On the density of rectangular unimodular matrices over the ring of algebraic integers

Violetta Weger

joint work with Giacomo Micheli

University of Zurich

Number theory and coding theory
Contemporary applications in security
May 31, 2018

Density

Definition

The density of a set $S \subset \mathbb{Z}^d$ *is defined to be*

$$\rho(S) = \lim_{B \to \infty} \frac{|S \cap [-B, B[^d|}{(2B)^d}$$

if the limit exists. Then one defines the upper density $\bar{\rho}$ *and the lower density* $\underline{\rho}$ *equivalently with the* $\limsup$ *and the* $\liminf$ *respectively.*

Mertens-Cesáro Theorem

Theorem (Mertens, 1874 and Cesáro, 1883)

The density of the set of coprime pairs of $\mathbb{Z}$ is equal to

$$\frac{1}{\zeta(2)},$$

where ζ denotes the Riemann zeta function.

Mertens-Cesáro Theorem

This can be generalized to

Theorem (Nymann, 1972)

The density of the set of coprime m-tuples of $\mathbb{Z}$ is equal to

$$\frac{1}{\zeta(m)},$$

where ζ denotes the Riemann zeta function.

Mertens-Cesáro Theorem

This can be generalized to

Theorem (Nymann, 1972)

The density of the set of coprime m-tuples of $\mathbb{Z}$ is equal to

$$\frac{1}{\zeta(m)},$$

where ζ denotes the Riemann zeta function.

And this can be further generalized to

Theorem (Ferraguti, Micheli, 2016)

The density of the set of coprime m-tuples of $\mathcal{O}_K$ is equal to

$$\frac{1}{\zeta_K(m)},$$

where ζ_K denotes the Dedekind zeta function over K.

Rectangular Unimodular Matrices

Definition

Let $\mathcal{R}$ be a domain and $n < m \in \mathbb{N}$. Let $M \in \mathrm{Mat}_{n \times m}(\mathcal{R})$. M is said to be rectangular unimodular, if there exist $m - n$ rows in $\mathcal{R}^m$, such that when adjoining these rows to M the resulting $m \times m$ matrix $\widetilde{M}$ is invertible, i.e. $\det(\widetilde{M})$ is a unit in $\mathcal{R}$.

Rectangular Unimodular Matrices

Over Dedekind domains, there are the following characterization of rectangular unimodular matrices:

Proposition (Gustafson, Moore, Reiner, 1981)

Let $\mathcal{D}$ be a Dedekind domain and $n < m \in \mathbb{N}$. Let $M \in \mathrm{Mat}_{n\times m}(\mathcal{D})$. M is rectangular unimodular, if and only if the ideal generated by all the $n \times n$ minors of M is $\mathcal{D}$.

Rectangular Unimodular Matrices

Over Dedekind domains, there are the following characterization of rectangular unimodular matrices:

Proposition (Gustafson, Moore, Reiner, 1981)

Let $\mathcal{D}$ be a Dedekind domain and $n < m \in \mathbb{N}$. Let $M \in \mathrm{Mat}_{n\times m}(\mathcal{D})$. M is rectangular unimodular, if and only if the ideal generated by all the $n \times n$ minors of M is $\mathcal{D}$.

Proposition (Gustafson, Moore, Reiner, 1981)

Let $\mathcal{D}$ be a Dedekind domain and $n < m \in \mathbb{N}$. $M \in \mathrm{Mat}_{n\times m}(\mathcal{D})$ is rectangular unimodular, if and only if $M \mod \mathfrak{p}$ has full rank for any $\mathfrak{p}$ non-zero prime ideal of $\mathcal{D}$.

Main Result

Theorem (Micheli, W., 2018)

Let n and m be positive integers such that $n < m$ and K be an algebraic number field. The density of the set of $n \times m$ rectangular unimodular matrices over $\mathcal{O}_K$ is

$$\prod_{i=0}^{n-1} \frac{1}{\zeta_K(m-i)},$$

where ζ_K denotes the Dedekind zeta function of K.

