. One ring that has many properties in common with the ring of integers, is the polynomial ring over the finite field $\mathbb{F}_q$, where q is a power of a prime number. Since the ring $\mathbb{F}_q[T]$ shares a lot of properties with $\mathbb{Z}$, one may look at its quotient field $\mathbb{F}_q(T)$.

We define a global field as a field that is one of two types, algebraic number fields, which are finite extensions of $\mathbb{Q}$, and global function fields. Global function fields are function fields of irreducible algebraic curves over finite fields. This is equivalent to a finite extension of $\mathbb{F}_q(T)$. If we want to study irreducible algebraic curves one may look at finite extensions of $\mathbb{F}_q(T)$.

If we define a height function H on $\mathbb{P}^n(\mathbb{F}_q(T))$, one may want to know the answer to certain questions about the set of points of bounded height,

$$\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H(x) \leq B\},$$

such as: What is the cardinality of this set? If it is not empty, is it finite or infinite? If the size is finite, can one predict the growth rate of the set as $B \to \infty$. The goal of this thesis is to study the last question. In particular, what happens if we require the point $x \in \mathbb{P}^n(\mathbb{F}_q(T))$ to satisfy certain additional properties, which will be discussed later.

1.2 Content of the thesis

In Chapter 2 we start by looking at the ring $\mathbb{F}_q[T]$. This ring has many properties in common with the ring of integers $\mathbb{Z}$. We discuss what the prime elements of the ring $\mathbb{F}_q[T]$ are. Furthermore we will show that this ring is a unique factorization domain. We will see that the ring $F_q[T]$ has analogous results to many classical number theoretic results, like the Chinese remainder theorem and the little theorems of Euler and Fermat.

Then in Chapter 3, we define the zeta function, ζ_A, for the the ring $\mathbb{F}_q[T]$. We can write ζ_A as a product over all primes in $\mathbb{F}_q[T]$. This is a analogues result of the Riemann zeta function, which can be written as a product over all prime numbers. The fact that we can write the zeta function as a product over all primes helps us to solve some elementary counting problems. We illustrate this by computing the number of monic irreducible polynomials in $\mathbb{F}_q[T]$. Furthermore we will compute the number of square-free polynomials in $\mathbb{F}_q[T]$ using the zeta function.

In Chapter 4 we will discuss the theory of heights. Before defining the height function for global function fields, we will be familiarizing ourselves with the theory heights over number fields. We will show that a number field satisfies the product formula. Then we will develop the theory of heights over the field $\mathbb{F}_q(T)$. And we will be defining a height function on the projective space over $\mathbb{F}_q(T)$. Just like $\mathbb{Q}$, the field $\mathbb{F}_q(T)$ satisfy the product formula.

Then in Chapter 5 we state some powerful results which we need to state our main results. After defining the Dirichlet series associated to a function, we discuss the function field version of the Wiener-Ikehara Tauberian theorem, which gives the asymptotic behavior of the Dirichlet series, if some conditions about absolute convergence is met. Then we will state the Tauberian theorem for multi-variable Dirichlet series. This theorem gives us the asymptotic behavior of multi-variable Dirichlet series.

In Chapter 6 we will use the Tauberian theorems from Chapter 5, to determine the sizes of certain sets. In particular we will start by finding the size of the set of points in $\mathbb{P}^n(\mathbb{F}_q(T))$, which have bounded height. This means that we want to give an upper bound for

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^N\right\}.$$

Using the function field version of the Wiener-Ikehara Tauberian theorem we show the following result.

Theorem 1.1. *There exists a constant $\delta < 1$ such that*

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N\right\} = S_{\mathbb{F}_q(T)}(n+1,1)q^{N(n+1)} + \mathcal{O}\left(q^{N(\delta+n)}\right),$$

where $S_{\mathbb{F}_q(T)}(n+1,1) = \frac{(q^{n+1}-1)(1-q^{-n})}{q-1}$.

Then we will look at what happens when we require the points in $\mathbb{P}^n(\mathbb{F}_q(T))$ to satisfy certain arithmetic properties. After defining what it means for a point $x \in \mathbb{P}^n(\mathbb{F}_q(T))$ to be a l-th power, we will compute the size of the set

$$\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x \text{ is a } l\text{-th power}\right\}.$$

Then using the same application of the function field version of the Wiener-Ikehara Tauberian theorem we show the following result.

Theorem 1.2. *There exists a $\delta < 1$ such that,*

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^M, x \text{ is a } l\text{-th power}\right\} = S_{\mathbb{F}_q(T)}(n+1,1)q^{N(n+1)/l} + \mathcal{O}(q^{N(\delta+n/l)}).$$

In chapter 7 we will look at the size of the set

$$\#\left\{x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x_0 \text{ is a square}\right\}.$$

After defining

$$F(s_0, \ldots, s_n) = \sum_{\substack{x_0,\ldots x_n \in \mathbb{F}_q[T] \\ \gcd(x_0,\ldots,x_n)=1 \\ x_0 \text{ square}}} \frac{1}{|x_0|^{s_0} \ldots |x_n|^{s_n}},$$

our goal is to apply the Tauberian theorem for multi-variable Dirichlet series to this map. We will analyze this map and see that it satisfies two of the three properties of the Tauberian theorem. Furthermore we will see that the map F almost satisfies the final property of this theorem. Then we state a conjecture to heuristically determine the size of the set in which we are interested.

Conjecture 1.3. *There exists a constant $V \in \mathbb{R}$ such that,*

$$\#\left\{x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x_0 \text{ is a square}\right\} = \frac{V}{q-1}q^{N(1/2+n)} + \mathcal{O}(q^{(N-1)(1/2+n)})$$

In the heuristic for this conjecture we heavily relied on the usage of the Tauberian theorem for multi-variable Dirichlet series.

2 Polynomials over finite fields

In this chapter we will discuss the theory of polynomials over a finite field. We will follow chapter 1 of a book by Rosen [11].

2.1 The primes of $\mathbb{F}_q[T]$

Let $\mathbb{F}_q$ be the finite field with q elements. where q is the power of a prime. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. It happens that the ring A has many properties in common with $\mathbb{Z}$, the ring of the integers. In this chapter we will explore some of these properties. The elements of A can be written in the form $f(T) = a_0T^n + a_1T^{n-1} + \dots a_n$. If $a_0 \neq 0$ we say that f has degree n, which we denote by $\deg(f)$. If f is the zero polynomial we say that $\deg(f) = -\infty$. Then the degree of such polynomials holds some important properties, namely for $f, g \in A$ we have

$$\deg(fg) = \deg(f) + \deg(g) \quad \text{and} \quad \deg(f + g) \leq \max(\deg(f), \deg(g)).$$

The second property is an equality if $\deg(f) \neq \deg(g)$. Furthermore we call a polynomial $f \in A$ monic if $a_0 = 1$.

Proposition 2.1. *Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg+r$ and r is either 0 or $\deg(r) < \deg(g)$. Moreover, q and r are uniquely determined by these conditions.*

Proof. Take $f, g \in A$ and let $n = \deg(f)$ and $m = \deg(g)$. We write $f(T) = a_0T^n + \dots + a_n$ and $g(T) = b_0T^m + \dots + b_m$. We give a proof by induction on n, the degree of f. If $n < m$ we take $q = 0$ and $r = f$. Now we assume that $n \geq m$, we define $f_1 = f - a_0b_0^{-1}T^{n-m}g$, which has a smaller degree than f. By induction we know that there exist $q_1, r_1 \in A$ such that $f_1 = q_1g + r_1$, where r_1 is either 0 or with degree less than $\deg(g)$. In this case we set $q = a_0b_0^{-1}T^{n-m} + q_1$ and $r = r_1$. Then we have that $qg + r = (a_0b_0^{-1}T^{n-m} + q_1)g + r_1 = f - f_1 + q_1g + r_1 = f$. So we have now shown the existence of such q and r. Now suppose that $f = qg + r = q'g + r'$, then g divides $r - r'$, and by the degree considerations we wee that $r = r'$. Therefore we have that $qg = q'g$ which implies that $q = q'$, and we have proven the uniqueness. □

This proposition shows that the ring A is a Euclidean domain. In particular this means that A is a principal ideal domain and a unique factorization domain. One other result from this proposition is the finiteness of the residue class ring.

Proposition 2.2. *Suppose $g \in A$ and $g \neq 0$. Then A/gA is a finite ring with $q^{\deg(g)}$ elements.*

Proof. Let $m = \deg(g)$. By Proposition 2.1 we can see that $\{r \in A \mid \deg(r) < m\}$ is a complete set of representatives for A/gA. These elements are of the form $r = a_0T^{m-1} + a_1T^{m-2} + \dots + a_{m-1}$, with $a_i \in \mathbb{F}_q$. Since the a_i vary independently through $\mathbb{F}_q$, we can conclude that there are q^m such polynomials. □

Definition 2.3. *Let $g \in A$. If $g \neq 0$, set $|g| = q^{\deg(g)}$. If $g = 0$, set $|g| = 0$.*

This definition gives a notion of the size of a polynomial in A. We see that for $f, g \in A$ we have $|fg| = |f||g|$ and $|f + g| \leq \max(|f|, |g|)$ with equality if $|f| \neq |g|$. If we now want the determine what the unit group of A is, we take $g \in A$ such that g is an unit. Then there exist $f \in A$ such that $fg = 1$. So in particular we have that $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. Therefore we have that $\deg(g) = \deg(f) = 0$. So the unit group of A is given by $\mathbb{F}_q^*$.

By definition, a non-constant polynomial in A is irreducible if it cannot be written as the product of two polynomials, each of positive degree. Since every ideal in A is principal, we see that a polynomial is irreducible if that polynomial generates a prime ideal, which means that the polynomial is prime. In the ring A every non-zero polynomial, can be written uniquely as a the product of a non-zero constant and a monic polynomial. Therefore, every non-zero ideal in A has a unique monic generator. Finally we can sharpen the unique factorization property of A to the following statement. Every $f \in A$ non-zero, can be written uniquely in the form

$$f = aP_1^{e_1} \dots P_t^{e_t},$$

where $a \in \mathbb{F}_q^*$, each P_i is a monic irreducible polynomial, $P_i \neq P_j$ for $i \neq j$, and each e_i is a non-negative integer.

One property that the ring A has in common with the ring of integers $\mathbb{Z}$, is the Chinese Remainder Theorem.

Proposition 2.4. *Let $m_1, \ldots, m_t$ be elements of A which are pairwise relative prime. Let $m = m_1 m_2 \ldots m_t$ and φ_i be the natural homomorphism from A/mA to A/m_iA. Then the map $\varphi : A/mA \to A/m_1A \oplus \cdots \oplus A/m_tA$ given by*

$$\varphi(a) = (\varphi_1(a), \ldots, \varphi_t(a))$$

is a ring isomorphism.

This is a standard result that holds for any principal ideal domain. A proof can be found in [4, Thm. 17, p. 265-266].

Corollary 2.5. *The map φ restricted to the units of A, give rise to a group isomorphism*

$$(A/mA)^* \simeq (A/m_1A)^* \times \cdots \times (A/m_tA)^*.$$

Now let $f \in A$ be non-zero and not equal to a unit. Let $f = aP_1^{e_1} \ldots P_t^{e_t}$ be its prime decomposition, where $a \in \mathbb{F}_q^*$ and each P_i is a monic irreducible polynomial, $P_i \neq P_j$, for $i \neq j$, and each e_i is a non-negative integer. Then with the above corollary we have that

$$(A/fA)^* \cong (A/P_1^{e_1}A)^* \times \ldots \times (A/P_t^{e_t}A)^*.$$

To understand the structure of $(A/fA)^*$, for a polynomial $f \in A$, we need look at the structure of $(A/P^eA)^*$, where P is a monic irreducible polynomial and $e \in \mathbb{Z}_{>0}$. For a prime $p \in \mathbb{Z}$, we know that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group with $p-1$ elements. The structure of $(A/PA)^*$, which is the case when $e = 1$ is a result which is very similar to the situation of $\mathbb{Z}$.

Proposition 2.6. *Let $P \in A$ be an irreducible polynomial. Then $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.*

Proof. Since A is a principal ideal domain, we have that PA is a maximal ideal. So in particular we have that A/PA is a field. A finite subgroup of the multiplicative group of a field is cyclic [4, Prop. 18, p. 314]. Thus $(A/PA)^*$ is cyclic and the order is $|P| - 1$. □

Now we consider the case when $e > 1$. In the integer case we get that $p \in \mathbb{Z}$ is an odd prime number, then $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a group of order $p^{e-1}(p-1)$. For the ring A, we get a similar result.

Proposition 2.7. *Let $P \in A$ be an irreducible polynomial and e a positive integer. The order of $(A/P^eA)^*$ is $|P|^{e-1}(|P|-1)$. Let $(A/P^eA)^{(1)}$ be the kernel of the natural map from $(A/P^eA)^*$ to $(A/PA)^*$. It is a group of order $|P|^{e-1}$.*

Proof. The ring A/P^eA has only one maximal ideal, namely PA/P^eA, which has $|P|^{e-1}$ elements. Therefore $(A/P^eA)^* = (A/P^eA) \backslash (PA/P^eA)$ has $|P|^e - |P|^{e-1} = |P|^{e-1}(|P|-1)$ number of elements. Since the map $(A/P^eA)^* \to (A/PA)^*$ is surjective, and the group $(A/PA)^*$ has $|P| - 1$ elements, the assertion of the size of $(A/P^eA)^{(1)}$ follows. □

2.2 Analogous results to the little theorems of Euler and Fermat

Now we will discus the analogues of the Euler φ-function and the little theorems of Euler and Fermat for the ring A. Let $f \in A$ be a non-zero polynomial. We define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$. We can state a characterization of this number which makes the relation to the Euler ϕ-function more apparent. We have seen that the set $\{r \in A \,|\, \deg(r) < \deg(f)\}$, is a set of representatives for the quotient A/fA. Such an r represents a unit in A/fA if and only if it is relatively prime to f. Thus $\Phi(f)$ is the number of non-zero polynomials which have degree less than $\deg(f)$ and are relatively prime to f.

Proposition 2.8.

$$\Phi(f) = |f| \prod_{P|f} \left(1 - \frac{1}{|P|}\right).$$

Proof. Let $f = aP_1^{e_1} \dots P_t^{e_t}$ be the prime decomposition of f. Then by Corollary 2.5 and Proposition 2.7, we get

$$\Phi(f) = \prod_{i=1}^{t} \Phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i - 1}),$$

from which the result follows. □

We can compare this result to the result of the Euler φ-function. For an integer $n \in \mathbb{Z}$ we can write $n = p_1^{a_1} \dots p_s^{a_s}$, we get by [4, Example 10, p. 7] that

$$\varphi(n) = \prod_{i=1}^{s} p_i^{a_i - 1}(p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

which is similar to the result in A. Now we state some results which are analogues of the little theorems of Euler and Fermat.

