





## A note on points on algebraic sets

Şermin Çam Çelik<sup>\*1</sup> , Haydar Göral<sup>2</sup> 

<sup>1</sup>*Department of Mathematics, Faculty of Engineering and Natural Sciences, Istanbul Bilgi University, Istanbul, Turkey*

<sup>2</sup>*Department of Mathematics, Izmir Institute of Technology, 35430 Urla, Izmir, Turkey*

### Abstract

In this short note, we count the points on algebraic sets which lie in a subset of a domain. It is proved that the set of points on algebraic sets coming from certain subsets of a domain has the full asymptotic. This generalizes the first theorem of [E. Alkan and E.S. Yörük, Statistics and characterization of matrices by determinant and trace, Ramanujan J., 2019] and also answers some questions from the same article.

**Mathematics Subject Classification (2020).** 13G05, 12E05, 11C08

**Keywords.** algebraic sets, heights, asymptotics

### 1. Introduction

Our goal in this short note is to generalize the first theorem of [1]. We also shed light on some questions asked in the same article. More precisely, it is proved in [1, Theorem 1] that asymptotically, almost all  $n \times n$  square matrices with prime number entries are invertible. Using elementary methods, we extend this result by counting points on algebraic sets which come from certain subsets of a domain.

Let

$$f(X) = a_d(X - \alpha_1) \cdots (X - \alpha_d)$$

be a non-zero polynomial in  $\mathbb{C}[X]$ . The *Mahler measure* of  $f(X)$  is defined by

$$m(f) = |a_d| \prod_{|\alpha_j| \geq 1} |\alpha_j|.$$

We define the Mahler measure of zero to be 1. *Lehmer's conjecture* states that there exists an absolute constant  $c > 1$  such that for any  $f(X) \in \mathbb{Z}[X]$ , if  $m(f) > 1$ , then  $m(f) \geq c$ . Lehmer [3] asked this question around 1933 and it is still open. In fact, Lehmer also conjectured that the polynomial

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$$

has the smallest Mahler measure among polynomials in  $\mathbb{Z}[X]$  whose Mahler measures are not 1, and this is also open.

\*Corresponding Author.

Email addresses: sermincamcelik@gmail.com (Ş. Çam Çelik), hgoral@gmail.com (H. Göral)

Received: 28.05.2020; Accepted: 13.01.2021

Let  $\overline{\mathbb{Q}}$  be the field of algebraic numbers and  $\alpha$  be in  $\overline{\mathbb{Q}}$  with irreducible polynomial  $f(X) \in \mathbb{Z}[X]$ . We define the *height* of  $\alpha$  as

$$H(\alpha) = m(f)^{1/d}$$

where  $d = \deg f$ . For a non-zero rational number  $a/b$  where  $a$  and  $b$  are coprime integers, observe that

$$H(a/b) = \max\{|a|, |b|\}$$

and  $H(0) = 1$ . Northcott’s theorem (see [2, Theorem 1.6.8]) states that there are only finitely many algebraic numbers of bounded degree and bounded height. In other words, for any real numbers  $x$  and  $y$ , the set

$$\{\alpha \in \overline{\mathbb{Q}} : \deg(\alpha) \leq x, H(\alpha) \leq y\}$$

is finite. A subset  $B$  of  $\overline{\mathbb{Q}}$  has the *Northcott property* if for every real number  $x$ , the set

$$\{\alpha \in B : H(\alpha) \leq x\}$$

is finite. For example, any number field  $K$  has the Northcott property. Another example is that for any  $m \geq 2$ , the field  $L_m = \mathbb{Q}(\sqrt[m]{1}, \sqrt[m]{2}, \sqrt[m]{3}, \dots)$  has the Northcott property, see [2, Corollary 4.5.6].

