Multiplicatively dependent vectors of algebraic numbers

C.L. Stewart
cstewart@uwaterloo.ca

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

Online number theory seminar, Debrecen, Hungary, January 21, 2022

Let n be a positive integer, G be a multiplicative group and let $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n)$ be in G^n. We say that $\boldsymbol{\nu}$ is multiplicatively dependent if there is a non-zero vector $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ for which

$$\boldsymbol{\nu}^{\mathbf{k}} = \nu_1^{k_1} \cdots \nu_n^{k_n} = 1. \tag{0.1}$$

We denote by $M_n(G)$ the set of multiplicatively dependent vectors in G^n.

For instance, the set $M_n(\mathbb{C}^*)$ of multiplicatively dependent vectors in $(\mathbb{C}^*)^n$ is of Lebesgue measure zero, since it is a countable union of sets of measure zero. Further, if we fix an exponent vector $\mathbf{k}$ the subvariety of $(\mathbb{C}^*)^n$ determined by (0.1) is an algebraic subgroup of $(\mathbb{C}^*)^n$.

We shall be interested in counting the number of multiplicatively dependent n-tuples whose coordinates are algebraic numbers of fixed degree, or within a fixed number field, and bounded height.

Equivalently we shall count n-tuples of algebraic numbers in a fixed algebraic number field, or of fixed degree, and given height which occur in some proper algebraic subgroup of the algebraic group G_m^n, where G_m is the multiplicative group of an algebraic closure of $\mathbb{Q}$.

For any algebraic number α, let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

be the minimal polynomial of α over the integers $\mathbb{Z}$ (so with content 1 and positive leading coefficient). Suppose that f factors as

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

over the complex numbers $\mathbb{C}$. The *naive height* $H_0(\alpha)$ of α is given by

$$H_0(\alpha) = \max\{|a_d|, \ldots, |a_1|, |a_0|\},$$

and $H(\alpha)$, the height of α, also known as the *absolute Weil height* of α, is defined by

$$H(\alpha) = (a_d \prod_{i=1}^{d} \max\{1, |\alpha_i|\})^{1/d}.$$

Let K be a number field of degree d (over $\mathbb{Q}$). We use the following standard notation:

- r_1 and r_2 for the number of real and pairs of complex conjugate embeddings of K, respectively, and put $r = r_1 + r_2 - 1$;
- D, h, R and ζ_K for the discriminant, class number, regulator and Dedekind zeta function of K, respectively;
- w for the number of roots of unity in K.

Note that r is exactly the rank of the unit group of the ring of algebraic integers of K. As usual, let $\zeta(s)$ be the Riemann zeta function.

For any real number x, let $\lceil x \rceil$ denote the smallest integer greater than or equal to x, and let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x.

For a finite set S we use $|S|$ to denote its cardinality.

Let K be a number field of degree d. Denote the set of algebraic integers of K of height at most H by $\mathcal{B}_K(H)$ and the set of algebraic numbers of K of height at most H by $\mathcal{B}_K^*(H)$. Set

$$B_K(H) = |\mathcal{B}_K(H)|; B_K^*(H) = |\mathcal{B}_K^*(H)|.$$

Put

$$C_1(K) = \frac{2^{r_1}(2\pi)^{r_2} d^r}{|D|^{1/2} r!}.$$

Widmer(2016) proved that

$$B_K(H) = C_1(K) H^d (\log H)^r + O(H^d (\log H)^{r-1}). \qquad (0.2)$$

For any positive integer n, we denote by $L_{n,K}(H)$ the number of multiplicatively dependent n-tuples whose coordinates are algebraic integers of height at most H, and we denote by $L^*_{n,K}(H)$ the number of multiplicatively dependent n-tuples whose coordinates are algebraic numbers of height at most H.