Proposition 2.9. *If $f \in A, f \neq 0$ and $a \in A$ is relatively prime to f, then $a^{\Phi(f)} \equiv 1 \pmod f$.*

Proof. By definition we have that the group $(A/fA)^*$ has $\Phi(f)$ elements. The coset of a modulo f, denoted by $\overline{a}$, lies in this group. Therefore we have that $\overline{a}^{\Phi(f)} = \overline{1}$. From this we can conclude that $a^{\Phi(f)} \equiv 1 \pmod f$. □

Corollary 2.10. *Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then, $a^{|P|-1} \equiv 1 \pmod P$.*

Proof. Since P is prime and does not divide a, we have that $\gcd(P, a) = 1$. Furthermore we have seen that $(A/PA)^*$ is a cyclic group of order $|P| - 1$, if P is an irreducible polynomial. Thus when we apply the previous proposition the result follows. □

3 Arithmetic functions and the zeta function

In this section we will discuss properties of the primes in the ring $A = \mathbb{F}_q[T]$. We will use the zeta function associated to the ring A to discuss these properties. We will follow chapter 2 of the book by Rosen [11].

3.1 The zeta function for $\mathbb{F}_q[T]$

We will first state the definition of the zeta function associated to the ring A. This zeta function is an analogue of the classical zeta function introduced by L. Euler. The study of the classical zeta function was heavily improved by the contribution of B. Riemann. This zeta function is also known as the Riemann zeta function. In the case of the ring A, its associated zeta function is a much simpler object.

Definition 3.1. *The zeta function of A, denoted by ζ_A, is defined by the infinite series*

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s},$$

where $s \in \mathbb{C}$.

We know that there are exactly q^d monic polynomials of degree d in A, so we have that

$$\sum_{\deg(f) \leq d} |f|^{-s} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} \cdots + \frac{q^d}{q^{ds}} = \sum_{i=0}^{d} (q^{s-1})^i.$$

This is a geometric series which we can easily compute. This gives us that

$$\zeta_A(s) = \frac{1}{1 - q^{1-s}}$$

for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Now we see that ζ_A, which is initially defined for $\mathrm{Re}(s) > 1$, is meromorphic on the whole complex plane with a simple pole at $s = 1$. We can see that the function ζ_A is periodic with period $\frac{2\pi i}{\log(q)}$, this gives us that ζ_A has a simple pole at $s = 1 + \frac{2\pi i m}{\log(q)}$, where $m \in \mathbb{Z}$. We can compute the residue of the simple pole at $s = 1$ using L'Hôpital's rule [2] as follows

$$\lim_{s \to 1} \frac{s-1}{1 - q^{1-s}} = \lim_{s \to 1} \frac{1}{\log(q) q^{1-s}} = \frac{1}{\log(q)}.$$

For the classical Riemann zeta function Euler noted that the unique decomposition of integers into products of primes leads to the following identity for the Riemann zeta function:

$$\zeta(s) = \prod_{\substack{p \text{ prime} \\ p > 0}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

which holds for $\mathrm{Re}(s) > 1$. A proof of this result can be found in [10, Lemma 1.2.]. With the exact same reasoning we get the following identity

$$\zeta_A(s) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(1 - \frac{1}{|P|^s}\right)^{-1}, \tag{1}$$

which is valid for $\mathrm{Re}(s) > 1$.

3.2 Solving counting problems using the zeta function

We can immediately use Equation (1) to show that there exists infinite many primes in A. Suppose we only have a finite amount of irreducible polynomials in A. The right-hand side of the equation would then be defined at $s = 1$ and even have a non-zero value there. The left-hand side of the equation has a pole at $s = 1$. So there cannot be only finitely many irreducible polynomials in A. Now we will illustrate how we can apply this decomposition of the zeta function to a counting problem. We define a_d to be the number of monic irreducible polynomials of degree d. Then, from equation (1) we find that

$$\zeta_A(s) = \prod_{d=1}^{\infty} \left(1 - q^{-ds}\right)^{-a_d}.$$

If we use that $\zeta_A(s) = 1/(1 - q^{1-s})$ and substitute $u = q^{-s}$ we obtain

$$\frac{1}{1-qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Taking the logarithmic derivative with respect to u of both sides, and then multiplying by u we get

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} \frac{da_d u^d}{1-u^d}.$$

Now we extend the left-hand side into a power series using the geometric series and compare the coefficients of u^n. This leads to the following formula

Proposition 3.2. $\sum_{d|n} da_d = q^n$.

If we now define the Möbius function $\mu : \mathbb{F}_q[T] \to \{-1, 0, 1\}$, by

$$\mu(k) = \begin{cases} (-1)^{\#\text{prime divisors of } k} & \text{if } k \text{ is square-free,} \\ 0 & \text{if } k \text{ is not square-free.} \end{cases}$$

We can apply the Möbius inversion formula [1, Theorem 2.9] to the proposition above to conclude that

$$a_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}. \tag{2}$$

Now we want to write a_n in a way which makes it easy to see how big it is. In equation (2), q^n is the highest power of q that occurs. The next highest power that may occur is $q^{n/2}$, which occurs if and only if $2 \mid n$. All the other terms are of the form $\pm q^m$, where $m \leq n/3$. The total number of terms is given by

$$\sum_{d|n} |\mu(d)|.$$

To compute this number of terms we note that $\mu(d) = 0$ if d is not square-free. Thus $\mu(d) = 1$ if $d = p_1 \dots p_s$, where the p_i are distinct primes dividing n. So to get the total number of terms we must count the divisors of n which are in this form. Therefore the total number of terms is given by 2^t, where t is the number of distinct prime divisors of n.

Let $p_1, \dots, p_t$ be the distinct primes that divides n. Then we have that $2^t \leq p_1 \dots p_t \leq n$. Thus we get the following estimate

$$\left| a_n - \frac{q^n}{n} \right| \leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}}.$$

Now we define the big $\mathcal{O}$ notation.

Definition 3.3. *Let f, g and h be functions defined on $\mathbb{R}$. Then we write*

$$f(x) = g(x) + \mathcal{O}(h(x)),$$

as $x \to \infty$, if there exists an constant $C > 0$ and a real $x_0 \in \mathbb{R}$ such that $|f(x) - g(x)| \leq Ch(x)$, for all $x \geq x_0$.

Furthermore we denote $f(x) \ll h(x)$ if $f(x) = \mathcal{O}(h(x))$.

Since in our context we are interested in the growth rate as the variable x goes to infinity, we simple write $f(x) = g(x) + \mathcal{O}(h(x))$. One may note that $f(x) \ll h(x)$ precisely means that $f(x) = \mathcal{O}(h(x))$, as $x \to \infty$. Using this notation we have proved the following theorem.

Theorem 3.4. *Let a_n denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,*

$$a_n = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Now we will show how to use the zeta function for other counting problems. One such problem is counting the number of square-free monic polynomials of degree n. Then we can use the zeta function to get the following result.

Proposition 3.5. *Let b_n be the number of square-free monic polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then $b_1 = q$ and for $n > 1$ we have $b_n = q^n(1 - q^{-1})$.*

Proof. Consider the product

$$\prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(1 + \frac{1}{|P|^s}\right).$$

If we expand this product we get the terms 1 and $\frac{1}{|p_1|^s \ldots |p_k|^s}$, where $\{p_1, \ldots, p_k\}$ ranges over all possible subsets of the set of all primes in A. If we denote $\mathcal{P}$ for the set of all primes in A, then we get that the product equals

$$\sum_{B \subseteq \mathcal{P}} \frac{1}{\prod_{P \in B} |P|^s}.$$

Since A is a unique factorization domain we have that the product equals

$$\sum_{g \text{ monic square-free}} \frac{1}{|g|^s},$$

since every monic square-free polynomial in A corresponds to a subset $B \subseteq \mathcal{P}$. If we define the function $\delta : A \to \{0, 1\}$ by

$$\delta(f) = \begin{cases} 1, & \text{if } f \text{ is square-free,} \\ 0, & \text{otherwise,} \end{cases}$$

then we get the following equality

$$\prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(1 + \frac{1}{|P|^s}\right) = \sum_{f \text{ monic}} \frac{\delta(f)}{|f|^s}.$$

If we make the substitution $u = q^{-s}$, then we obtain

$$\sum_{f \text{ monic}} \frac{\delta(f)}{|f|^s} = \sum_{n=0}^{\infty} b_n u^n.$$

Now we notice that

$$(1 + 1/|P|^s) = (1 - |P|^{-2s})/(1 - |P|^{-s}).$$

Thus we get that

$$\prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(1 + \frac{1}{|P|^s}\right) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(\frac{1 - \frac{1}{|P|^{2s}}}{1 - \frac{1}{|P|^s}}\right) = \frac{\zeta_A(s)}{\zeta_A(2s)} = \frac{1 - q^{1-2s}}{1 - q^{1-s}}.$$

If we put everything in terms of $u = q^{-s}$, we obtain

$$\frac{1 - qu^2}{1 - qu} = \sum_{n=0}^{\infty} b_n u^n.$$

Finally, if we extend the left-hand side in a geometric series and compare the coefficients of u^n, we obtain that $b_1 = q$ and $b_n = q^n(1 - q^{-1})$ for $n > 1$. $\square$

We compare this result, with what is known to be true in the integer case. If B_n denotes the number of square-free integers less or equal to n, then it is know that

$$\lim_{n \to \infty} B_n/n = 6/\pi^2.$$

This result can be found in [6, Page 202]. Therefore the probability that a positive integer is square free is $6/\pi^2$. The probability that a monic polynomial is square free in $\mathbb{F}_q[T]$ is $(1 - q^{-1})$. One may see that $6/\pi^2 = 1/\zeta(2)$, and it is interesting to note that $(1 - q^{-1}) = 1/\zeta_A(2)$.

3.3 Upper bound for the Riemann-zeta function

Now that we have seen how to solve certain counting problems with the use of zeta functions, we will state a result about an upper bound for the Riemann zeta function near the critical strip [12, Theorem II.3.9.], which will be useful later on.

Theorem 3.6. *Let $s = \sigma + \tau i \in \mathbb{C}$ and take $0 < \alpha < 1$. Then we have*

$$|\zeta(s)| \ll \frac{3|\tau|^{1-\alpha}}{2\alpha(1-\alpha)},$$

for $\sigma \geq \alpha$ and $|\tau| \geq 1$.

From this result we can obtain an upper bound for the term $|s||\zeta(s+1)|$.

Corollary 3.7. *Let $s \in \mathbb{C}$ and take $\epsilon > 0$ sufficiently small. Let $R \in \mathbb{R}$, be a constant such that $\operatorname{Re}(s) \leq R$. Then we have for $\operatorname{Re}(s) \geq -\epsilon$,*

$$|s||\zeta(s+1)| \ll (|\operatorname{Im}(s)| + 1)^{1-\min\{\operatorname{Re}(s),0\}+\epsilon}.$$

Proof. First we assume $|\operatorname{Im}(s)| \geq 1$, then from Theorem 3.7 we obtain, for $0 < \alpha < 1$, that

$$|s||\zeta(s+1)| \ll |s| \frac{3|\operatorname{Im}(s+1)|^{1-\alpha}}{2\alpha(1-\alpha)}$$

if $\operatorname{Re}(s+1) \geq \alpha$. Now we notice that

$$|s| = \sqrt{\operatorname{Re}(s)^2 + \operatorname{Im}(s)^2} \leq \sqrt{2\max\{\operatorname{Re}(s)^2, \operatorname{Im}(s)^2\}} = \sqrt{2}\max\{|\operatorname{Re}(s)|, |\operatorname{Im}(s)|\}.$$

So we obtain that $|s| \ll \max\{\operatorname{Re}(s), \operatorname{Im}(s)\}$. Combing this and using the fact that $\operatorname{Im}(s+1) = \operatorname{Im}(s)$ we get

$$|s||\zeta(s+1)| \ll \max\left\{\frac{3\operatorname{Re}(s)|\operatorname{Im}(s)|^{1-\alpha}}{2\alpha(1-\alpha)}, \frac{3|\operatorname{Im}(s)|^{2-\alpha}}{2\alpha(1-\alpha)}\right\}.$$

Since the hypothesis of the corollary states that $\operatorname{Re}(s)$ is bounded from above by the real number R, we get $\operatorname{Re}(s) \leq R$, then we obtain

$$|s||\zeta(s+1)| \ll \max\left\{\frac{3R|\operatorname{Im}(s)|^{1-\alpha}}{2\alpha(1-\alpha)}, \frac{3|\operatorname{Im}(s)|^{2-\alpha}}{2\alpha(1-\alpha)}\right\} \ll_{R,\alpha} \max\left\{|\operatorname{Im}(s)|^{1-\alpha}, |\operatorname{Im}(s)|^{2-\alpha}\right\}.$$

Now we take $\alpha = 1 - \epsilon$, which gives

$$|s||\zeta(s+1)| \ll \max\left\{|\operatorname{Im}(s)|^{\epsilon}, |\operatorname{Im}(s)|^{\epsilon+1}\right\}.$$

Now we separate between two cases. First let $\mathrm{Re}(s) \geq 0$, then we get that

$$|s||\zeta(s+1)| \ll \max\left\{|\operatorname{Im}(s)|^{\epsilon}, |\operatorname{Im}(s)|^{\epsilon+1}\right\} \ll (1+|\operatorname{Im}(s)|)^{1+\epsilon}.$$

Lastly we assume that $\mathrm{Re}(s) < 0$. Then we obtain

$$|s||\zeta(s+1)| \ll \max\left\{|\operatorname{Im}(s)|^{\epsilon}, |\operatorname{Im}(s)|^{\epsilon+1}\right\} \ll (1+|\operatorname{Im}(s)|)^{1+\epsilon} \leq (1+|\operatorname{Im}(s)|)^{1-\mathrm{Re}(s)+\epsilon}.$$

Combing these cases we arrive at

$$|s||\zeta(s+1)| \ll (|\operatorname{Im}(s)|+1)^{1-\min\{\mathrm{Re}(s),0\}+\epsilon}.$$

On the domain $|\operatorname{Im}(s)| \leq 1$, $-\epsilon \leq \mathrm{Re}(s) \leq R$, the function $s\zeta(s+1)$ is holomorphic and hence bounded. Therefore the result extends to the case where $|\operatorname{Im}(s)| \leq 1$. which is our wanted result.

□

4 Height functions

A key tool for studying rational and integral points on an algebraic variety is a method of measuring the “size” of a point. To define such a size function we require two important properties. First, there should be a finite number of points of bounded size. Secondly, the size of a point should reflect the arithmetic and geometric nature of the variety. These size functions that we will discus in this chapter are called height functions. First we discuss the theory of heights on number fields as described in [5, Part B]. Then we will show the analogues results for the field $\mathbb{F}_q(T)$.

4.1 Height functions for number fields

Before we can define a height function on the rational points of an algebraic variety, we first need a way of measuring the size of an algebraic number. The most common way to describe the size of an algebraic number is through the use of absolute values.

Definition 4.1. *An absolute value on a field k is a real-valued function*

$$|\,.\,| : k \to [0, \infty)$$

with the following properties:

(i) $|x| = 0$ *if and only if* $x = 0$.