Before stating our main result, we need one more definition. Let  $D$  be an integral domain and  $\gamma : D \rightarrow [0, \infty)$  be any function. We say that a subset  $B$  of  $D$  has the  *$\gamma$ -Northcott property* if

$$B_\gamma(x) = |\{b \in B : \gamma(b) \leq x\}|$$

is finite for every real number  $x$ . In this note, we prove the following result:

**Theorem 1.1.** *Let  $D$  be an integral domain and  $\gamma : D \rightarrow [0, \infty)$  be a function. Let  $B$  be a subset of  $D$  which has the  $\gamma$ -Northcott property and let  $x$  be a positive real number. Let  $f(X_1, \dots, X_k) \in D[X_1, \dots, X_k]$  be a non-zero polynomial with total degree  $\deg(f)$ . Then,*

$$\begin{aligned} &|\{(b_1, \dots, b_k) \in B^k : \gamma(b_i) \leq x \text{ for all } i = 1, \dots, k \text{ and } f(b_1, \dots, b_k) = 0\}| \\ &\leq \deg(f) \cdot B_\gamma(x)^{k-1}. \end{aligned} \tag{1.1}$$

Hence,

$$\begin{aligned} &|\{(b_1, \dots, b_k) \in B^k : \gamma(b_i) \leq x \text{ for all } i = 1, \dots, k \text{ and } f(b_1, \dots, b_k) \neq 0\}| \\ &= B_\gamma(x)^k + O_f(B_\gamma(x)^{k-1}). \end{aligned} \tag{1.2}$$

If moreover,  $\lim_{x \rightarrow \infty} B_\gamma(x) = \infty$ , then

$$|\{(b_1, \dots, b_k) \in B^k : \gamma(b_i) \leq x \text{ for all } i = 1, \dots, k \text{ and } f(b_1, \dots, b_k) \neq 0\}| \sim B_\gamma(x)^k \tag{1.3}$$

as  $x$  tends to infinity.

Some remarks are in order. In [1, Theorem 1], it is shown that asymptotically, almost all square matrices of size  $n$  with prime number entries are non-singular. This means that if  $M_n(x)$  is the number of non-singular square matrices of size  $n$  with prime number entries which are in  $[0, x]$  and  $\pi(x)$  denotes the number of prime numbers in  $[0, x]$ , then

$$\lim_{x \rightarrow \infty} \frac{M_n(x)}{\pi(x)^{n^2}} = 1.$$

Note that the determinant in the ring of  $n \times n$  matrices is a polynomial of degree  $n$  with  $n^2$  variables. As mentioned in the introduction, for any prime number  $p$ , we have that  $H(p) = p$  and so the set of prime numbers  $\mathbb{P}$  has the  $\gamma$ -Northcott property when  $\gamma = H$  and  $D = \overline{\mathbb{Q}}$ . Therefore, our main result generalizes the corresponding theorem of [1]. The proof in [1] is using the prime number theorem for arithmetic progressions. However, our

proof is on the elementary side, it is effective as we have an error term, and more general. For instance, our result implies that

$$M_n(x) = \pi(x)^{n^2} + R_n(x)$$

where

$$|R_n(x)| \leq n \cdot \pi(x)^{n^2-1}.$$

We also answer a question from [1], as our theorem indicates that one can take any infinite subset of positive integers in [1, Theorem 1] instead of subsets of primes or thin subsets of positive integers. In fact, one can choose any subset of  $D = \overline{\mathbb{Q}}$  which has the Northcott property.

## 2. Proof of Theorem 1.1

To prove that Inequality (1.1) holds, we will proceed by induction on the number of variables  $k$  of the non-zero polynomial  $f$ .

For  $k = 1$ , since  $D$  is an integral domain, the polynomial  $f(X_1) \in D[X_1]$  has at most  $\deg(f)$  many roots in  $D$ . So,

$$|\{b \in B : \gamma(b) \leq x, f(b) = 0\}| \leq \deg(f)$$

as desired.

For the inductive step, assume that Inequality (1.1) holds for all polynomials whose number of variables is less than  $k$  and consider the non-zero polynomial  $f(X_1, \dots, X_k)$  with  $k$  variables. Set

$$\mathcal{B} = \{(b_1, \dots, b_k) \in B^k : \gamma(b_i) \leq x \text{ for all } i = 1, \dots, k \text{ and } f(b_1, \dots, b_k) = 0\}$$

and let  $(b_1, \dots, b_k) \in \mathcal{B}$ .