Local to global principle: Notation

If S is a set, then we denote by 2^S its powerset.
Let $M_{\mathbb{Q}} = \{\infty\} \cup \{p \mid p \text{ prime}\}$ be the set of all places of $\mathbb{Q}$.
We denote by $\mathbb{Z}_p$ the p-adic integers.
Let μ_∞ denote the Lebesgue measure on $\mathbb{R}^d$ and μ_p the normalized Haar measure on $\mathbb{Z}_p^d$.
For T a subset of a metric space, let us denote by ∂T its boundary.

Local to global principle

Theorem (Poonen, Stoll, 1999)

Let $U_\infty \subset \mathbb{R}^d$*, such that* $\mathbb{R}_{\geq 0} \cdot U_\infty = U_\infty$ *and* $\mu_\infty(\partial(U_\infty)) = 0$*.*
Let $s_\infty = \frac{1}{2^d}\mu_\infty(U_\infty \cap [-1,1]^d)$*.*
For each prime p*, let* $U_p \subset \mathbb{Z}_p^d$*, such that* $\mu_p(\partial(U_p)) = 0$ *and define* $s_p = \mu_p(U_p)$*. Define*

$$\begin{aligned} P : \mathbb{Z}^d &\to 2^{M_{\mathbb{Q}}} \\ a &\mapsto \{\nu \in M_{\mathbb{Q}} \mid a \in U_\nu\}. \end{aligned}$$

If the following is satisfied:

$$\lim_{M\to\infty} \bar{\rho}\left(\left\{a \in \mathbb{Z}^d \mid a \in U_p \text{ for some prime } p > M\right\}\right) = 0, \quad (1)$$

Local to global principle

Theorem (continued)

then:

i) $\sum_{\nu \in M_{\mathbb{Q}}} s_\nu$ *converges.*

ii) *For* $\mathcal{S} \subset 2^{M_{\mathbb{Q}}}$, $\rho(P^{-1}(\mathcal{S}))$ *exists, and defines a measure on* $2^{M_{\mathbb{Q}}}$.

iii) *For each finite set* $S \in 2^{M_{\mathbb{Q}}}$, *we have that*

$$\rho(P^{-1}(\{S\})) = \prod_{\nu \in S} s_\nu \prod_{\nu \notin S} (1 - s_\nu),$$

and if $\mathcal{S}$ *consists of infinite subsets of* $2^{M_{\mathbb{Q}}}$, *then* $\rho(P^{-1}(\mathcal{S})) = 0$.

Local to global principle

Lemma (Poonen, Stoll, 1999)

Let $f, g \in \mathbb{Z}[x_1, \ldots, x_d]$ *be relatively prime. Define*

$$S_M(f,g) = \left\{ a \in \mathbb{Z}^d \mid p \mid f(a), p \mid g(a) \text{ for some prime } p > M \right\},$$

then

$$\lim_{M \to \infty} \bar{\rho}(S_M(f,g)) = 0.$$

Proof of Main Result

Let

$$\pi_p : \mathbb{Z}_p \to \mathbb{F}_p,$$

be the reduction modulo a rational prime p and

$$\mathbb{E}_p : \mathbb{F}_p^k \to \mathcal{O}_K/(p).$$

and the natural projection

$$\psi_p : \mathcal{O}_K/(p) \to \prod_{\mathfrak{p}|p} \left(\mathcal{O}_K/\mathfrak{p}\right).$$

Proof of Main Result

Let

$$\pi_p : \mathbb{Z}_p \to \mathbb{F}_p,$$

be the reduction modulo a rational prime p and

$$\mathbb{E}_p : \mathbb{F}_p^k \to \mathcal{O}_K/(p).$$

and the natural projection

$$\psi_p : \mathcal{O}_K/(p) \to \prod_{\mathfrak{p}|p} (\mathcal{O}_K/\mathfrak{p}) \, .$$