(ii) $|xy| = |x| \cdot |y|$ *for all* $x, y \in k$.

(iii) $|x + y| \leq |x| + |y|$ *for all* $x, y \in k$.

An absolute value is said to be non-archimedean if it satisfies $|x+y| \leq \max\{|x|, |y|\}$ *for all* $x, y \in k$.

We give an example for the simplest number field, the field of rational numbers $\mathbb{Q}$. There exist an archimedean absolute value on $\mathbb{Q}$ defined by

$$|x|_\infty = \max\{x, -x\}.$$

This is the restriction to $\mathbb{Q}$ of the usual absolute value on $\mathbb{R}$. Furthermore, for each prime number p there exists a non-archimedean absolute value on $\mathbb{R}$. For any non-zero rational number $x \in \mathbb{Q}$, let $\text{ord}_p(x) \in \mathbb{Z}$ be the unique integer such that we can write x in the form

$$x = p^{\text{ord}_p(x)} \cdot \frac{a}{b},$$

with $a, b \in \mathbb{Z}$ and $p \nmid ab$. If $x = 0$, we set $\text{ord}_p(x) = \infty$. Then we have the p-adic absolute value

$$|x|_p = p^{-\text{ord}_p(x)}$$

for $x \in \mathbb{Q}$.

Now we note $M_{\mathbb{Q}}$ as the set of standard absolute values on $\mathbb{Q}$ consisting of the the absolute value $|\,.\,|_\infty$, and the p-adic absolute value $|\,.\,|_p$ for every prime p. For a number field k we denoted by M_k the set of all standard absolute values, consisting of all absolute values on a number field k whose restriction to $\mathbb{Q}$ is one of the standard absolute values on $\mathbb{Q}$. To make notation more convenient we will note $|\,.\,|_v$ for the absolute value corresponding to $v \in M_k$. Then $\mathbb{Q}$ satisfy the product rule [5, Prop. B.1.2.].

Lemma 4.2. *Let $x \in \mathbb{Q}$ be a non-zero rational number. Then we have*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1.$$

Proof. Let $x \in \mathbb{Q}\backslash\{0\}$. Since $\mathbb{Z}$ is a unique factorization domain, we can write $x = \pm \prod_{q \text{ prime}} q^{e_q}$, as a product of primes, where $e_q \in \mathbb{Z}$. Then we obtain

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = |x|_\infty \prod_{p \text{ prime}} |x|_p.$$

For $|x|_p$ we see that $|x|_p = |\prod_q \pm q^{e_q}|_p = |\pm 1|_p \prod_q |q|_p^{e_q}$. Now we get $|\pm 1|_p = 1$ and $|q|_p = 1$ if $q \neq p$ and $|q|_p = 1/q$ if $p = q$. Combing this gives

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = |x|_\infty \prod_{\substack{p|x \\ p \text{ prime}}} \frac{1}{p^{e_p}} = \frac{|x|_\infty}{|x|_\infty} = 1.$$

Which finishes our proof. □

This product formula has a generalization to general number fields. Before we can state this generalized version we need some results for extensions of number fields.

Definition 4.3. *Let k'/k be an extension of number fields and let $v \in M_k, w \in M_{k'}$, be absolute values. We say that w divides v (or w lies over v) and write $w \mid v$ of the restriction of w to k is v. We say that v is p-adic if it lies over the p-adic absolute value of $\mathbb{Q}$.*

To state the generalized version of the product rule, we need to assign weights to the absolute values. For a number field k and an absolute value $v \in M_k$, we write k_v for the completion of the field k with respect to v. For example, let v be an absolute value in $\mathbb{Q}$, so $v \in M_{\mathbb{Q}}$. Then $\mathbb{Q}_v = \mathbb{R}$ if $v = \infty$. Now we need a well-know result for the local and global degrees of an extension.

Proposition 4.4. *Let k'/k be an extension of number fields, and let $v \in M_k$ be an absolute value on k. Then*

$$\sum_{w \in M_{k'}, w|v} [k'_w : k_v] = [k' : k].$$

A proof of this result can be found in [7, II. Corollary 1 to Theorem 2]. Then we can define the local degree of an absolute value as follows.

Definition 4.5. *Let $v \in M_k$ be an absolute value on number field k. The local degree of v is the number $n_v = [k_v : \mathbb{Q}_v]$, where $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ at the restriction of v to $\mathbb{Q}$. The normalized absolute value associated to v is $||x||_v = |x|_v^{n_v}$.*

Now we have all the required tools to state the product formula for number fields.

Proposition 4.6. *Let k be a number field and let $x \in k^*$. Then*

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

A proof of this generalized product formula can be found in [5, Prop B.1.2.].

We now have the right tool to discus the theory of heights on the projective space. There is a natural way to measure the size of a rational point $P \in \mathbb{P}^n(\mathbb{Q})$. We can write the point $P = [x_0 : \cdots : x_n]$, with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. We define the height of the point P as

$$H(P) = \max\{|x_0|, \ldots, |x_n|\}.$$

Then we see see that for any $B \in \mathbb{Z}$, the set $\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \leq B\}$ is finite, since there are only finitely many integers $x \in \mathbb{Z}$ with $|x| \leq B$. We can generalize this notion of height to number fields in the following way.

Definition 4.7. *Let k be a number field, and let $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k)$ be a point whose homogeneous coordinates are chosen in k. The height of P (relative to k) is given by*

$$H_k(P) = \prod_{v \in M_k} \max\{||x_0||_v, \ldots, ||x_n||_v\}.$$

The product formula ensures that the height $H_k(P)$ is well-defined. So $H_k(P)$ is independent on the choice of homogeneous coordinates for P. We state this result in the following Lemma.

Lemma 4.8. *Let k be a number field and let $P \in \mathbb{P}^n(k)$ be a point. Then $H_k(P)$ is independent on the choice of homogeneous coordinates of P.*

Proof. We write $P = [x_0 : \cdots : x_n]$. Then any other choice of coordinates for P is of the form $[cx_0 : \cdots : cx_n]$, for $c \in k^*$. Using the product formula (Proposition 4.6) we find

$$\prod_{v \in M_k} \max\{||cx_0||_v, \ldots, ||cx_n||_v\} = \left(\prod_{v \in M_k} ||c||_v\right)\left(\prod_{v \in M_k} \max\{||x_0||_v, \ldots, ||x_n||_v\}\right)$$
$$= \prod_{v \in M_k} \max\{||x_0||_v, \ldots, ||x_n||_v\}.$$

This shows that H_k is independent of the choice of homogeneous coordinates for P. □

Now we want to see if we can express the height function $H_{k'}$ in terms of H_k if k' is a finite extension of k. This leads to the following result.

Lemma 4.9. *Let k' be a finite extension of k. Then*

$$H_{k'}(P) = H_k(P)^{[k':k]}.$$

A proof can be found in [5, Lemma B.2.1. (c)]. This result allows us to define a new height function that is independent of the field k.

Definition 4.10. *The absolute (multiplicative) height on $\mathbb{P}^n$ is the function $H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [1, \infty)$ defined by*

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

Note that Lemma 4.9 ensures that the absolute height is well-defined independent of the choice of the field k. We will also define the height of an element $a \in k$ to be the height of the corresponding projective point $[a : 1] \in \mathbb{P}^1(k)$.

For a point $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. We denote $\mathbb{Q}(P)$ by $\mathbb{Q}(x_0/x_j, \ldots, x_n/x_j)$, for any j with $x_j \neq 0$. The following theorem states an important result for the application of height functions.

Theorem 4.11. *For any numbers $B, D \geq 0$, the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

is finite. In particular, for any fixed number field k, the set

$$\{P \in \mathbb{P}^n(k) \mid H_k(P) \leq B\}$$

is finite.

A proof of this theorem can be found in [5, Theorem B.2.3.].

4.2 Height functions over $\mathbb{F}_q(T)$

In this section we will describe the theory of heights for the field $\mathbb{F}_q(T)$. Before we can define the height function on $\mathbb{F}_q(T)$ we need to define some absolute values on the ring $\mathbb{F}_q[T]$. First we have already seen an absolute value on $\mathbb{F}_q[T]$ in Definition 2.3.. This leads to the following result.

Lemma 4.12. *Let $g \in \mathbb{F}_q[T]$. Then*

$$|g| = \begin{cases} q^{\deg(g)}, & \text{if } g \text{ is non-zero,} \\ 0, & \text{if } g = 0. \end{cases}$$

defines an absolute value on $\mathbb{F}_q[T]$.

Proof. By construction we have that $|g| = 0$ if and only if $g = 0$. Now take $f, g \in \mathbb{F}_q[T]$, then we get

$$|fg| = q^{\deg(fg)} = q^{\deg(f)+\deg(g)} = q^{\deg(f)}q^{\deg(g)} = |f||g|,$$

if f and g are both non-zero. If at least one of them were zero, it follows that $|fg| = |f||g|$ trivially. Furthermore we have that

$$|f + g| = q^{\deg(f+g)} \leq q^{\max\{\deg(f),\deg(g)\}} \leq q^{\deg(f)} + q^{\deg(g)} = |f| + |g|.$$

This gives us that $| \, . \, |$ defines an absolute value on $\mathbb{F}_q[T]$. □

We denote this absolute value by $| \, . \, |_\infty$.We can extend this absolute value to $\mathbb{F}_q(T)$ in the following way. For $\frac{a}{b} \in \mathbb{F}_q(T)$, with $b \neq 0$, we define $|\frac{a}{b}|_\infty = q^{\deg(a)-\deg(b)}$. Just like for $\mathbb{Q}$, we can define a non-archimedean absolute value in $\mathbb{F}_q(T)$ corresponding to a prime $P \in \mathbb{F}_q[T]$. We define $\text{ord}_P(x)$ to be the unique integer such that we can write x in the from

$$x = P^{\text{ord}_P(x)} \cdot \frac{a}{b},$$

with $a, b \in \mathbb{F}_q[T]$ and $P \nmid ab$. If $x = 0$, we set $\text{ord}_P(x) = \infty$. Then we can define

$$|x|_P = q^{-ord_P(x)\deg(P)},$$

for $x \in \mathbb{F}_q(T)$.

Now we denote $M_{\mathbb{F}_q(T)}$ as the set of standard absolute values on $\mathbb{F}_q(T)$, consisting of the absolute value $| \, . \, |_\infty$ and the absolute value $| \, . \, |_P$ for every prime P. For a finite extension $k \supset \mathbb{F}_q(T)$ we define M_k as the set of all absolute values on k whose restriction to $\mathbb{F}_q(T)$ is one of the standard absolute values on $\mathbb{F}_q(T)$. For notation we will note $| \, . \, |_v$ for the absolute value corresponding to $v \in M_{\mathbb{F}_q(T)}$. Then we will see that $\mathbb{F}_q(T)$ satisfies the product formula.

Lemma 4.13. *Let $x \in \mathbb{F}_q(T)$ be non-zero. Then we have,*

$$\prod_{v \in M_{\mathbb{F}_q(T)}} |x|_v = 1.$$

Proof. Since $\mathbb{F}_q[T]$ is a unique factorization domain, we can write $x = \alpha \prod_{S \text{ prime}} S^{e_S}$, where $\alpha \in \mathbb{F}_q^*$ and $e_S \in \mathbb{Z}$. Then we will rewrite the product over all standard absolute values as follows.

$$\prod_{v \in M_{\mathbb{F}_q(T)}} |x|_v = |x|_\infty \prod_{P \text{ prime}} |x|_P.$$

For $|x|_P$ we have that

$$|x|_P = |\alpha \prod_{S \text{ prime}} S^{e_S}|.$$

We have that $|\alpha|_P = 1$, for every prime P. Furthermore we have that $|S^{e_P}|_P = 1$ if $S \neq P$, and $|S^{e_P}|_P = \frac{1}{q^{e_S \deg(P)}}$, if $S = P$. Therefore we obtain

$$\prod_{v \in M_{\mathbb{F}_q(T)}} |x|_v = |x|_\infty \prod_{\substack{P|x \\ P \text{ prime}}} \frac{1}{q^{e_P \deg(P)}} = |x| \frac{1}{q^A},$$

where $A = \sum_{\substack{P|x \\ P \text{ prime}}} e_P \deg(P)$. But here we have that $A = \deg(x)$. So we have that

$$\prod_{v \in M_{\mathbb{F}_q(T)}} |x|_v = \frac{|x|_\infty}{q^{\deg(x)}} = \frac{q^{\deg(x)}}{q^{\deg(x)}} = 1.$$

This completes in showing that $\mathbb{F}_q(T)$ satisfies the product formula. □

Now we will discuss the theory of heights on the projective space $\mathbb{P}^n(\mathbb{F}_q(T))$. Here, there is a natural way to measure the size of a point $Q \in \mathbb{P}^n(\mathbb{F}_q(T))$. We can write the point Q in the form $Q = [x_0 : \cdots : x_n]$, where $x_0, \ldots, x_n \in \mathbb{F}_q[T]$ such that $\gcd(x_0, \ldots, x_n) = 1$. Then we define the height of the point Q as

$$H(Q) = \max\{|x_0|, \ldots, |x_n|\}.$$

Since we only have a finite amount of polynomials $x \in \mathbb{F}_q[T]$ such that $|x| \leq B$, for $B \in \mathbb{R}$, we have that

$$\{Q \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H(Q) \leq B\},$$

is finite. Now we define for an absolute value $v \in M_{\mathbb{F}_q(T)}$ and $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q(T)^n$, the following

$$|\boldsymbol{x}|_v = \max\{|x_1|_v, \ldots, |x_n|_v\}.$$

Then we have that $|\boldsymbol{x}|_v = 1$ for all but finitely many v, and we define the height of $\boldsymbol{x}$, by

$$H_{n-1}(\boldsymbol{x}) = \prod_{v \in M_{\mathbb{F}_q(T)}} |\boldsymbol{x}|_v.$$

Let $c \in \mathbb{F}_q(T)$, then we have by the product formula that

$$H_{n-1}(c\boldsymbol{x}) = \prod_{v \in \ M_{\mathbb{F}_q(T)}} |c\boldsymbol{x}| = \prod_{v \in M_{\mathbb{F}_q(T)}} |\boldsymbol{x}|_v = H_{n-1}(\boldsymbol{x}).$$

Thus we have that the function H_{n-1} is a function on $\mathbb{P}^{n-1}(\mathbb{F}_q(T))$.