If none of the distinct monomials of  $f$  contains  $X_1$  as a factor, then  $f(X_1, \dots, X_k) = g(X_2, \dots, X_k)$  for some non-zero polynomial  $g(X_2, \dots, X_k) \in D[X_2, \dots, X_k]$ . So,

$$f(b_1, \dots, b_k) = g(b_2, \dots, b_k) = 0.$$

By induction hypothesis,

$$\begin{aligned} &|\{(b_2, \dots, b_k) \in B^{k-1} : \gamma(b_i) \leq x \text{ for all } i = 2, \dots, k \text{ and } g(b_2, \dots, b_k) = 0\}| \\ &\leq \deg(g) \cdot B_\gamma(x)^{k-2} = \deg(f) \cdot B_\gamma(x)^{k-2}. \end{aligned}$$

So,  $(b_2, \dots, b_k)$  can take at most  $\deg(f) \cdot B_\gamma(x)^{k-2}$  many distinct values. Then, since  $b_1$  can take exactly  $B_\gamma(x)$  many distinct values, we get

$$|\mathcal{B}| \leq \deg(f) \cdot B_\gamma(x)^{k-1}$$

and we are done.

If at least one of the distinct monomials of  $f$  contains  $X_1$  as a factor, then we can uniquely write  $f(X_1, \dots, X_k)$  as

$$f(X_1, \dots, X_k) = \sum_{i=0}^d (X_1)^i f_i(X_2, \dots, X_k)$$

for some positive integer  $d$  and some polynomials  $f_0, \dots, f_d \in D[X_2, \dots, X_k]$  with  $f_d \neq 0$ . Then,

$$f(b_1, \dots, b_k) = \sum_{i=0}^d (b_1)^i f_i(b_2, \dots, b_k) = 0.$$

So, if  $f_i(b_2, \dots, b_k) \neq 0$  for some  $i = 0, \dots, d$ , then  $b_1$  is a root of the non-zero polynomial

$$\sum_{i=0}^d f_i(b_2, \dots, b_k)(X_1)^i \in D[X_1]$$

whose degree is at most  $d$ . Thus,  $b_1$  can take at most  $d$  many distinct values in  $D$ . Hence,

$$|\{(b_1, \dots, b_k) \in \mathcal{B} : f_i(b_2, \dots, b_k) \neq 0 \text{ for some } i = 0, \dots, d\}| \leq d \cdot B_\gamma(x)^{k-1}. \quad (2.1)$$

On the other hand, if  $f_i(b_2, \dots, b_k) = 0$  for all  $i = 0, \dots, d$ , then in particular we have  $f_d(b_2, \dots, b_k) = 0$ . However, since  $f_d \neq 0$ , by the induction assumption,

$$\begin{aligned} & |\{(b_2, \dots, b_k) \in B^{k-1} : \gamma(b_i) \leq x \text{ for all } i = 2, \dots, k \text{ and } f_d(b_2, \dots, b_k) = 0\}| \\ & \leq \deg(f_d) \cdot B_\gamma(x)^{k-2}. \end{aligned}$$

Then, since  $b_1$  can take  $B_\gamma(x)$  many distinct values,

$$\begin{aligned} & |\{(b_1, \dots, b_k) \in \mathcal{B} : f_i(b_2, \dots, b_k) = 0 \text{ for all } i = 0, \dots, d\}| \\ & \leq |\{(b_1, \dots, b_k) \in \mathcal{B} : f_d(b_2, \dots, b_k) = 0\}| \\ & \leq \deg(f_d) \cdot B_\gamma(x)^{k-1}. \end{aligned} \quad (2.2)$$

Thus, combining (2.1) and (2.2), we get

$$|\mathcal{B}| \leq (d + \deg(f_d)) \cdot B_\gamma(x)^{k-1} \leq \deg(f) \cdot B_\gamma(x)^{k-1}$$

as desired.

### References

- [1] E. Alkan and E.S. Yörük, *Statistics and characterization of matrices by determinant and trace*, Ramanujan J. **48**, 131–149, 2019.
- [2] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press; 1st edition, 2007.
- [3] D.H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2), **34**, 461–479, 1933.