Then the composition of their extension is $F_p = \overline{\psi}_p \circ \overline{\mathbb{E}}_p \circ \overline{\pi}_p$:

$$\mathbb{Z}_p^{knm} \xrightarrow{\overline{\pi}_p} \mathbb{F}_p^{knm} \xrightarrow{\overline{\mathbb{E}}_p} (\mathcal{O}_K/(p))^{n\times m} \xrightarrow{\overline{\psi}_p} \prod_{\mathfrak{p}|p} (\mathcal{O}_K/\mathfrak{p})^{n\times m} = T_p.$$

Proof of Main Result

Define

$$\mathcal{L}_p = \left\{ \left(a_{\mathfrak{p}_1}, \dots, a_{\mathfrak{p}_{\ell_p}} \right) \in T_p \mid a_{\mathfrak{p}_i} \in \mathbb{F}_{p^{\deg(\mathfrak{p}_i)}}^{n \times m} \text{ has full rank} \right\}.$$

Define

$$\mathcal{L}_p = \left\{ \left(a_{\mathfrak{p}_1}, \dots, a_{\mathfrak{p}_{\ell_p}} \right) \in T_p \mid a_{\mathfrak{p}_i} \in \mathbb{F}_{p^{\deg(\mathfrak{p}_i)}}^{n \times m} \text{ has full rank} \right\}.$$

Consider now the following set

$$A_p = \left\{ A \in \mathbb{Z}_p^{knm} \mid F_p(A) \in \mathcal{L}_p \right\}.$$

Proof of Main Result

$$
\begin{aligned}
\mu_p(A_p) &= \mu_p\left(\bigsqcup_{f\in\mathcal{L}_p} F_p^{-1}(f)\right)\\
&= \sum_{f\in\mathcal{L}_p} \mu_p(F_p^{-1}(f))\\
&= \sum_{f\in\mathcal{L}_p} \mu_p(\overline{\pi}_p^{-1}\overline{\mathbb{E}}_p^{-1}\overline{\psi}_p^{-1}(f))\\
&= \sum_{f\in\mathcal{L}_p} \mu_p(\overline{\pi}_p^{-1}(\overline{\mathbb{E}}_p^{-1}(\overline{f}+\mathrm{Ker}(\overline{\psi}_p))))\\
&= \sum_{f\in\mathcal{L}_p} \mu_p\left(\bigsqcup_{i=1}^{|\mathrm{Ker}(\overline{\psi}_p)|}\left(f_i + p\mathbb{Z}_p^{knm}\right)\right)\\
&= \mid \mathcal{L}_p \mid \cdot \mid \mathrm{Ker}(\overline{\psi}_p) \mid p^{-knm}.
\end{aligned}
$$

Proof of Main Result

For

$$\overline{\psi}_p : (\mathcal{O}_K/(p))^{n\times m} \to \prod_{\mathfrak{p}|p} (\mathcal{O}_K/\mathfrak{p})^{n\times m}$$

we have

$$\dim_{\mathbb{F}_p}\left(\mathrm{Ker}(\overline{\psi}_p)\right) = knm - \sum_{\mathfrak{p}|p} \deg(\mathfrak{p}) nm.$$

For

$$\overline{\psi}_p : (\mathcal{O}_K/(p))^{n\times m} \to \prod_{\mathfrak{p}|p} (\mathcal{O}_K/\mathfrak{p})^{n\times m}$$

we have

$$\dim_{\mathbb{F}_p}\left(\mathrm{Ker}(\overline{\psi}_p)\right) = knm - \sum_{\mathfrak{p}|p} \deg(\mathfrak{p})nm.$$

Therefore

$$|\ \mathrm{Ker}(\overline{\psi}_p)\ | = p^{knm - \sum_{\mathfrak{p}|p} \deg(\mathfrak{p})nm}.$$