With this definition of a height function, we have that the height of a point in $\mathbb{F}_q(T)$ is of the form q^M, for a $M \in \mathbb{Z}_{\geq 0}$. Let $\boldsymbol{x} \in \mathbb{P}^n(\mathbb{F}_q(T))$, then we have that

$$H_n(\boldsymbol{x}) = \prod_{v \in M_{\mathbb{F}_q(T)}} |\boldsymbol{x}|_v = \prod_{v \in M_{\mathbb{F}_q(T)}} \max\{|x_0|_v, \ldots, |x_n|_v\}.$$

We know that $\max\{|x_0|_v, \ldots, |x_n|_v\}$ is of the form q^{M_v}, where

$$M_v = \begin{cases} \deg(\max\{|x_0|_v, \ldots, |x_n|_v\}), & \text{if } v = \infty, \\ -\mathrm{ord}_P(\max\{|x_0|_v, \ldots, |x_n|_v\}) \deg(P), & \text{if } v = P, \text{for a prime } P. \end{cases}$$

We have that only a finite amount of M_v are non-zero. Therefore we get that $H_n(\boldsymbol{x}) = q^M$, where

$$M = \sum_{v \in \mathbb{F}_q(T)} M_v.$$

5 Tauberian theorems for function fields

In this chapter we will first discuss the function field version of the Wiener-Ikehara Tauberian theorem. Then we will discuss the Tauberian theorem for multi-variable Dirichlet series, which will be defined in this chapter.

5.1 Function field version of the Wiener-Ikehara Tauberian theorem

Before we can state the Tauberian theorem, we start by defining the Dirichlet series associated to a function.

Definition 5.1. *Let $f : \mathbb{F}_q[T] \to \mathbb{C}$ be a function. Then the Dirichlet series associated to f is defined by*

$$D_f(s) := \sum_{h \text{ monic}} \frac{f(h)}{|h|^s}.$$

Then for a function $f : \mathbb{F}_q[T] \to \mathbb{C}$ we define $F(n)$ as the sum of $f(h)$ over all monic polynomials h, of degree n. We can rewrite the associated Dirichlet series in terms of $F(n)$ as follows:

$$D_f(s) = \sum_{h \text{ monic}} \frac{f(h)}{|h|^s} = \sum_{n=0}^{\infty} \frac{F(n)}{q^{ns}}.$$

We notice that the function q^{-s} is periodic with period $\frac{2\pi i}{\log(q)}$. This implies that the associated Dirichlet series is periodic with the same period. This means that nothing is lost by confining our attention to the region

$$B := \left\{ s \in \mathbb{C} \mid -\frac{\pi}{\log(q)} \le \operatorname{Im}(s) < \frac{\pi}{\log(q)} \right\}.$$

Now we state the function field version of the Wiener-Ikehara Tauberian theorem [11, Theorem 17.1.].

Theorem 5.2. *Let $f : \mathbb{F}_q[T] \to \mathbb{C}$ be a function with its associated Dirichlet series $D_f(s)$. Suppose that $D_f(s)$ converges absolutely for $\operatorname{Re}(s) > 1$ and is holomorphic on $\{s \in B \mid \operatorname{Re}(s) = 1\}$ except for a simple pole at $s = 1$ with residue α. Then, there is a real number $\delta < 1$ such that*

$$F(N) = \alpha \log(q) q^N + \mathcal{O}(q^{\delta N}).$$

Proof. We define $Z_f(u)$ as the function for which $Z_f(q^{-s}) = D_f(s)$. Then we have

$$Z_f(u) = \sum_{N=0}^{\infty} F(N) u^N.$$

Since we assumed $D_f(s)$ to be holomorphic on $\{s \in B \mid \operatorname{Re}(s) = 1\}$ except for a simple pole at $s = 1$, we get that $Z_f(u)$ is holomorphic on the disk $\{u \in \mathbb{C} \mid |u| \le q^{-1}\}$ with the exception of a simple pole at $u = q^{-1}$, where $|u| = \sqrt{Re(u)^2 + \operatorname{Im}(u)^2}$ denotes the usual absolute value on $\mathbb{C}$. The residue of $Z_f(u)$ at $u = q^{-1}$ is given by

$$\begin{aligned}
\lim_{u \to q^{-1}} (u - q^{-1}) Z_f(u) &= \lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} (s-1) D_f(s) \\
&= \left(\lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} \right) \left(\lim_{s \to 1} (s-1) D_f(s) \right) \\
&= \left(\lim_{s \to 1} \frac{-q^{-s} \log(q)}{1} \right) \alpha \\
&= -\frac{\log(q)}{q} \alpha.
\end{aligned}$$

Now we notice that since the circle $\{u \in \mathbb{C} \,|\, |u| = q^{-1}\}$ is compact, we can take a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disk $\{u \in \mathbb{C} \,|\, |u| \leq q^{-\delta}\}$ except for the simple pole at $u = q^{-1}$. Let C be the boundary of this disk oriented counterclockwise and let C_ϵ be a small disk about the origin of radius $\epsilon < q^{-1}$. We orient C_ϵ clockwise, which is illustrated in Figure 1, and consider the integral

$$\frac{1}{2\pi i} \oint_{C_\epsilon + C} \frac{Z_f(u)}{u^{N+1}} du.$$

Then by the Cauchy integral formula [8, Theorem VI.1.2.], this equals the sum of the residues of $Z_f(u)u^{-N-1}$ between the two circles. There is only one pole at $u = q^{-1}$, and the residue is given by

$$-\frac{\log(q)}{q} \alpha \left(q^{-1}\right)^{-N-1} = -\frac{\log(q)}{q} \alpha q^{N+1} = -\alpha \log(q) q^N.$$

We define the function

$$h(u) = \frac{Z_f(u)}{u^{N+1}}.$$

Since $Z_f(u)$ is holomorphic on the circle $\{s \in \mathbb{C} \; |s| \leq \epsilon\}$, and u^{-N-1}, has a pole at $u = 0$, the function h has a pole at $u = 0$. Then using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$h(u) = \frac{Z_f(u)}{u^{N+1}} = \sum_{K=0}^{\infty} F(K) u^{K-N-1},$$

gives the Laurent expansion at $u = 0$. Therefore we get that the residue of the pole at $u = 0$ equals the coefficient of u^{-1} which equals $F(N)$. Using the Cauchy integral formula, and using that C_ϵ is oriented clockwise, we get that

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du = -F(N).$$

Since we have that

$$\frac{1}{2\pi i} \oint_{C_\epsilon + C} \frac{Z_f(u)}{u^{N+1}} du = \frac{1}{2\pi i} \oint_{C} \frac{Z_f(u)}{u^{N+1}} du + \frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du,$$

we obtain with our results that

$$F(N) = \alpha \log(q) q^N + \frac{1}{2\pi i} \oint_{C} \frac{Z_f(u)}{u^{N+1}} du.$$

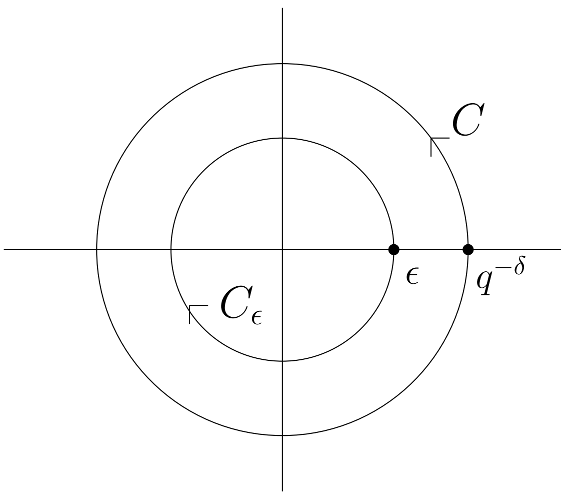

Figure 1: The circles C and C_ϵ

We now look at the asymptotic behavior of

$$\frac{1}{2\pi i}\oint_C \frac{Z_f(u)}{u^{N+1}}du.$$

Let M be the maximum value of $|Z_f(u)|$ on the circle C. Then the integral

$$\frac{1}{2\pi i}\oint_C \frac{Z_f(u)}{u^{N+1}}du$$

is bounded by

$$\begin{aligned}\left|\frac{1}{2\pi i}\oint_C \frac{Z_f(u)}{u^{N+1}}du\right| &\leq \frac{1}{2\pi}\oint_C \left|\frac{Z_f(u)}{u^{N+1}}\right| du \\ &\leq \frac{1}{2\pi}\oint_C \frac{M}{|u^{N+1}|}du \\ &\leq \oint_C Mq^{\delta N}du \\ &= Mq^{\delta N}\oint_C du \\ &= 2\pi q^{-\delta}Mq^{\delta N} \\ &\leq Mq^{\delta N}.\end{aligned}$$

This gives us that

$$F(N) = \alpha \log(q)q^N + \mathcal{O}(q^{\delta N}),$$

which completes our proof. □

5.2 Tauberian theorem for multi-variable Dirichlet series

To state the Tauberian theorem for multi-variable Dirichlet series, we first need the notion of an arithmetic function and its associated multi-variable Dirichlet series.

Definition 5.3. *An arithmetic function is a function $f : \mathbb{N}^m \to \mathbb{C}$. Its associated multi-variable Dirichlet series is defined by*

$$F(s_1, \dots, s_m) = \sum_{d_1=1}^{\infty} \cdots \sum_{d_m=1}^{\infty} \frac{f(d_1, \dots, d_m)}{d_1^{s_1} \dots d_m^{s_m}}.$$

Before we state the Tauberian theorem for multi-variable Dirichlet series, we will give some notation. Let $\boldsymbol{s}$ be the m-tuple given by $\boldsymbol{s} = (s_1, \dots, s_m)$. Let $\mathcal{L}_m(\mathbb{C})$ be the space of linear forms from $\mathbb{C}^m$ to $\mathbb{C}$. Let $\{e_j\}_{j=1}^m$ be a canonical basis of $\mathbb{C}_m$ and $\{e_j^*\}_{j=1}^m$ be the dual basis of $\mathcal{L}_m(\mathbb{C})$. We denote $\mathcal{LR}_m(\mathbb{C})$ (respectively $\mathcal{LR}_m^+(\mathbb{C})$) as the set of linear forms of $\mathcal{L}_m(\mathbb{C})$ restricted to $\mathbb{R}^m$ (resp. $(\mathbb{R}_{>0})^m$). Let $\beta_j > 0$ for $j = 1, \dots m$, then we denote $\mathcal{B}$ for the linear form in $\mathcal{LR}_m^+(\mathbb{C})$ of the form $\mathcal{B} = \sum_{j=1}^m \beta_j e_j^*$, and let $\boldsymbol{\beta} = (\beta_1, \dots, \beta_m)$ be its associated matrix. Then for $\boldsymbol{a} = (a_1, \dots, a_m) \in \mathbb{R}^m$ we define the $||\,.||_1$ norm as $||\boldsymbol{a}|| = \sum_{j=1}^m |a_m|$. Now we will state the Tauberian theorem for multi-variable Dirichlet series [3, Theorem 1].

Theorem 5.4. *Let $f : \mathbb{N}^m \to \mathbb{R}_{\geq 0}$ be an arithmetic function and F its associated multi-variable Dirichlet series*

$$F(s_1, \dots, s_m) = \sum_{d_1=1}^{\infty} \cdots \sum_{d_m=1}^{\infty} \frac{f(d_1, \dots, d_m)}{d_1^{s_1} \dots d_m^{s_m}}.$$

Suppose that there exists $\boldsymbol{a} \in (\mathbb{R}_{>0})^m$ such that F satisfies the following properties.

(P1) The series $F(\boldsymbol{s})$ is absolutely convergent for all $\boldsymbol{s} = (s_1, \dots, s_m)$ such that $\mathrm{Re}(s_i) > a_i$ for all $i = 1, \dots, m$.

(P2) There exist a family $\mathscr{L} = \{\ell^{(i)}\}_{i=1}^{n}$ *of non-zero linear forms in* $\mathcal{LR}_m^+(\mathbb{C})$*, and a finite family* $\{h^{(i)}\}_{r\in\mathcal{R}}$ *of linear forms in* $\mathcal{LR}_m^+(\mathbb{C})$ *such that the function* $H : \mathbb{C}^m \to \mathbb{C}$ *defined by*

$$H(\boldsymbol{s}) := F(\boldsymbol{s}+\boldsymbol{a}) \prod_{i=1}^{n} \ell^{(i)}(\boldsymbol{s})$$

can be extended to a holomorphic function on the domain

$$\mathcal{D}(\delta_1, \delta_3) := \left\{ \boldsymbol{s} \in \mathbb{C}^m \mid \operatorname{Re}(\ell^{(i)}(\boldsymbol{s})) > -\delta_1 \text{ for all } i = 1, \dots, n, \operatorname{Re}(h^{(r)}(\boldsymbol{s})) > -\delta_3 \text{ for all } r \in \mathcal{R} \right\}.$$

Where $\delta_1, \delta_3 \in \mathbb{R}_{>0}$.

(P3) There exists $\delta_2 > 0$ *such that for* $\epsilon > 0$ *and* $\epsilon' > 0$ *we have that*

$$|H(\boldsymbol{s})| \ll \prod_{i=1}^{n} (|\operatorname{Im}(\ell^{(i)}(\boldsymbol{s}))| + 1)^{1-\delta_2 \min\{0, \operatorname{Re}(\ell^{(i)}(\boldsymbol{s}))\}} (1 + ||\operatorname{Im}(\boldsymbol{s})||_1)^{\epsilon}$$

uniformly on the domain $\mathcal{D}(\delta_1 - \epsilon', \delta_3 - \epsilon')$.

Then there exists a polynomial $Q_{\boldsymbol{\beta}} \in \mathbb{R}[X]$ *of degree at most* $n - \operatorname{rank}(\{\ell^{(i)}\}_{i=1}^{n})$ *and a real* $\theta = \theta(\mathscr{L}, \{h^{(r)}\}_{r\in\mathcal{R}}, \delta_1, \delta_2, \delta_3, \boldsymbol{a}, \boldsymbol{\beta}) > 0$*, such that for* $X \geq 1$ *we have*

$$\begin{aligned} S(X, (\beta_1, \dots, \beta_m)) &= \sum_{1 \leq d_1 \leq X^{\beta_1}} \cdots \sum_{1 \leq d_m \leq X^{\beta_m}} f(d_1, \dots, d_m) \\ &= X^{\langle \boldsymbol{a}, \boldsymbol{\beta} \rangle} (Q_{\beta}(\log X) + \mathcal{O}(X^{-\theta})), \end{aligned}$$

where $\langle \boldsymbol{a}, \boldsymbol{\beta} \rangle = a_1\beta_1 + a_2\beta_2 + \cdots + a_m\beta_m$ *defines the standard inner product.*

6 Counting points of bounded height

In this chapter we will discus the main results of this thesis. We look at some counting problems which we solve by using the theory of zeta functions and the Tauberian theorems we described before. In particular, we will discuss the size of the set $\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M\right\}$, where H_n is the height function on $\mathbb{P}^n(\mathbb{F}_q(T))$ and $M \in \mathbb{Z}_{\geq 0}$ is an non-negative integer. Then we will discuss the size of this set with some extra constrains on the points in the projective space. Throughout this chapter, to make the notation more clear, we will write $|x|_\infty$ as $|x|$, for $x \in \mathbb{F}_q(T)$.