Put

$$C_3(n, K) = \frac{n(n+1)}{2} w C_1(K)^{n-1}.$$

Theorem (Pappalardi, Sha, Shparlinski, S., 2018)

Let K be a number field of degree d over $\mathbb{Q}$ and let n be an integer with $n \geq 2$. We have

$$\begin{aligned} L_{n,K}(H) = C_3(n,K)H^{d(n-1)}(\log H)^{r(n-1)} \\ + O\left(H^{d(n-1)}(\log H)^{r(n-1)-1}\right); \end{aligned} \tag{0.3}$$

if furthermore $K = \mathbb{Q}$ or is an imaginary quadratic field, we have

$$L_{n,K}(H) = C_3(n,K)H^{d(n-1)} + O\left(H^{d(n-3/2)}\right). \tag{0.4}$$

Define

$$C_2(K) = \frac{2^{2r_1}(2\pi)^{2r_2}2^r hR}{|D|w\zeta_K(2)}.$$

Schanuel proved in 1979 that

$$B_K^*(H) = C_2(K)H^{2d} + O(H^{2d-1}(\log H)^{\sigma(d)}), \qquad (0.5)$$

where $\sigma(1) = 1$ and $\sigma(d) = 0$ for $d > 1$.

We estimate $L^*_{n,K}(H)$ next. Put

$$C_4(n,K) = n^2 w C_2(K)^{n-1}.$$

Theorem (Pappalardi, Sha, Shparlinski, S., 2018)

Let K be a number field of degree d, and let n be an integer with $n \geq 2$. Then, we have

$$L^*_{n,K}(H) = C_4(n,K)H^{2d(n-1)} + O(H^{2d(n-1)-1}g(H)), \tag{0.6}$$

where

$$g(H) = \begin{cases} \log H & \text{if } d = 1 \text{ and } n = 2 \\ \exp(c \log H/ \log\log H) & \text{if } d = 1 \text{ and } n > 2 \\ 1 & \text{if } d > 1 \text{ and } n \geq 2, \end{cases}$$

and c is a positive number depending only on n.

The following notion plays a crucial role in our argument. Let $\overline{\mathbb{Q}}$ be an algebraic closure of the rational numbers $\mathbb{Q}$. For each $\boldsymbol{\nu}$ in $(\overline{\mathbb{Q}}^*)^n$, we define s, the *multiplicative rank* of $\boldsymbol{\nu}$, in the following way. If $\boldsymbol{\nu}$ has a coordinate which is a root of unity, we put $s = 0$; otherwise let s be the largest integer with $1 \leq s \leq n$ for which any s coordinates of $\boldsymbol{\nu}$ form a multiplicatively independent vector. Notice that

$$0 \leq s \leq n - 1, \tag{0.7}$$

whenever $\boldsymbol{\nu}$ is multiplicatively dependent.

We now outline the strategy of the proofs. Given a number field K, we define $L_{n,K,s}(H)$ and $L^*_{n,K,s}(H)$ to be the number of multiplicatively dependent n-tuples of multiplicative rank s whose coordinates are algebraic integers in $\mathcal{B}_K(H)$ and algebraic numbers in $\mathcal{B}^*_K(H)$ respectively. It follows from (0.7) that

$$\begin{cases} L_{n,K}(H) = L_{n,K,0}(H) + \cdots + L_{n,K,n-1}(H) \\ L^*_{n,K}(H) = L^*_{n,K,0}(H) + \cdots + L^*_{n,K,n-1}(H). \end{cases} \tag{0.8}$$

The main term in (0.3) comes from the contributions of $L_{n,K,0}(H)$ and $L_{n,K,1}(H)$ in (0.8), and the main term in our second theorem comes from the contributions of $L^*_{n,K,0}(H)$ and $L^*_{n,K,1}(H)$ in (0.8). To prove our results we make use of (0.8) and the following result.

Theorem (Pappalardi, Sha, Shparlinski, S., 2018)

Let K be a number field of degree d. Let n and s be integers with $n \geq 2$ and $0 \leq s \leq n-1$. Then, there exist positive numbers c_1 and c_2 which depend on n and K, such that

$$L_{n,K,s}(H) < H^{d(n-1)-d(\lceil (s+1)/2 \rceil -1)} \exp(c_1 \log H / \log\log H) \quad (0.9)$$

and

$$L^*_{n,K,s}(H) < H^{2d(n-1)-d(\lceil (s+1)/2 \rceil -1)} \exp(c_2 \log H / \log\log H). \quad (0.10)$$

The next result shows that if algebraic numbers $\alpha_1, \ldots, \alpha_n$ are multiplicatively dependent, then we can find a relation where the exponents are not too large. Such a result has found application in transcendence theory.

Lemma

Let $n \geq 2$, and let $\alpha_1, \ldots, \alpha_n$ be multiplicatively dependent non-zero algebraic numbers of degree at most d and height at most H. Then, there is a positive number c, which depends only on n and d, and there are rational integers $k_1, \ldots, k_n$, not all zero, such that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1$$

and

$$\max_{1 \leq i \leq n} |k_i| < c(\log H)^{n-1}.$$

This follows from a result of van der Poorten and Loxton.