Proof of Main Result

Since for a prime power q the number of full rank matrices over $\mathbb{F}_q^{n\times m}$ is

$$\prod_{i=0}^{n-1}\left(q^m - q^i\right),$$

we have that

$$\mid \mathcal{L}_p \mid = \prod_{\mathfrak{p}\mid p}\prod_{i=0}^{n-1}\left(p^{\deg(\mathfrak{p})m} - p^{\deg(\mathfrak{p})i}\right).$$

Proof of Main Result

$$\begin{aligned}
\mu_p(A_p) &= p^{-knm} \mid \mathrm{Ker}(\overline{\psi}_p) \mid \cdot \mid \mathcal{L}_p \mid \\
&= \frac{1}{p^{knm}} \left(p^{knm - \sum_{\mathfrak{p}|p} \deg(\mathfrak{p}) nm} \right) \prod_{\mathfrak{p}|p} \prod_{i=0}^{n-1} \left(p^{\deg(\mathfrak{p})m} - p^{\deg(\mathfrak{p})i} \right) \\
&= p^{-\sum_{\mathfrak{p}|p} \deg(\mathfrak{p}) nm} \prod_{\mathfrak{p}|p} \prod_{i=0}^{n-1} \left(p^{\deg(\mathfrak{p})m} - p^{\deg(\mathfrak{p})i} \right) \\
&= \prod_{\mathfrak{p}|p} \prod_{i=0}^{n-1} p^{-\deg(\mathfrak{p})m} \left(p^{\deg(\mathfrak{p})m} - p^{\deg(\mathfrak{p})i} \right) \\
&= \prod_{\mathfrak{p}|p} \prod_{i=0}^{n-1} \left(1 - p^{\deg(\mathfrak{p})(i-m)} \right).
\end{aligned}$$

Let U be the set of rectangular unimodular $n \times m$ matrices over $\mathcal{O}_K$, hence we can write

$$U = \{M \in \mathrm{Mat}_{n\times m}(\mathcal{O}_K) \quad | \quad M \bmod \mathfrak{p} \text{ has full rank for any prime ideal } \mathfrak{p} \subset \mathcal{O}_K\}.$$

We choose $U_\infty = \emptyset$, then clearly $s_\infty = 0$.
We want to choose U_p such that $P^{-1}(\{\emptyset\}) = U$.

Proof of Main Result

Let U be the set of rectangular unimodular $n \times m$ matrices over $\mathcal{O}_K$, hence we can write

$$U = \{M \in \mathrm{Mat}_{n\times m}(\mathcal{O}_K) \quad | \quad M \bmod \mathfrak{p} \ \text{ has full rank} \\ \text{for any prime ideal } \mathfrak{p} \subset \mathcal{O}_K\}.$$

We choose $U_\infty = \emptyset$, then clearly $s_\infty = 0$.
We want to choose U_p such that $P^{-1}(\{\emptyset\}) = U$.
We choose $U_p = \mathbb{Z}_p^{knm} \setminus A_p$. Hence

$$s_p = \mu_p(U_p) = 1 - \mu_p(A_p) = 1 - \prod_{\mathfrak{p}|p} \prod_{i=0}^{n-1} \left(1 - p^{\deg(\mathfrak{p})(i-m)}\right).$$

Proof of Main Result

To show:

$$\lim_{M\to\infty} \bar{\rho}\left(\left\{A \in \mathbb{Z}^{knm} \mid A \in U_p \text{ for some prime } p > M\right\}\right) = 0.$$

Proof of Main Result

To show:

$$\lim_{M\to\infty} \bar{\rho}\left(\left\{A \in \mathbb{Z}^{knm} \mid A \in U_p \text{ for some prime } p > M\right\}\right) = 0.$$