6.1 Counting points of bounded height over $\mathbb{F}_q(T)$

We will now show how the size of $\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M\right\}$ behaves asymptotically as M goes to infinity. Before we state the result we recall the Möbius function $\mu : \mathbb{F}_q[T] \to \{-1, 0, 1\}$, which is defined by

$$\mu(k) = \begin{cases} (-1)^{\#\text{prime divisors of } k} & \text{if } k \text{ is square-free,} \\ 0 & \text{if } k \text{ is not square-free.} \end{cases}$$

Then the Möbius function satisfies the following property [9, Lemma 2.2.2.],

Lemma 6.1. *Let $g \in \mathbb{F}_q[T]$. We have that*

$$\sum_{\substack{k \in \mathbb{F}_q[T] \\ monic \\ k|g}} \mu(k) = \begin{cases} 1 & \textit{if } g = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $g = 1$, then the only monic divisor of g equals 1. This implies that

$$\sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k|g}} \mu(k) = \sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k|1}} \mu(k) = \mu(1) = 1.$$

Now assume that $g \neq 1$, since $\mathbb{F}_q[T]$ is an unique factorization domain, we can write

$$g = aP_1^{e_1} \dots P_s^{e_s},$$

where $a \in \mathbb{F}_q$, non-zero, $P_i \in \mathbb{F}_q[T]$ are monic irreducible polynomials and $e_i \in \mathbb{Z}_{\geq 1}$, for all $1 \leq i \leq s$. We see that all possible monic divisors of g are given by the set

$$\{P_1^{l_1} \dots P_s^{l_s} \in \mathbb{F}_q[T] \,|\, 0 \leq l_i \leq e_i, \text{ for all } 1 \leq i \leq s\}.$$

Since we apply the Möbius function to these monic divisors, we only have to account for the divisors which are square-free, since the Möbius function maps a non square-free divisor to zero. Therefore we get

$$\sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k|g}} \mu(k) = \mu(1) + \sum_{i=1}^{s} \mu(P_i) + \sum_{\substack{1 \leq i,j \leq s \\ i \neq j}} \mu(P_i P_j) + \dots + \mu(P_1 \dots P_s)$$

We can compute this using the definition of the Möbius function as

$$\sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k|g}} \mu(k) = 1 + \binom{s}{1}(-1) + \binom{s}{2}(1) + \dots + \binom{s}{s}(-1)^s$$

$$= \binom{s}{0} 1^s (-1)^0 + \binom{s}{1}(1^{s-1})(-1)^1 + \dots + \binom{s}{s}(1^0)(-1)^s.$$

Then by the binomial theorem this equals

$$\sum_{\substack{k\in\mathbb{F}_q[T]\\ \text{monic}\\ k|g}} \mu(k) = (1+(-1))^s = 0^s = 0.$$

This concludes the proof. $\square$

This sum gives us an indicator function for when $g = 1$. The Möbius function also satisfies the following property [9, Lemma 2.2.3.],

Lemma 6.2. *We have*

$$\sum_{\substack{k\in\mathbb{F}_q[T]\\ \text{monic}\\ |k|=q^j}} \mu(k) = \begin{cases} 1, & \text{if } j=0,\\ -q, & \text{if } j=1,\\ 0, & \text{if } j>1. \end{cases}$$

Now we state the result which gives us the size of $\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M\right\}$.

Theorem 6.3. *There exists a $0 < \delta < 1$ such that*

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^N\right\} = S_{\mathbb{F}_q(T)}(n+1,1)q^{N(n+1)} + \mathcal{O}\left(q^{N(\delta+n)}\right),$$

where $S_{\mathbb{F}_q(T)}(n+1,1) = \frac{(q^{n+1}-1)(1-q^{-n})}{q-1}$.

Proof. We define the zeta function

$$Z_n(s) = \sum_{x\in\mathbb{P}^n(\mathbb{F}_q(T))} \frac{1}{H_n(x)^s}.$$

Then we will rewrite this function by taking the sum over all possible values of H_n, we have already seen that $H_n(x)$ is of the form q^N, where $N \in \mathbb{Z}_{\geq 0}$. Therefore we can sum over all N, instead of summing over all points in $\mathbb{P}^n(\mathbb{F}_q(T))$, to obtain

$$Z_n(s) = \sum_{N\geq 0} \frac{1}{q^{Ns}} \#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^N\right\}.$$

We know that a point $x \in \mathbb{P}^n(\mathbb{F}_q(T))$ can be written in the form $x = [a_0/b_0 : \ldots : a_n/b_n]$, where $a_0, b_0, \ldots, a_n, b_n \in \mathbb{F}_q(T)$ and $b_i \neq 0$ for all $0 \leq i \leq n$. Since x is a point in the projective space of $\mathbb{P}^n(\mathbb{F}_q(T))$, we can multiply every coordinate by $b_0 \ldots b_n$ to rewrite x in the form

$$x = [a_0 b_0 \ldots b_n : \cdots : a_n b_0 \ldots b_n].$$

We note that every coordinate is an element in $\mathbb{F}_q[T]$. If we divide every coordinate by

$$\gcd(a_0 b_0 \ldots b_n, \ldots, a_n b_0 \ldots b_n),$$

we can write x as $[x_0 : \cdots : x_n]$ where $x_1, \ldots, x_n \in \mathbb{F}_q[T]$ and $\gcd(x_1, \ldots, x_n) = 1$. This gives us that

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^N\right\} = \frac{1}{q-1}\#\left\{x = (x_0,\ldots,x_n) \in \mathbb{F}_q[T]^{n+1}\backslash\{\vec{0}\} \mid \gcd(x_0,\ldots,x_n) = 1, \max_{0\leq i\leq n} |x_i| = q^N\right\},$$

where the $\frac{1}{q-1}$, comes from the fact that $\mathbb{F}_q$ has $q-1$ non-zero elements. Therefore we can rewrite the zeta function as

$$Z_n(s) = \frac{1}{q-1}\sum_{N\geq 0} \frac{1}{q^{Ns}}\#\left\{(x_0,\ldots,x_n) \in \mathbb{F}_q[T]^{n+1}\backslash\{\vec{0}\} \mid \gcd(x_0,\ldots,x_n) = 1, \max_{0\leq i\leq n} |x_i| = q^N\right\}.$$

Since we have that the greatest common divisor of the coordinates should be equal to one, we can use the indicator function from Lemma 6.1 to rewrite the zeta function as

$$Z_n(s) = \frac{1}{q-1} \sum_{N \geq 0} \frac{1}{q^{Ns}} \sum_{\substack{(x_0,\ldots,x_n) \in \mathbb{F}_q[T]^{n+1} \\ \max_{0 \leq i \leq n} |x_i| = q^N}} \sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k | \gcd(x_0,\ldots,x_n)}} \mu(k).$$

Now we notice that if $k \mid \gcd(x_0, \ldots, x_n)$ if and only if $k \mid x_i$ for all $0 \leq i \leq n$. Let $y_i := x_i/k \in \mathbb{F}_q[T]$, Then we have that $x_i = ky_i$ for all $0 \leq i \leq n$. So by a change of variables we get that

$$Z_n(s) = \frac{1}{q-1} \sum_{N \geq 0} \frac{1}{q^{Ns}} \sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k \neq 0}} \sum_{\substack{(y_0,\ldots,y_n) \in \mathbb{F}_q[T]^{n+1} \\ \max_{0 \leq i \leq n} |ky_i| = q^N}} \mu(k).$$

Now we notice that $\max_{0 \leq i \leq n} |ky_i| = q^N$ is equivalent to $\max_{0 \leq i \leq n} |y_i| = q^N/|k|$. Therefore if we sum over all possible values of $|k| = q^{\deg k}$ we arrive at

$$Z_n(s) = \frac{1}{q-1} \sum_{j \geq 0} \sum_{\substack{k \in \mathbb{F}_q[T] \\ k \text{ monic} \\ |k| = q^j}} \mu(k) \sum_{N \geq 0} \frac{1}{q^{Ns}} \# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \mid \max_{0 \leq i \leq n} |x_i| = q^{N-j} \right\}.$$

If $N = 0$, then j must be zero, since $N - j \geq 0$. For $x \in \mathbb{F}_q[T]^{n+1}$, such that $|x| = \max_{0 \leq 1 \leq n} |x_i| = 1$, we have that $|x_i| = 1$ for all $0 \leq i \leq 1$. This gives us that $\deg(x_i) = 0$, which means that x_i is constant for all $0 \leq i \leq n$. Thus we get that

$$\# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \mid \max_{0 \leq i \leq n} |x_i| = 1 \right\} = q^{n+1} - 1.$$

If $N \geq 1$, then we have q^{N-j} monic polynomials of degree $N - j$ if $N \geq j$. This gives that

$$\# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \mid \max_{0 \leq i \leq n} |x_i| \leq q^{N-j}, x_i \text{ monic, for all } 0 \leq i \leq n \right\} = q^{(N-j)(n+1)}.$$

But since we do not require for x_i to be monic for $0 \leq i \leq n$, we must determine the number of possible leading coefficients, not all zero, of these $n + 1$ polynomials. But this is precisely the case when $N = j = 0$, therefore we obtain

$$\# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \mid \max_{0 \leq i \leq n} |x_i| = q^{N-j} \right\} = q^{(N-j)(n+1)}(q^{n+1} - 1).$$

From Lemma 6.2, we recall that

$$\sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ |k| = q^j}} \mu(k) = \begin{cases} 1, & \text{if } j = 0, \\ -q, & \text{if } j = 1, \\ 0, & \text{if } j > 1. \end{cases}$$

Since $Z_n(s)$ is a sum over $j \geq 0$, we can compute it by first taking $j = 0$, and then the sum over $j \geq 1$. For $j = 0$, we get that

$$\frac{1}{q-1} \sum_{\substack{k \in \mathbb{F}_q[T] \\ k \text{ monic} \\ |k| = q^j}} \mu(k) \sum_{N \geq 0} \frac{1}{q^{Ns}} \# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \mid \max_{0 \leq i \leq n} |x_i| = q^{N-j} \right\} =$$

$$\frac{1}{q-1} \left(q^{n+1} - 1 + \sum_{N \geq 1} \frac{q^{N(n+1)}(q^{n+1} - 1)}{q^{Ns}} \right).$$

If $j = 1$, we get that

$$\frac{1}{q-1}\sum_{\substack{k\in\mathbb{F}_q[T]\\ k \text{ monic}\\ |k|=q^j}}\mu(k)\sum_{N\geq 0}\frac{1}{q^{Ns}}\#\left\{(x_0,\ldots,x_n)\in\mathbb{F}_q[T]^{n+1}\backslash\{\vec{0}\} \mid \max_{0\leq i\leq n}|x_i| = q^{N-j}\right\} =$$

$$\frac{1}{q-1}\left(-q\left(\sum_{N\geq 0}\frac{q^{(N-1)(n+1)}(q^{n+1}-1)}{q^{Ns}}\right)\right).$$

Now we see that

$$\frac{1}{q-1}\left(-q\left(\sum_{N\geq 0}\frac{q^{(N-1)(n+1)}(q^{n+1}-1)}{q^{Ns}}\right)\right) = -\frac{1}{q-1}\left(\sum_{N\geq 0}\frac{q^{(N-1)(n+1)+1}(q^{n+1}-1)}{q^{Ns}}\right)$$
$$= -\frac{1}{q-1}\left(\sum_{N\geq 1}\frac{q^{(N-1)(n+1)+1}(q^{n+1}-1)}{q^{Ns}}\right).$$

Finally if $j > 1$, then we get by Lemma 6.2 that

$$\frac{1}{q-1}\sum_{\substack{k\in\mathbb{F}_q[T]\\ k \text{ monic}\\ |k|=q^j}}\mu(k)\sum_{N\geq 0}\frac{1}{q^{Ns}}\#\left\{(x_0,\ldots,x_n)\in\mathbb{F}_q[T]^{n+1}\backslash\{\vec{0}\} \mid \max_{0\leq i\leq n}|x_i| = q^{N-j}\right\} = 0.$$

If we combine these results we arrive at

$$\begin{aligned}
Z_n(s) &= \frac{1}{q-1}\left(q^{n+1}-1+\sum_{N\geq 1}\frac{q^{N(n+1)}(q^{n+1}-1)}{q^{Ns}}\right) - \frac{1}{q-1}\left(\sum_{N\geq 1}\frac{q^{(N-1)(n+1)+1}(q^{n+1}-1)}{q^{Ns}}\right)\\
&= \frac{q^{n+1}-1}{q-1} + \frac{q^{n+1}-1}{q-1}\sum_{N\geq 1}\frac{q^{N(n+1)}-q^{(N-1)(n+1)+1}}{q^{Ns}}\\
&= \frac{q^{n+1}-1}{q-1}\cdot\frac{1-q^{1-s}}{1-q^{n+1-s}}.
\end{aligned}$$

Therefore we can see that $Z_n(s)$ has a simple pole at $s = n+1$, where the residue of this pole is given by,

$$\begin{aligned}
\lim_{s\to n+1}(s-n-1)Z_n(s) &= \lim_{s\to n+1}(s-n-1)\left(\frac{q^{n+1}-1}{q-1}\cdot\frac{1-q^{1-s}}{1-q^{n+1-s}}\right)\\
&= \frac{q^{n+1}-1}{q-1}\lim_{s\to n+1}\left(\frac{(s-n-1)(1-q^{1-s})}{1-q^{n+1-s}}\right).
\end{aligned}$$

Using L'Hôpital's rule [2], we can compute this limit as follows

$$\begin{aligned}
\lim_{s\to n+1}(s-n-1)Z_n(s) &= \frac{q^{n+1}-1}{q-1}\lim_{s\to n+1}\frac{1-q^{1-s}+(s-n-1)q^{1-s}\log(q)}{q^{n+1-s}\log(q)}\\
&= \frac{(q^{n+1}-1)(1-q^{-n})}{(q-1)\log(q)}\\
&= \frac{S_{\mathbb{F}_q(T)}(n+1,1)}{\log(q)}.
\end{aligned}$$

Now we want to apply the function field version of the Wiener-Ikehara Tauberian theorem, Theorem 5.2. But $Z_n(s)$ has a pole at $s = n+1$ so we cannot apply the theorem directly. If we substitute s by $s+n$ we get

$$Z_n(s+n) = \frac{q^{n+1}-1}{q-1}\cdot\frac{1-q^{1-n-s}}{1-q^{1-s}},$$

which has a simple pole at $s = 1$ with the same residue. Since we have that

$$Z_n(s) = \sum_{N\geq 0} \frac{1}{q^{Ns}} \# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N \right\},$$

we get that

$$Z_n(s+n) = \sum_{N\geq 0} \frac{1}{q^{N(s+n)}} \# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N \right\}.$$

If we define $F : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ by

$$F(N) = \# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N \right\} q^{-nN},$$

we can use theorem 5.2 to conclude that there exists a $\delta < 1$, such that

$$F(N) = \frac{S_{\mathbb{F}_q(T)}(n+1,1)}{\log(q)} \log(q) q^N + \mathcal{O}(q^{\delta N}).$$

This gives us that

$$\# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N \right\} = S_{\mathbb{F}_q(T)}(n+1,1) q^{N(n+1)} + q^{nN} \mathcal{O}(q^{\delta N}).$$

So we get the following result

$$\# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N \right\} = S_{\mathbb{F}_q(T)}(n+1,1) q^{N(n+1)} + \mathcal{O}\left(q^{N(\delta+n)} \right).$$

Which completes our proof. □

6.2 Points of bounded height where all coordinates are the same power

We want to generalize our previous result to the situation where all coordinates are the same given power. Let $l \in \mathbb{Z}_{>0}$, we say that $x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T))$ is a l-th power if we can write $x = [x_0' : \cdots : x_n']$ such than $x_0', \ldots, x_n' \in \mathbb{F}_q[T]$ and $\gcd(x_0', \ldots, x_n') = 1$ and we have that for every x_i' there exist a $y_i \in \mathbb{F}_q(T)$ such that $y_i^l = x_i'$ for all $0 \leq i \leq n$. Note that we can write every point $x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T))$ such that there exists $x_0', \ldots, x_n' \in \mathbb{F}_q[T]$ with $\gcd(x_0', \ldots, x_n') = 1$, and $x = [x_0' : \cdots : x_n']$. So the extra property that we require our point to have is that all coordinates are l-th powers.