Let x and y be positive real numbers with y larger than 2, and let $\psi(x, y)$ denote the number of positive integers not exceeding x which contain no prime factors greater than y. Put

$$Z = \left(\log\left(1 + \frac{y}{\log x}\right)\right)\frac{\log x}{\log y} + \left(\log\left(1 + \frac{\log x}{y}\right)\right)\frac{y}{\log y}$$

and

$$u = (\log x)/(\log y).$$

Lemma

For $2 < y \leq x$, *we have*

$$\psi(x, y) = \exp\left(Z\left(1 + O((\log y)^{-1}) + O((\log\log x)^{-1}) + O((u+1)^{-1})\right)\right).$$

This is a result of N.G. de Bruijn from 1966.

Let d be a positive integer, and let $\mathcal{A}_d(H)$, respectively $\mathcal{A}_d^*(H)$, be the set of algebraic integers of degree d (over $\mathbb{Q}$), respectively algebraic numbers of degree d, of height at most H. We set

$$A_d(H) = |\mathcal{A}_d(H)|; A_d^*(H) = |\mathcal{A}_d^*(H)|.$$

Put

$$C_5(d) = d2^d \prod_{j=1}^{\lfloor (d-1)/2 \rfloor} \frac{d(2j)^{d-2j-1}}{(2j+1)^{d-2j}}$$

and

$$C_6(d) = \frac{d2^d}{\zeta(d+1)} \prod_{j=1}^{\lfloor (d-1)/2 \rfloor} \frac{(d+1)(2j)^{d-2j}}{(2j+1)^{d-2j+1}}.$$

It follows from the work of Barroero from 2014 that

$$A_d(H) = C_5(d)H^{d^2} + O\left(H^{d(d-1)}(\log H)^{\rho(d)}\right), \qquad (0.11)$$

where $\rho(2) = 1$ and $\rho(d) = 0$ for any $d \neq 2$.

Masser and Vaaler showed in 2008 that

$$A_d^*(H) = C_6(d)H^{d(d+1)} + O\left(H^{d^2}(\log H)^{\vartheta(d)}\right), \qquad (0.12)$$

where $\vartheta(1) = \vartheta(2) = 1$ and $\vartheta(d) = 0$ for any $d \geq 3$.

For any positive integer n, we denote by $M_{n,d}(H)$ the number of multiplicatively dependent n-tuples whose coordinates are algebraic integers in $\mathcal{A}_d(H)$, and we denote by $M^*_{n,d}(H)$ the number of multiplicatively dependent n-tuples whose coordinates are algebraic numbers in $\mathcal{A}^*_d(H)$.

For each positive integer d, we define $w_0(d)$ to be the number of roots of unity of degree d. Let φ denote Euler's totient function. Since $\varphi(k) \gg k/\log\log k$ for any integer $k \geq 3$, it follows that

$$w_0(d) \ll d^2 \log\log d, \qquad (0.13)$$

where $d \geq 3$ and the implied constant is absolute. We remark that $w_0(d)$ can be zero, such as for an odd integer $d > 1$.

Given positive integers n and d, we define $C_7(n, d)$ and $C_8(n, d)$ as

$$C_7(n, d) = (nw_0(d) + n(n-1))\, C_5(d)^{n-1}$$

and

$$C_8(n, d) = (nw_0(d) + 2n(n-1))\, C_6(d)^{n-1}.$$

THEOREM (PAPPALARDI, SHA, SHPARLINSKI, S., 2018)

Let d and n be positive integers with $n \geq 2$. Then, the following hold.

(I) *We have*

$$M_{n,d}(H) = C_7(n,d)H^{d^2(n-1)} + O\left(H^{d^2(n-1)-d/2}\right); \quad (0.14)$$

furthermore if $d = 2$ or d is odd, we have

$$M_{n,d}(H) = C_7(n,d)H^{d^2(n-1)} + O\left(H^{d^2(n-1)-d}\exp(c_0 \log H / \log\log H)\right) \quad (0.15)$$

Theorem (Pappalardi, Sha, Shparlinski, S., 2018)

Let d and n be positive integers with $n \geq 2$. Then, the following hold.