Let $\overline{\mathbb{E}} : \mathbb{Z}^{knm} \to \mathcal{O}_K^{n\times m}$.
For $A \in \mathbb{Z}^{knm}$, let us denote the $n \times n$ minors of $\overline{\mathbb{E}}(A)$ by A_i for $i \in \left\{1, \dots, \binom{m}{n}\right\}$.
Hence $A \in U_p$ is equivalent to $\langle A_1, \dots, A_{\binom{m}{n}}\rangle \subseteq \mathfrak{p}$ for some $\mathfrak{p} \mid p$.
Thus for all $i \in \left\{1, \dots, \binom{m}{n}\right\}$ we have that $\langle A_i\rangle \subseteq \mathfrak{p}$ and hence that $N_{K/\mathbb{Q}}(A_i) \equiv 0 \mod p$. Hence it is a subset of

$$B_M = \Big\{A \in \mathbb{Z}^{knm} \quad \mid \quad p \mid N_{K/\mathbb{Q}}(A_1), p \mid N_{K/\mathbb{Q}}(A_2) \\ \text{for some prime } p > M\}\,.$$

Proof of Main Result

Remark

Let $\mathcal{R}$ *be an integral domain and* $n \in \mathbb{N}$. *Recall that, if* X *is an* $n \times n$ *polynomial matrix over* $\mathcal{R}[x_{1,1}, \ldots, x_{n,n}]$ *having as* (i,j) *entry the variable* $x_{i,j}$, *then* $\det(X) \in \mathcal{R}[x_{1,1}, \ldots, x_{n,n}]$ *is irreducible.*

Proof of Main Result

Remark

Let $\mathcal{R}$ be an integral domain and $n \in \mathbb{N}$. Recall that, if X is an $n \times n$ polynomial matrix over $\mathcal{R}[x_{1,1}, \dots, x_{n,n}]$ having as (i,j) entry the variable $x_{i,j}$, then $\det(X) \in \mathcal{R}[x_{1,1}, \dots, x_{n,n}]$ is irreducible.

Let $\ell, k \in \mathbb{N}, f \in \mathbb{C}[x_1, \dots, x_\ell]$ and $e = (e_1, \dots, e_k) \in (\mathbb{C} \setminus \{0\})^k$. In the new polynomial ring $\mathbb{C}[x_1^{(1)}, x_1^{(2)}, \dots, x_\ell^{(k)}]$ let us denote by f_e

$$f\left(\sum_{u=1}^{k} x_1^{(u)} e_u, \dots, \sum_{u=1}^{k} x_\ell^{(u)} e_u\right).$$

Lemma

Let ℓ, k, f and e be as above. If $f \in \mathbb{C}[x_1, \dots, x_\ell]$ is irreducible, then f_e is irreducible in $\mathbb{C}[x_1^{(1)}, x_1^{(2)}, \dots, x_\ell^{(k)}]$.

Lemma

Let N be the norm map for the extension field $K(x_1, \ldots x_M)/\mathbb{Q}(x_1, \ldots x_M)$. Let $F, G \in \mathcal{O}_K[x_1, \ldots, x_M]$ be irreducible and such that there are variables appearing in F but not in G, then $N(F)$ and $N(G)$ are coprime.

Proof of Main Result

Using the local to global principle, we get

$$\begin{aligned}
\rho(U) = \rho(P^{-1}(\{\emptyset\})) &= \prod_{\nu \in \emptyset} s_\nu \prod_{\nu \notin \emptyset} (1 - s_\nu) \\
&= (1 - s_\infty) \prod_{p \text{ prime}} (1 - s_p) \\
&= \prod_{p \text{ prime}} \prod_{\mathfrak{p} | p} \prod_{i=0}^{n-1} \left(1 - p^{\deg(\mathfrak{p})(i-m)}\right) \\
&= \prod_{i=0}^{n-1} \prod_{p \text{ prime}} \prod_{\mathfrak{p} | p} \left(1 - \frac{1}{p^{\deg(\mathfrak{p})(m-i)}}\right) \\
&= \prod_{i=0}^{n-1} \frac{1}{\zeta_K(m-i)}.
\end{aligned}$$

Thank you