Then we are interested in the points of bounded height, where every point is a l-th power. In particular we want to find $\# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^M, x \text{ is a } l\text{-th power} \right\}$. Then we get the following result

Theorem 6.4. *There exists a $0 < \delta < 1$ such that*

$$\# \left\{ x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^M, x \textit{ is a } l\textit{-th power} \right\} = S_{\mathbb{F}_q(T)}(n+1,1) q^{N(n+1)/l} + \mathcal{O}(q^{N(\delta+n/l)}).$$

Proof. We define the following zeta function

$$\zeta_g(s) = \sum_{x \in \mathbb{P}^n(\mathbb{F}_q(T))} \frac{g(x)}{H_n(x)^s},$$

where we take $g : \mathbb{P}^n(\mathbb{F}_q(T)) \to \{0,1\}$ by

$$g(x) = \begin{cases} 1 & \text{if } x \text{ is a } l\text{-th power}, \\ 0 & \text{otherwise} \end{cases}$$

as an indicator function of the property that x is a l-th power. Then we can rewrite this function by taking the sum over all possible values of H_n. We have seen that $H_n(x)$ is of the form q^N, with

$N \in \mathbb{Z}_{\geq 0}$. If we take x to be a l-th power, we have that $H_n(x)$ has to be of the form q^{lN}. Thus we can take the sum over all possible N, to obtain

$$\begin{aligned}\zeta_g(s) &= \sum_{N\geq 0} \frac{1}{q^{Ns}} \#\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x \text{ is a } l\text{-th power}\} \\ &= \sum_{N\geq 0} \frac{1}{q^{lNs}} \#\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^{lN}, x \text{ is a } l\text{-th power}\}.\end{aligned}$$

With the same steps as in the proof of 6.3 we have that

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^{lN}, x \text{ is a } l\text{-th power}\right\} = \\ \frac{1}{q-1} \# \left\{x = (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \;\middle|\; {\scriptstyle \gcd(x_0,\ldots,x_n)=1, \max_{0\leq i\leq n} |x_i| = q^{lN}, \atop x_i \text{ is a } l\text{-th power for all } 0\leq i\leq n} \right\}.$$

Therefore we can rewrite the zeta function as

$$\zeta_g(s) = \frac{1}{q-1} \sum_{N\geq 0} \frac{1}{q^{lNs}} \# \left\{x = (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{\vec{0}\} \;\middle|\; {\scriptstyle \gcd(x_0,\ldots,x_n)=1, \max_{0\leq i\leq n} |x_i| = q^{lN}, \atop x_i \text{ is a } l\text{-th power for all } 0\leq i\leq n} \right\}.$$

Using the Möbius function we can rewrite the zeta function as

$$\zeta_g(s) = \frac{1}{q-1} \sum_{N\geq 0} \frac{1}{q^{lNs}} \sum_{\substack{(x_0,\ldots,x_n) \in \mathbb{F}_q[T]^{n+1} \\ \max_{0\leq i\leq n} |x_i| = q^{lN} \\ x_i \text{ is a } l\text{-th power for all } 0\leq i\leq n}} \sum_{\substack{k \in \mathbb{F}_q[T] \\ \text{monic} \\ k \mid \gcd(x_0,\ldots,x_n)}} \mu(k).$$

We know that $k \mid \gcd(x_0, \ldots, x_n)$ if and only if $k \mid x_i$, for all $0 \leq i \leq n$. Therefore for every $0 \leq i \leq n$ we can find a $y_i \in \mathbb{F}_q[T]$ such that $x_i = ky_i$. Furthermore we have that x_i is a l-th power for every $0 \leq i \leq n$, so we can find $z_i \in \mathbb{F}_q[T]$ such that $z_i^l = x_i$. If we combine this we get that $z_i^l = ky_i$ for all $0 \leq i \leq n$. If $\mu(k) \neq 0$, then k is square free, and we have that $k \mid z_i^l$ for all $0 \leq i \leq n$. Therefore we can conclude that $k \mid z_i$, for every $0 \leq i \leq n$. Thus we can find a $w_i \in \mathbb{F}_q[T]$ such that $z_i = kw_i$ for every $0 \leq i \leq n$. Therefore we are counting the points that are given by $(w_0, \ldots, w_n) \in \mathbb{F}_q[T]$ such that $\max_{0\leq i\leq n} |w_i^l k^l| \leq q^{lN}$. Thus we are in fact counting the points that are given by $(w_0, \ldots, w_n) \in \mathbb{F}_q[T]$ such that $\max_{0\leq i\leq n} |w_i k| \leq q^N$. So if we now sum over all possible values of the degree of k, we get

$$\zeta_g(s) = \frac{1}{q-1} \sum_{j\geq 0} \sum_{\substack{k \in \mathbb{F}_q[T] \\ k \text{ monic} \\ |k| = q^j}} \mu(k) \sum_{N\geq 0} \frac{1}{q^{lNs}} \# \left\{(x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \backslash \{0\} \mid \max_{0\leq i\leq n} |x_i| = q^{N-j}\right\} = Z_n(ls).$$

This has a simple pole at $s = \frac{n+1}{l}$. Therefore we substitute s by $\frac{s+n}{l}$ and we get

$$\zeta_g(\frac{s+n}{l}) = Z_n(s+n) = \frac{q^{n+1}-1}{q-1} \cdot \frac{1-q^{1-s+n}}{1-q^{1-s}}.$$

Which has a pole at $s = 1$, with residue $\frac{S_{\mathbb{F}_q(T)}(n+1,1)}{\log q}$. We recall that we have

$$\zeta_g(s) = \sum_{N\geq 0} \frac{1}{q^{lNs}} \#\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^{lN}, x \text{ is a } l\text{-th power}\},$$

therefore we have that

$$\zeta_g(\frac{s+n}{l}) = \sum_{N\geq 0} \frac{1}{q^{lN(\frac{s+n}{l})}} \#\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^{lN}, x \text{ is a } l\text{-th power}\}.$$

If we now define $G : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ by

$$G(N) = \#\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x \text{ is a } l\text{-th power}\} q^{-nN/l}.$$

Then we can apply theorem 5.2 and conclude that there exists a $\delta < 1$ such that

$$G(N) = \frac{S_{\mathbb{F}_q(T)}(n+1,1)}{\log(q)} \log(q) q^{N/l} + \mathcal{O}(q^{\delta N}).$$

This gives us that

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M, x \text{ is a } l\text{-th power}\right\} = S_{\mathbb{F}_q(T)}(n+1,1) q^{N(n+1)/l} + q^{nN/l}\mathcal{O}(q^{\delta N}).$$

Therefore we get that

$$\#\left\{x \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M, x \text{ is a } l\text{-th power}\right\} = S_{\mathbb{F}_q(T)}(n+1,1) q^{N(n+1)/l} + \mathcal{O}(q^{N(\delta+n/l)}).$$

Which concludes our proof □

7 Points of bounded height where the first coordinate is a square

Now that we have seen the generalized result where every coordinate is the same power, we want to generalize even further, by taking an arbitrary power for every coordinate. First we will look at the size of the set $\left\{x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, H_n(x) = q^M, x_0 \text{ is a square}\right\}$. To heuristically determine the size of this set we will use Theorem 5.4.

7.1 The three properties of the Tauberian theorem for multi-variable Dirichlet series

We look at the following sum:

$$F(s_0, \ldots, s_n) = \sum_{\substack{x_0, \ldots x_n \in \mathbb{F}_q[T] \\ \gcd(x_0, \ldots, x_n) = 1 \\ x_0 \text{ square}}} \frac{1}{|x_0|^{s_0} \ldots |x_n|^{s_n}}.$$

Then our main goal is to apply Theorem 5.4 to this sum. The first thing that we notice is that this function is not of the same form as stated in the theorem. Therefore we need to rewrite the function.

Lemma 7.1. *We define*

$$G(d_0, \ldots, d_n) = \begin{cases} \# \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q[T]^{n+1} \,\middle|\, \substack{x_0 \text{ square} \\ \gcd(x_0, \ldots, x_n) = 1 \\ |x_i| = q^{v_i}} \right\}, & \text{if } d_i = q^{v_i} \text{ for all } i = 0, \ldots, n, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

$$F(s_0, \ldots s_n) = \sum_{d_0=1}^{\infty} \cdots \sum_{d_n=1}^{\infty} \frac{G(d_0, \ldots, d_n)}{d_0^{s_0} \ldots d_n^{s_n}}.$$

Proof. For all $i = 0, \ldots, n$ we have that $|x_i| = q^{\deg x_i}$. This gives us that

$$F(s_0, \ldots, s_n) = \sum_{\substack{x_0, \ldots x_n \in \mathbb{F}_q[T] \\ \gcd(x_0, \ldots, x_n) = 1 \\ x_0 \text{ square}}} \frac{1}{q^{s_0 \deg x_0} \ldots q^{s_n \deg x_n}}.$$

So instead of summing over all polynomials $x_0, \ldots, x_n \in \mathbb{F}_q[T]$, we sum over all possible values of $q^{s_0 \deg x_0}, \ldots, q^{s_n \deg x_n}$. So if we take $d_i = q^{\deg x_i}$, for all $i = 0, \ldots, n$, and take the sum over all d_i's we get that

$$F(s_0, \ldots s_n) = \sum_{d_0=1}^{\infty} \cdots \sum_{d_n=1}^{\infty} \frac{G(d_0, \ldots, d_n)}{d_0^{s_0} \ldots d_n^{s_n}}.$$

Which gives our wanted result. □

Now we see that the function F is in the form of Theorem 5.4. Now we want to show that the function F satisfies the properties of the Theorem. To better understand this function, we will write it as a product over the primes in $\mathbb{F}_q[T]$. Then we will see that this helps us in understanding the convergence of the sum, which is needed in the first property of Theorem 5.4.

Lemma 7.2. *We define* $f : \mathbb{F}_q[T]^{n+1} \to \{0, 1\}$ *as*

$$f(x_0, \ldots, x_n) = \begin{cases} 1, & \text{if } \gcd(x_0, \ldots, x_n) = 1, \text{and } x_0 \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$$

Suppose that $F(s_0, \ldots, s_n)$ *converges absolutely on some set* $T \subseteq \mathbb{C}$*, then we have that*

$$F(s_0, \ldots, s_n) = \prod_{P \text{ prime}} \sum_{v_0, \ldots v_n \in \mathbb{Z}_{\geq 0}} \frac{f(P^{v_0}, \ldots, P^{v_n})}{|P|^{s_0 v_0 + \cdots + s_n v_n}},$$

for $(s_0, \ldots, s_n) \in T$.

Proof. First we notice that

$$F(s_0,\dots,s_n) = \sum_{x_0,\dots,x_n\in\mathbb{F}_q[T]} \frac{f(x_0,\dots,x_n)}{|x_0|^{s_0}\dots|x_n|^{s_n}}.$$

Since $\mathbb{F}_q[T]$ is a unique factorization domain we can factor the polynomials x_i in terms of primes or every $0\le i\le n$. Therefore we have that $x_i=\prod_{P \text{ prime}} P^{e_{i,P}}$, for every $0\le i\le n$. Thus instead of taking the sum over all $x_0,\dots,x_n\in\mathbb{F}_q[T]$, we can take the product over all primes P and all possible values of $e_{i,p}\in\mathbb{Z}_{\ge 0}$. Therefore we get that

$$F(s_0,\dots,s_n) = \prod_{P \text{ prime}} \sum_{v_0,\dots,v_n\in\mathbb{Z}_{\ge0}} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0}\dots|P|^{s_nv_n}} = \prod_{P \text{ prime}} \sum_{v_0,\dots v_n\in\mathbb{Z}_{\ge0}} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}.$$

□

Before we look at which values of $\boldsymbol{s}=(s_0,\dots,s_n)$ the function F is absolutely convergent we need a strong classical result [13, Theorem 1].

Lemma 7.3. *Let $\{a_n\}_{n\in\mathbb{Z}_{\ge1}}$ be a sequence of complex numbers. Then the infinite product given by $\prod_{n=1}^{\infty}(1+a_n)$ converges absolutely if and only if $\sum_{n=1}^{\infty}|a_n|<\infty$.*

We can now use this lemma to prove the following result about the absolute convergence of F.