(ii) *We have*

$$M^*_{n,d}(H) = C_8(n,d)H^{d(d+1)(n-1)} + O\left(H^{d(d+1)(n-1)-d/2}\log H\right); \qquad (0.16)$$

furthermore if $d = 2$ or d is odd, we have

$$M^*_{n,d}(H) = C_8(n,d)H^{d(d+1)(n-1)} + O\left(H^{d(d+1)(n-1)-d}\exp(c\log H/\log\log H)\right) \qquad (0.17)$$

and where c is a positive number which depends only on n and d.

How are multiplicatively dependent vectors distributed?
What is the distribution of the elements of $\mathcal{M}_n(S)$ when S is a subset of the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$ with number theoretic interest?

Let K be a number field, which we always identify with one of its models, that is, $K = \mathbb{Q}(\alpha)$ for some algebraic number α. Let $\mathcal{O}_K$ denote the ring of integers of K. We study the distribution of $\mathcal{M}_n(K)$ and $\mathcal{M}_n(\mathcal{O}_K)$ in $\mathbb{R}^n$ and also in $\mathbb{C}^n$.

We say that a subset S of a ring R is *closed under powering* if for any α in S we also have α^m in S for every non-zero integer m.

THEOREM (KONYAGIN, SHA, SHPARLINSKI, S., 2021)

Let $n \geq 2$ and let S be a dense subset of $\mathbb{R}$ which is closed under powering. Then $\mathcal{M}_n(S)$ is dense in $\mathbb{R}^n$.

Since the rationals are dense in $\mathbb{R}$ and closed under powering, we deduce the following result.

COROLLARY (KONYAGIN, SHA, SHPARLINSKI, S., 2021)

Let $n \geq 2$. Then $\mathcal{M}_n(\mathbb{Q})$ is dense in $\mathbb{R}^n$.

If $\mathcal{O}_K \cap \mathbb{R} \neq \mathbb{Z}$, then $\mathcal{O}_K \cap \mathbb{R}$ is easily seen to be dense in $\mathbb{R}$, and since it is closed under powering we have the following result.

Corollary (Konyagin, Sha, Shparlinski, S., 2021)

Let $n \geq 2$, and let K be a number field. If $\mathcal{O}_K \cap \mathbb{R} \neq \mathbb{Z}$, then $\mathcal{M}_n(\mathcal{O}_K \cap \mathbb{R})$ is dense in $\mathbb{R}^n$.

We next consider the situation when $\mathbb{R}$ is replaced by $\mathbb{C}$.

THEOREM (KONYAGIN, SHA, SHPARLINSKI, S., 2021)

Let $n \geq 2$ and let S be a dense subset of $\mathbb{C}$ which is closed under powering. Then $\mathcal{M}_n(S)$ is dense in $\mathbb{C}^n$.

The condition that S be closed under powering can not be removed from the previous two theorems. For example, let S be the set of all algebraic numbers of the form $\zeta p/q$ with ζ a root of unity and with p and q distinct primes. Then S is dense in $\mathbb{C}$, but $\mathcal{M}_n(S)$ is not dense in $\mathbb{C}^n$ for any $n \geq 2$.

Corollary (Konyagin, Sha, Shparlinski, S., 2021)

Let $n \geq 2$, and let K be a number field. If K is not contained in $\mathbb{R}$, then $\mathcal{M}_n(K)$ is dense in $\mathbb{C}^n$.

Further if K is a number field of degree at least 3 which is not contained in $\mathbb{R}$, then $\mathcal{O}_K$ is dense in $\mathbb{C}$ and we have the following result.

Corollary (Konyagin, Sha, Shparlinski, S., 2021)

Let $n \geq 2$, and let K be a number field. If $[K : \mathbb{Q}] \geq 3$ and K is not contained in $\mathbb{R}$, then $\mathcal{M}_n(\mathcal{O}_K)$ is dense in $\mathbb{C}^n$.

To study the cases of $\mathcal{M}_n(\mathbb{Z})$, which is not dense in $\mathbb{R}^n$, and of $\mathcal{M}_n(\mathcal{O}_K)$ when K is an imaginary quadratic field, which is not dense in $\mathbb{C}^n$, we introduce a refinement of the notion of the covering radius of a set .