Lemma 7.4. *The function $F(s_0,\dots,s_n)$ is absolutely convergent for $\mathrm{Re}(s_0)>\frac{1}{2}$ and $\mathrm{Re}(s_i)>1$ for $i=1,\dots,n$.*

Proof. We have shown in Lemma 7.2 that

$$F(s_0,\dots,s_n) = \prod_{P \text{ prime}} \sum_{v_0,\dots v_n\in\mathbb{Z}_{\ge0}} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}.$$

Then for every prime P, if we can take $v_0=v_1=\dots=v_n=0$, we get $\frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}=1$. Thus we have a product of the form $\prod_{P \text{ prime}}(1+a_P)$. But since the set of all primes in $\mathbb{F}_q[T]$ is countable, we can apply Lemma 7.3, to conclude that $F(s_0,\dots,s_n)$ is absolutely convergent if and only if

$$\sum_{P \text{ prime}} \sum_{(v_0,\dots,v_n)\neq(0,\dots,0)} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}$$

is absolutely convergent. Then we rewrite this sum as

$$\sum_{P \text{ prime}} \left(\left(\sum_{v_0=0}^{\infty}\dots\sum_{v_n=0}^{\infty} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}\right)-1\right).$$

Here we subtract one for the case when $v_0=\dots=v_n=0$. We have

$$|P|^{s_0v_0+\dots+s_nv_n} = |P|^{s_0v_0}\dots|P|^{s_nv_n},$$

so we get that the sum equals

$$\sum_{P \text{ prime}} \left(\left(\sum_{v_0=0}^{\infty}\dots\sum_{v_n=0}^{\infty} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0}\dots|P|^{s_nv_n}}\right)-1\right).$$

Now we see that $f(P^{v_0},\dots,P^{v_n})=1$, if v_0 is even, and 0 otherwise. Therefore we can rewrite the sum as

$$\sum_{P \text{ prime}} \left(\left(\sum_{v_0=0}^{\infty}\dots\sum_{v_n=0}^{\infty} \frac{1}{|P|^{2s_0v_0}\dots|P|^{s_nv_n}}\right)-1\right).$$

Since every power of $|P|$ of the form $|P|^{s_i v_i}$, is only dependent on v_i, for every $i = 0, \dots n$, and independent of v_j, for $j \neq i$, we get that the sum is equal to

$$\sum_{P \text{ prime}} \left(\left(\sum_{v_0=0}^{\infty} \frac{1}{|P|^{2v_0 s_0}} \sum_{v_1=0}^{\infty} \frac{1}{|P|^{v_1 s_1}} \cdots \sum_{v_n=0}^{\infty} \frac{1}{|P|^{v_n s_n}} \right) - 1 \right).$$

If we now look at the sum

$$\sum_{v_0=0}^{\infty} \frac{1}{|P|^{2v_0 s_0}} = \sum_{v_0=0}^{\infty} \frac{1}{(|P|^{2s_0})^{v_0}},$$

we may recognize it as a geometric series. Therefore we have for $\mathrm{Re}(2s_0) > 1$ that

$$\sum_{v_0=0}^{\infty} \frac{1}{(|P|^{2s_0})^{v_0}} = \left(1 - \frac{1}{|P|^{2s_0}}\right)^{-1}.$$

Notice that $\mathrm{Re}(2s_0) > 1$ if and only if $\mathrm{Re}(s_0) > 1/2$. Let $i \in \{1, \dots, n\}$, then we look at the sum

$$\sum_{v_i=0}^{\infty} \frac{1}{|P|^{v_i s_i}} = \sum_{v_i=0}^{\infty} \frac{1}{(|P|^{s_i})^{v_i}},$$

which is again a geometric series. Therefore we get that for $\mathrm{Re}(s_i) > 1$, that the sum equals

$$\sum_{v_i=0}^{\infty} \frac{1}{(|P|^{s_i})^{v_i}} = \left(1 - \frac{1}{|P|^{s_i}}\right)^{-1}.$$

If we combine these results we obtain

$$\sum_{P \text{ prime}} \left(\left(\sum_{v_0=0}^{\infty} \frac{1}{|P|^{2v_0 s_0}} \sum_{v_1=0}^{\infty} \frac{1}{|P|^{v_1 s_1}} \cdots \sum_{v_n=0}^{\infty} \frac{1}{|P|^{v_n s_n}} \right) - 1 \right) =$$
$$\sum_{P \text{ prime}} \left(\left(1 - \frac{1}{|P|^{2s_0}}\right)^{-1} \left(1 - \frac{1}{|P|^{s_1}}\right)^{-1} \cdots \left(1 - \frac{1}{|P|^{s_n}}\right)^{-1} - 1 \right).$$

Now we apply Lemma 7.3 we see that this sum converges absolutely if and only if

$$F(s_0, \dots, s_n) = \prod_{P \text{ prime}} \left(\left(1 - \frac{1}{|P|^{2s_0}}\right)^{-1} \left(1 - \frac{1}{|P|^{s_1}}\right)^{-1} \cdots \left(1 - \frac{1}{|P|^{s_n}}\right)^{-1} \right) \tag{3}$$

converges absolutely. If we recall from equation (1) that

$$\zeta_A(s) = \prod_{P \text{ prime}} \left(1 - \frac{1}{|P|^{s}}\right)^{-1},$$

then we get that

$$\prod_{P \text{ prime}} \left(\left(1 - \frac{1}{|P|^{2s_0}}\right)^{-1} \left(1 - \frac{1}{|P|^{s_1}}\right)^{-1} \cdots \left(1 - \frac{1}{|P|^{s_n}}\right)^{-1} \right) = \zeta_A(2s_0)\zeta_A(s_1) \dots \zeta_A(s_n).$$

We know that $\zeta_A(s)$ is a meromorphic function on $\mathbb{C}$ with simple poles at the points

$$\left\{ z \in \mathbb{C} \mid \mathrm{Re}(z) = 1, \mathrm{Im}(z) = \frac{2\pi m}{\log(q)} \text{ for } m \in \mathbb{Z} \right\}.$$

Therefore we have that

$$\zeta_A(2s_0)\zeta_A(s_1) \dots \zeta_A(s_n)$$

is absolutely convergent on for $\mathrm{Re}(s_0) > \frac{1}{2}$ and $\mathrm{Re}(s_i) > 1$ for $i = 1, \dots, n$. This implies that $F(s_0, \dots, s_n)$ is absolutely convergent for $\mathrm{Re}(s_0) > \frac{1}{2}$ and $\mathrm{Re}(s_i) > 1$ for $i = 1, \dots, n$. □

Now that we have seen that the sum

$$F(s_0,\dots,s_n) = \sum_{\substack{x_0,\dots x_n\in\mathbb{F}_q[T]\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ square}}} \frac{1}{|x_0|^{s_0}\dots|x_n|^{s_n}}$$

is convergent for $\mathrm{Re}(s_0) > 1/2$ and $\mathrm{Re}(s_i) > 1$ for $i = 1,\dots,n$, we define $\boldsymbol{a} = (a_0, a_1, \dots, a_n) = (1/2, 1, \dots, 1)$. This means that the series F satisfies the first property of Theorem 5.4.

Now we look at the second property of the theorem. We define the following function

$$H(s_0,\dots,s_n) = F(s_0 + 1/2, s_1 + 1,\dots,s_n + 1)\prod_{i=0}^{n} s_i.$$

We will now show that the function H is holomorphic on

$$\left\{(s_0,\dots,s_n)\in\mathbb{C}^{n+1} \mid \mathrm{Re}(s_i)\geq 0, -\frac{\pi}{\log(q)} \leq \mathrm{Im}(s_i) \leq \frac{\pi}{\log(q)} \text{ for all } i = 0,\dots,n\right\}.$$

This will imply that there exists a $\delta_1 > 0$ such that $H(s_0,\dots,s_n)$ is holomorphic on the domain

$$\left\{\boldsymbol{s}\in\mathbb{C}^{n+1} \mid \mathrm{Re}(s_i) > -\delta_1, -\frac{\pi}{\log(q)} \leq \mathrm{Im}(s_i) \leq \frac{\pi}{\log(q)}, \text{for all } i = 0,\dots,n\right\}.$$

Now we state the following result,

Lemma 7.5. *The function $H(s_0,\dots,s_n)$ can be extended to a holomorphic function on*

$$\left\{(s_0,\dots,s_n)\in\mathbb{C}^{n+1} \mid \mathrm{Re}(s_i)\geq 0, -\frac{\pi}{\log(q)} \leq \mathrm{Im}(s_i) \leq \frac{\pi}{\log(q)},\ \textit{for all } i = 0,\dots,n\right\}.$$

Proof. From Lemma 7.2 we have that

$$F(s_0,\dots,s_n) = \prod_{P\text{ prime}}\left(\sum_{v_0,\dots v_n\in\mathbb{Z}_{\geq 0}} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{s_0v_0+\dots+s_nv_n}}\right).$$

This means that we have that

$$F(s_0+1/2, s_1+1\dots,s_n+1) = \prod_{P\text{ prime}}\left(\sum_{v_0,\dots v_n\in\mathbb{Z}_{\geq 0}} \frac{f(P^{v_0},\dots,P^{v_n})}{|P|^{(s_0+1/2)v_0+\dots+(s_n+1)v_n}}\right).$$

Then by equation (3) we get that

$$F(s_0+1/2,\dots,s_n+1) = \zeta_A(2s_0+1)\prod_{i=1}^{n}\zeta_A(s_i+1).$$

We have that $\zeta_A(2s_0+1)$ is meromorphic function on $\mathbb{C}$ with simple poles at $\mathrm{Re}(s_0) = 0, \mathrm{Im}(s_0) = \frac{2\pi m}{\log(q)}$, with $m\in\mathbb{Z}$. For $1\leq i\leq n$, we have that $\zeta_A(s_i+1)$ is meromorphic function on $\mathbb{C}$ with simple poles at $\mathrm{Re}(s_i) = 0, \mathrm{Im}(s_i) = \frac{2\pi m}{\log(q)}$, with $m\in\mathbb{Z}$. Therefore we have that F can be extended to a meromorphic function on $\mathbb{C}^{n+1}$, except for simple poles at $\mathrm{Re}(s_0) = 0$ or $\dots$ or $\mathrm{Re}(s_n) = 0$.

By definition we have that

$$H(s_0,\dots,s_n) = F(s_0 + 1/2, s_1 + 1,\dots,s_n + 1)\prod_{i=0}^{n} s_i.$$

Here we can easily see that the product

$$\prod_{i=0}^{n} s_i$$

has simple zeros at $s_i = 0$, for $i = 0, \ldots, n$. This means that this product multiplied with $F(s_0 + 1/2, \ldots .s_n + 1)$, can be extended to a holomorphic function at

$$\left\{(s_0, \ldots, s_n) \in \mathbb{C}^{n+1} \mid \operatorname{Re}(s_i) \geq 0, -\frac{\pi}{\log(q)} \leq \operatorname{Im}(s_i) \leq \frac{\pi}{\log(q)}, \text{ for all } i = 0, \ldots, n\right\}.$$

Which concludes our proof. □

In this proof, we notice that we don't need a family of linear forms $\{h^{(r)}\}_{r\in\mathcal{R}}$, which is used in the second property of Theorem 5.4. This means that we can choose an arbitrary δ_3.

Now that we looked at the the second property of Theorem 5.4, we will look at the third property of the theorem. This property looks for an upper bound for the series H. Here we can use the result from Corollary 3.7 to show that H, has an upper bound which is in the right shape.

Lemma 7.6. *Let H be defined as before, and δ_1 as in the proof of Lemma 7.5. Then, for $\tilde{\epsilon} > 0$ and $\epsilon' > 0$ sufficiently small, we have,*

$$H(s_0, \ldots, s_n) \ll \prod_{i=1}^{n} (|\operatorname{Im}(s_i) + 1|)^{1-\min\{\operatorname{Re}(s_i),0\}} (1 + ||\operatorname{Im}(s_0, \ldots, s_n)||_1^{\tilde{\epsilon}}),$$

on the domain $\mathcal{D}(\delta_1 - \epsilon', \delta_3 - \epsilon')$.

Proof. First we rewrite $H(s_0, \ldots, s_n)$ as follows,

$$H(s_0, \ldots, s_n) = L(s_0, \ldots, s_n)\zeta(2s_0 + 1) \prod_{i=1}^{n} \zeta(s_i + 1) \prod_{i=0}^{n} s_i,$$

where we define

$$L(s_0, \ldots, s_n) := F(s_0 + 1/2, \ldots, s_n + 1)\zeta(2s_0 + 1)^{-1} \prod_{i=1}^{n} \left(\zeta(s_i + 1)^{-1}\right).$$

Here ζ denotes the Riemann-zeta function. Then we first look at $|L(s)|$, then we have seen in the proof of Lemma 7.5, that

$$F(s_0 + 1/2, \ldots, s_n + 1) = \zeta_A(2s_0 + 1) \prod_{i=1}^{n} \zeta_A(s_i + 1),$$

for $\operatorname{Re}(s_0), \ldots, \operatorname{Re}(s_n) > 0$. This gives us that the function $F(s_0 + 1/2, \ldots, s_n + 1)$ is analytic when $\operatorname{Re}(s_0), \ldots, \operatorname{Re}(s_n) > 0$. Furthermore we have that $\zeta(s)^{-1}$ is analytic when $\operatorname{Re}(s) > 1$. Therefore we get that the function $L(s_0, \ldots, s_n)$ is analytic on $\operatorname{Re}(s_0), \ldots, \operatorname{Re}(s_n) > 0$. This means that for a bounded domain in $\mathcal{D}(\delta_1 - \epsilon', \delta_3 - \epsilon')$ we can find a constant in $C \in \mathbb{R}$ such that $|L(s_0, \ldots, s_n)| \leq C$, for $(s_0, \ldots, s_n) \in \mathcal{D}(\delta_1 - \epsilon', \delta_3 - \epsilon')$.

Now we will look at

$$\zeta(2s_0 + 1) \prod_{i=1}^{n} \zeta(s_i + 1) \prod_{i=0}^{n} s_i.$$

If we take the absolute value we get

$$|\zeta(2s_0 + 1) \prod_{i=1}^{n} \zeta(s_i + 1) \prod_{i=0}^{n} s_i| = |s_0||\zeta(2s_0 + 1)| \prod_{i=1}^{n} |s_i||\zeta(s_i + 1)|.$$

Then we will first find an upper bound for $|s_0||\zeta(2s_0+1)|$. We get,

$$|s_0||\zeta(2s_0+1)| = \frac{1}{2}|2s_0||\zeta(2_0+1)|.$$

Then we apply Corollary 3.7 to obtain that $|s_0||\zeta(2s_0+1)| \ll \frac{1}{2}(|\operatorname{Im}(2s_0)|+1)^{1-\min\{\operatorname{Re}(2s_0),0\}+\epsilon_0}$, where ϵ_0 is sufficiently small. Since $\min\{\operatorname{Re}(2s_0),0\} \leq \min\{\operatorname{Re}(s_0),0\}$ we get that

$$\frac{1}{2}(|\operatorname{Im}(2s_0)|+1)^{1-\min\{\operatorname{Re}(2s_0),0\}+\epsilon_0} \leq \frac{1}{2}(|\operatorname{Im}(2s_0)|+1)^{1-\min\{\operatorname{Re}(s_0),0\}+\epsilon_0}.$$

Furthermore we have that $\frac{1}{2}(|\operatorname{Im}(2s_0)|+1)^{1-\min\{\operatorname{Re}(s_0),0\}+\epsilon_0} \leq (|\operatorname{Im}(s_0)|+1)^{1-\min\{\operatorname{Re}(s_0),0\}+\epsilon_0}$. So we can conclude that $|s_0||\zeta(2s_0+1)| \ll (|\operatorname{Im}(s_0)|+1)^{1-\min\{\operatorname{Re}(s_0),0\}+\epsilon_0}$.

If we take $i \in \{1,\dots,n\}$ then we apply Corollary 3.7 to obtain

$$|s_i||\zeta(s_i+1)| \leq\ll (|\operatorname{Im}(s_i)|+1)^{1-\min\{\operatorname{Re}(s_i),0\}+\epsilon_i}.$$

Then everything combined gives us that

$$H(s_0,\dots,s_n) \ll \prod_{i=0}^{n}(|\operatorname{Im}(s_i)|+1)^{1-\min\{\operatorname{Re}(s_i),0\}+\epsilon_i}.$$

Now we take $\epsilon = \max_{i\in\{0,\dots,n\}} \epsilon_i$, then we obtain

$$H(s_0,\dots,s_n) \ll \prod_{i=0}^{n}(|\operatorname{Im}(s_i)|+1)^{1-\min\{\operatorname{Re}(s_i),0\}+\epsilon}.$$

We can further rewrite this as

$$\prod_{i=0}^{n}(|\operatorname{Im}(s_i)|+1)^{1-\min\{\operatorname{Re}(s_i),0\}}(|\operatorname{Im}(s_i)|+1)^{\epsilon}.$$

WWe find the following upper bound for $\prod_{i=0}^{n}(|\operatorname{Im}(s_i)|+1)^{\epsilon}$ by,

$$\prod_{i=0}^{n}(|\operatorname{Im}(s_i)|+1)^{\epsilon} \leq \prod_{i=0}^{n}\left(\max_{i=0,\dots,n}\{|\operatorname{Im}(s_i)|+1\}\right)^{\epsilon}.$$

If we define $M := \max_{i=0,\dots,n}\{|\operatorname{Im}(s_i)|\}$, we get

$$\prod_{i=0}^{n}\left(\max_{i=0,\dots,n}\{|\operatorname{Im}(s_i)|+1\}\right)^{\epsilon} = (M+1)^{(n+1)\epsilon}.$$

Using the binomial theorem we obtain,

$$(M+1)^{(n+1)\epsilon} = \left(1+(n+1)M+\binom{n+1}{2}M^2+\cdots+M^{n+1}\right)^{\epsilon} \leq (1+C'M^{n+1})^{\epsilon},$$

where C' is a constant independent of M. Now we can further estimate this from above as follows,

$$\begin{aligned}(1+C'M^{n+1})^{\epsilon} &\leq (2\max\{1,C'M^{n+1}\})^{\epsilon}\\ &= 2^{\epsilon}\max\{1,C'M^{n+1}\}^{\epsilon}\end{aligned}$$

If we take $\tilde{\epsilon} := (n+1)\epsilon$ and take $C = 2^{\epsilon}\max\{1,(C')^{\epsilon}\}$, we get

$$\begin{aligned}(1+C'M^{n+1})^{\epsilon} &\leq 2^{\epsilon}\max\{1,C'M^{n+1}\}^{\epsilon}\\ &\leq 2^{\epsilon}(1+(C')^{\epsilon}M^{\tilde{\epsilon}})\\ &\leq 2^{\epsilon}\max\{1,(C')^{\epsilon}\}(1+M^{\tilde{\epsilon}})\\ &= C(1+M^{\tilde{\epsilon}}).\end{aligned}$$

Since C' was independent of M we have that C is independent of M. We get,

$$\begin{aligned}C(1+M^{\tilde{\epsilon}}) &= C(1+\max_{i=0,\dots,n}\{|\operatorname{Im}(s_i)|\}^{\tilde{\epsilon}}) \\ &\leq C\left(1+\left(\sum_{i=0}^{n}|\operatorname{Im}(s_i)|\right)^{\tilde{\epsilon}}\right) \\ &= C(1+||\operatorname{Im}(s_0,\dots,s_n)||_1^{\tilde{\epsilon}}).\end{aligned}$$

We can finish our proof by concluding that for $\tilde{\epsilon} > 0$ and $\epsilon' > 0$ sufficiently small, we have,

$$H(s_0,\dots,s_n) \ll \prod_{i=1}^{n}(|\operatorname{Im}(s_i)+1|)^{1-\min\{\operatorname{Re}(s_i),0\}}(1+||\operatorname{Im}(s_0,\dots,s_n)||_1^{\tilde{\epsilon}}),$$

on the domain $\mathcal{D}(\delta_1-\epsilon',\delta_3-\epsilon')$. □

7.2 Determining the size of the set of points of bounded height where the first coordinate is a square

We have now seen that the series F satisfies almost all of the properties needed for the usage of Theorem 5.4. We will state a conjecture which uses the theorem heuristically. Recall by Lemma 7.1 that we have

$$F(s_0,\dots s_n) = \sum_{d_0=1}^{\infty}\cdots\sum_{d_n=1}^{\infty}\frac{G(d_0,\dots,d_n)}{d_0^{s_0}\dots d_n^{s_n}},$$

where we defined

$$G(d_0,\dots,d_n) = \begin{cases}\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1} \mid {\scriptstyle \substack{x_0 \text{ square} \\ \gcd(x_0,\dots,x_n)=1 \\ |x_i|=q^{v_i}}}\right\}, & \text{if } d_i = q^{v_i} \text{ for all } i=0,\dots,n,\\ 0, & \text{otherwise.}\end{cases}$$

With this notation we can finally state the result that follows from the theorem.

Conjecture 7.7. *There exists a constant $\theta > 0$ and a constant $V \in \mathbb{R}$ such that,*

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1} \;\middle|\; {\scriptstyle \substack{|x_i|\leq q^N,\ \textit{for all } i=0,\dots,n \\ \gcd(x_0,\dots,x_n)=1 \\ x_0 \textit{ is a square}}}\right\} = q^{N(1/2+n)}(V+\mathcal{O}(q^{-\theta N})),$$

Heuristic Proof. In the lemmas above, in particular Lemma 7.4, Lemma 7.5 and Lemma 7.6, we have seen that the series F satisfies the properties $(P1)$, $(P3)$ and almost property $(P2)$ of Theorem 5.4. If we could apply this theorem we would find that there exists a polynomial $Q_{\boldsymbol{\beta}}$, of degree at most $n+1-\operatorname{rank}\{s_i\}_{i=0}^n$, and a real number $\theta > 0$, such that

$$\begin{aligned}S(X,\boldsymbol{\beta}) &:= \sum_{1\leq d_0\leq X^{\beta_0}}\cdots\sum_{1\leq d_n\leq X^{\beta_n}} G(d_0,\dots,d_n) \\ &= X^{\langle \boldsymbol{a},\boldsymbol{\beta}\rangle}\left(Q_{\boldsymbol{\beta}}(\log(X)+\mathcal{O}(X^{-\theta})\right).\end{aligned}$$

If we take $\beta_0=\dots=\beta_n=1$, for all the values of the β_i's and we take $X=q^N$, then we have that

$$\begin{aligned}S(q^N,(1,\dots,1)) &= \sum_{1\leq d_0\leq q^N}\cdots\sum_{1\leq d_n\leq q^N} G(d_0,\dots,d_n) \\ &= \#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1} \;\middle|\; {\scriptstyle \substack{|x_i|\leq q^N,\ \text{for all } i=0,\dots,n \\ \gcd(x_0,\dots,x_n)=1 \\ x_0 \text{ is a square}}}\right\}.\end{aligned}$$

Since the theorem gives us in this case that

$$S(q^N,(1,\dots,1)) = X^{\langle \boldsymbol{a},\boldsymbol{\beta}\rangle}(Q_{\boldsymbol{\beta}}(\log(q^N))+\mathcal{O}(q^{-\theta N}).$$

Therefore we have

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1}\,\middle|\,\substack{|x_i|\le q^N,\text{ for all }i=0,\dots,n\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ is a square}}\right\}=X^{\langle \boldsymbol{a},\boldsymbol{\beta}\rangle}(Q_{\boldsymbol{\beta}}(\log(q^N))+\mathcal{O}(q^{-\theta N}).$$

If we now look at the degree of the polynomial $Q_{\boldsymbol{\beta}}$, then by the theorem we know that this is at most $n+1-\operatorname{rank}\{s_i\}_{i=0}^{n+1}$. If we look at $\operatorname{rank}\{s_i\}_{i=0}^{n}$, then we can easily see that $\operatorname{rank}\{s_)\}_{i=0}^{n}=n+1$. This means that the degree of the polynomial $Q_{\boldsymbol{\beta}}$ is at most zero. Hence the polynomial equals a constant $V\in\mathbb{R}$. Lastly we will compute the inner product $\langle \boldsymbol{a},\boldsymbol{\beta}\rangle$. Then we get

$$\begin{aligned}\langle \boldsymbol{a},\boldsymbol{\beta}\rangle &= \langle(1/2,1,\dots,1),(1,1,\dots,1)\rangle\\ &=(1/2+1+\dots+1)\\ &=1/2+n.\end{aligned}$$

So we can now conclude that there exist a constant $\theta>0$ and a constant $V\in\mathbb{R}$ such that,

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1}\,\middle|\,\substack{|x_i|\le q^N,\text{ for all }i=0,\dots,n\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ is a square}}\right\}=q^{N(1/2+n)}(V+\mathcal{O}(q^{-\theta N})),$$

which completes our heuristic. ☐

This conjecture actually states another result as well. If we use $X=q^{N-1}$ instead of $X=q^N$, we get that

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1}\,\middle|\,\substack{|x_i|\le q^{N-1},\text{ for all }i=0,\dots,n\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ is a square}}\right\}=q^{(N-1)(1/2+n)}(V+\mathcal{O}(q^{-\theta(N-1)})).$$

Now we can use these results to determine the size of the set

$$\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)=q^N,x_0\text{ is a square}\right\}.$$

Conjecture 7.8. *There exists a constant $V\in\mathbb{R}$ such that,*

$$\#\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)=q^N,x_0\text{ is a square}\right\}=\frac{V}{q-1}q^{N(1/2+n)}+\mathcal{O}(q^{(N-1)(1/2+n)})$$

Heuristic Proof. For convenience we note

$$I:=\#\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)=q^N,x_0\text{ is a square}\right\}$$

Then we notice that

$$\begin{aligned}I=\#&\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)\le q^N,x_0\text{ is a square}\right\}-\\ &\#\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)\le q^{N-1},x_0\text{ is a square}\right\}.\end{aligned}$$

Then we have that

$$\begin{aligned}&\#\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)\le q^N,x_0\text{ is a square}\right\}=\\ &\qquad\frac{1}{q-1}\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1}\,\middle|\,\substack{|x_i|\le q^N,\text{ for all }i=0,\dots,n\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ is a square}}\right\}.\end{aligned}$$

By Conjecture 7.7 we have that there exists constant $\theta>0$ and a constant $V\in\mathbb{R}$ such that

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{F}_q[T]^{n+1}\,\middle|\,\substack{|x_i|\le q^N,\text{ for all }i=0,\dots,n\\ \gcd(x_0,\dots,x_n)=1\\ x_0\text{ is a square}}\right\}=q^{N(1/2+n)}(V+\mathcal{O}(q^{-\theta N})).$$

Furthermore we find that

$$\begin{aligned}&\#\left\{x=[x_0:\dots:x_n]\in\mathbb{P}^n(\mathbb{F}_q(T))\,|\,H_n(x)=q^{N-1},x_0\text{ is a square}\right\}=\\ &\qquad\frac{1}{q-1}\cdot q^{(N-1)(1/2+n)}(V+\mathcal{O}(q^{-\theta(N-1)}))\end{aligned}$$

Combing this we get that

$$I = \frac{1}{q-1}(q^{N(1/2+n)}(V + \mathcal{O}(q^{-\theta N})) - q^{(N-1)(1/2+n)}(V + \mathcal{O}(q^{-\theta(N-1)}))).$$

Since we want to write this with only one big $\mathcal{O}$-term, we will look at which term is the smaller of the two. Firstly we obtain

$$q^{N(1/2+n)}\mathcal{O}(q^{-\theta N}) = \mathcal{O}(q^{N(1/2+n)-\theta N}),$$

and

$$q^{(N-1)(1/2+n)}\mathcal{O}(q^{-\theta(N-1)})) = \mathcal{O}(q^{N(1/2+n)-1/2-n-\theta N+\theta}).$$

To see which of these powers of q is smaller, we need to determine if $\theta - 1/2 - n > 0$ or $\theta - 1/2 - n < 0$. If we look at the proof of Theorem 5.4, precisely at [3, Page 268], then we can see that $\theta < \delta_1 + \delta_1\delta_2$, which is sufficiently small. Furthermore we see that $q^{N(1/2+n)} \geq q^{(N-1)(1/2+n)}$, so we get that

$$I = \frac{1}{q-1}(q^{N(1/2+n)}(V + \mathcal{O}(q^{-\theta N})) + \mathcal{O}(q^{(N-1)(1/2+n)})).$$

Since $\theta > 0$, we get

$$I = \frac{1}{q-1}(q^{N(1/2+n)}V + \mathcal{O}(q^{(N-1)(1/2+n)})).$$

Finally we can conclude that

$$\#\left\{x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_q(T)) \mid H_n(x) = q^N, x_0 \text{ is a square}\right\} = \frac{V}{q-1}q^{N(1/2+n)} + \mathcal{O}(q^{(N-1)(1/2+n)})$$

This completes our heuristic. □

Further research

The study of counting points of bounded height, doesn't stop at our three main results. One next question is to determine the size of the set

$$\{x = [x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{F}_q(T)) \,|\, x_i \text{ is a } l_i\text{-th power, for all } 0 \leq i \leq n\},$$

where the $l_i \in \mathbb{Z}_{>0}$, are arbitrary chosen. Here we expect that the the size of this set is of the form

$$Cq^{N(l_0^{-1}+l_1^{-1}+\cdots+l_n^{-1})} + \mathcal{O}(g(N)),$$

where $C \in \mathbb{R}$ is a constant, and $g(N)$ is a function which needs to be determined. This result may be solved using the same methods discussed in section 6.3. This conjecture agrees with our results. If we take $l_i = l$ for all $0 \leq i \leq n$, then we get that

$$Cq^{N(n+1)/l} + \mathcal{O}(g(N)),$$

which is the case in theorem 6.4. If we take $l_0 = 2$, and $l_1 = l_2 = \cdots = l_n = 1$, then we arrive at the case of Theorem 7.8.

One may also require other properties for the points in $\mathbb{P}^n(\mathbb{F}_q(T))$ to satisfy. One can look at the property that every coordinate x_i is m-full, which means that if a prime p divides x_i then p^m divides x_i for every $0 \leq i \leq n$. Furthermore we can study the size of sets, consisting of points of bounded height, for far more arithmetic properties.

One other type of study may be about points of bounded height over finite extensions of $\mathbb{F}_q(T)$. In section 4.3 we have seen that these finite extensions satisfy the product formula. Therefore one may define a height function over $\mathbb{P}^n(k)$, where k is such a finite extension. Then one may determine the size of the set

$$\{x \in \mathbb{P}^n(k) \,|\, H(x) \leq B\},$$

where $B \in \mathbb{R}_{>0}$. One may also ask the question what will happen if we require that the points in $\mathbb{P}^n(k)$ satisfy certain arithmetic properties.

References

[1] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] D. S. Carter. L'hospital's rule for complex-valued functions. *The American Mathematical Monthly*, 65(4):264–266, 1958.

[3] Régis de la Bretèche. Estimation de sommes multiples de fonctions arithmétiques. *Compositio Math.*, 128(3):261–298, 2001.

[4] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[5] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[6] Chao Hua Jia. The distribution of square-free numbers. *Sci. China Ser. A*, 36(2):154–169, 1993.

[7] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[8] Serge Lang. *Complex analysis*, volume 103 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1999.

[9] Adelina Manzateanu. *Rational points in function fields*. PhD thesis, University of Bristol, 2019.

[10] Ben Riffer-Reinert. The zeta function and its relation to the prime number theorem. https://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Riffer-Reinert.pdf, 2011. [Online; accessed 9-October-2024].

[11] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[12] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.

[13] William F. Trench. Conditional convergence of infinite products. *Amer. Math. Monthly*, 106(7):646–651, 1999.