$\|\mathbf{x}\|$ denotes the Euclidean norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, that is,

$$\|\mathbf{x}\| = \sqrt{x_1^2 + \ldots + x_n^2}.$$

For $H > 1$ we define

$$\rho_n(H; \mathbb{Z}) = \sup_{\substack{\mathbf{x} \in \mathbb{R}^n \\ \|\mathbf{x}\| \leq H}} \inf_{\mathbf{v} \in \mathcal{M}_n(\mathbb{Z})} \|\mathbf{x} - \mathbf{v}\|.$$

We must have

$$\rho_n(H; \mathbb{Z}) \geq c_1(n)H^{1/n}. \qquad (0.18)$$

If the points of $\mathcal{M}_n(\mathbb{Z})$ were evenly distributed, then the lower bound above would be sharp.

THEOREM (KONYAGIN, SHA, SHPARLINSKI, S., 2021)

For $H > 1$, we have

$$H \ll \rho_2(H;\mathbb{Z}) \ll H,$$

and for $n \geq 3$

$$H/(\log H)^{C_0(n)} \ll \rho_n(H;\mathbb{Z}) \ll H\frac{(\log\log H)^{n-1}}{(\log H)^{n-2}},$$

where $C_0(n)$ is a positive number which is effectively computable in terms of n.

For $H > 1$ and K an imaginary quadratic field, we put

$$\mu_n(H; \mathcal{O}_K) = \sup_{\substack{\mathbf{x} \in \mathbb{C}^n \\ \|\mathbf{x}\| \leq H}} \inf_{\mathbf{v} \in \mathcal{M}_n(\mathcal{O}_K)} \|\mathbf{x} - \mathbf{v}\|.$$

Theorem (Konyagin, Sha, Shparlinski, S., 2021)

Let K be an imaginary quadratic field, and let H be a real number with $H > 1$. Then, there exists a number $C_0(n)$, which is effectively computable in terms of n, such that

$$H \ll \mu_2(H; \mathcal{O}_K) \ll H,$$

and for $n \geq 3$,

$$H/(\log H)^{C_0(n)} \ll \mu_n(H; \mathcal{O}_K) \ll H \frac{\log \log H}{(\log H)^{1/2}}.$$

For the proof of the lower bounds in the previous two results we appeal to a result of Tijdeman from 1973 on integers composed of a finite set of primes while for the upper bound we give an explicit construction.

Let S be the set of all rational numbers of the form p/q or $-p/q$ with distinct primes p, q. Then the set S is dense in $\mathbb{R}$ and we now show that $\mathcal{M}_n(S)$ is not dense in $\mathbb{R}^n$ for any $n \geq 2$.

Let $(x_1, \ldots, x_n) \in \mathcal{M}_n(S)$. Then, there are integers $k_1, \ldots, k_n$, not all zero, such that

$$x_1^{k_1} \cdots x_n^{k_n} = 1. \tag{0.19}$$

As a first step we show that there are integers $k_1, \ldots, k_n$, not all zero, of absolute value at most 1 such that

$$|x_1^{k_1} \cdots x_n^{k_n}| = 1.$$

Let $\alpha_1, \ldots, \alpha_n$ be non-zero real numbers and assume that for all n-tuples $(\delta_1, \ldots, \delta_n) \neq (0, \ldots, 0)$ with $\delta_i \in \{-1, 0, 1\}$, $i = 1, \ldots, n$, we have

$$\alpha_1^{\delta_1} \cdots \alpha_n^{\delta_n} \neq \pm 1.$$

For example, we can choose

$$(\alpha_1, \ldots, \alpha_n) = \left(2, 2^3, \ldots, 2^{3^{n-1}}\right). \tag{0.20}$$

Notice that there is a positive number c such that

$$\left|\alpha_1^{\delta_1}\cdots\alpha_n^{\delta_n}-1\right|>c \qquad \text{and} \qquad \left|\alpha_1^{\delta_1}\cdots\alpha_n^{\delta_n}+1\right|>c \quad (0.21)$$

for any non-zero n-tuple $(\delta_1,\ldots,\delta_n)$ with $\delta_i\in\{-1,0,1\}$, $i=1,\ldots,n$.

It follows from (0.21) that there is a small ball around $(\alpha_1, \ldots, \alpha_n)$ which does not contain any element of $\mathcal{M}_n(S)$. As a consequence, we see that $\mathcal{M}_n(S)$ is not dense in $\mathbb{R}^n$.

Thank you for your attention.