Workshop on Interactions between Number Theory and Wireless Communication,
University of York ; July 05, 2016.

Quadratic forms, lattice points and interference alignment

Faustin ADICEAM
(joint with Evgeniy ZORIN)

University of York

Plan

Motivation

- Let $m, n \geq 1$ be integers and let $\gamma, c > 0$ be real numbers. Define

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n \times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

Initial Problem

Assume that the set $\mathcal{H}_{m,n}(\gamma, c)$ is equipped with a "uniform" probability measure. Let $s \geq 0$.

What is the probability that the quantity

$$\min_{\mathbf{a} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}} \mathbf{a}^T \cdot \left(\gamma I_m + H^T \cdot H\right) \cdot \mathbf{a} \qquad (1)$$

should be less than s ?

In other words, what is the cumulative distribution function of (1) seen as a random variable ?

Motivation

- Let $m, n \geq 1$ be integers and let $\gamma, c > 0$ be real numbers. Define

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n \times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

Initial Problem

Assume that the set $\mathcal{H}_{m,n}(\gamma, c)$ is equipped with a "uniform" probability measure. Let $s \geq 0$.

What is the probability that the quantity

$$\min_{\mathbf{a} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}} \mathbf{a}^T \cdot \left(\gamma I_m + H^T \cdot H\right) \cdot \mathbf{a} \qquad (1)$$

should be less than s ?

In other words, what is the cumulative distribution function of (1) seen as a random variable ?

Rephrasing the Initial Problem in a more general context

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Given $H \in \mathcal{H}_{m,n}(\gamma, c)$, let

$$\Sigma_H := c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++},$$

where Σ_m^{++} is the set of positive definite matrices *with determinant one.*
- Given $\Sigma \in \Sigma_d^{++}$, set

$$M_d(\Sigma) := \min_{\mathbf{a} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}} \mathbf{a}^T \cdot \Sigma \cdot \mathbf{a}$$

(which is easily seen to be well-defined).

Main Problem

Assume that the set $\Sigma \in \Sigma_d^{++}$ is equipped with a probability measure. What is the cumulative distribution function of the random variable $M_d(\Sigma)$?

Rephrasing the Initial Problem in a more general context

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{H \in \mathbb{R}^{n\times m} \; : \; \det\left(\gamma I_m + H^T \cdot H\right) = c\right\}.$$

- Given $H \in \mathcal{H}_{m,n}(\gamma, c)$, let

$$\Sigma_H := c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++},$$

where Σ_m^{++} is the set of positive definite matrices *with determinant one*.

- Given $\Sigma \in \Sigma_d^{++}$, set

$$M_d(\Sigma) := \min_{a \in \mathbb{Z}^d \setminus \{0\}} a^T \cdot \Sigma \cdot a$$

(which is easily seen to be well-defined).

Main Problem

Assume that the set $\Sigma \in \Sigma_d^{++}$ is equipped with a probability measure. What is the cumulative distribution function of the random variable $M_d(\Sigma)$?

Rephrasing the Initial Problem in a more general context

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \,:\, \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Given $H \in \mathcal{H}_{m,n}(\gamma, c)$, let

$$\Sigma_H := c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++},$$

  where Σ_m^{++} is the set of positive definite matrices *with determinant one*.
- Given $\Sigma \in \Sigma_d^{++}$, set

$$M_d(\Sigma) := \min_{\boldsymbol{a}\in\mathbb{Z}^d\setminus\{\boldsymbol{0}\}} \boldsymbol{a}^T \cdot \Sigma \cdot \boldsymbol{a}$$

  (which is easily seen to be well-defined).

Main Problem

Assume that the set $\Sigma \in \Sigma_d^{++}$ is equipped with a probability measure. What is the cumulative distribution function of the random variable $M_d(\Sigma)$?

The non–probabilistic case : the Hermite constant

- Recall that for $\Sigma \in \Sigma_d^{++}$,

$$M_d\left(\Sigma\right) := \min_{\boldsymbol{a}\in\mathbb{Z}^d\setminus\{\boldsymbol{0}\}} \boldsymbol{a}^T \cdot \Sigma \cdot \boldsymbol{a}$$

- Hermite proved that there exists a constant $\gamma_d > 0$ such that, for *any* $\Sigma \in \Sigma_d^{++}$,

$$M_d(\Sigma) \leq \gamma_d.$$

d (dimension)	1	2	3	4	5	6	7	8	24
γ_d^d	1	4/3	2	4	8	64/3	64	256	4^{24}

TABLE : Known values of the Hermite constant γ_d

- One can also prove for instance that

$$V_d^{-2/d} \leq \gamma_d \leq 4 \cdot V_d^{-2/d},$$

where V_d is the volume of the Euclidean unit ball in dimension $d \geq 1$.

The non–probabilistic case : the Hermite constant

- Recall that for $\Sigma \in \Sigma_d^{++}$,

$$M_d\left(\Sigma\right) := \min_{\boldsymbol{a}\in\mathbb{Z}^d\setminus\{\mathbf{0}\}} \boldsymbol{a}^T \cdot \Sigma \cdot \boldsymbol{a}$$

- Hermite proved that there exists a constant $\gamma_d > 0$ such that, for *any* $\Sigma \in \Sigma_d^{++}$,

$$M_d(\Sigma) \leq \gamma_d.$$

d (dimension)	1	2	3	4	5	6	7	8	24
γ_d^d	1	4/3	2	4	8	64/3	64	256	4^{24}

TABLE : Known values of the Hermite constant γ_d

- One can also prove for instance that

$$V_d^{-2/d} \leq \gamma_d \leq 4 \cdot V_d^{-2/d},$$

where V_d is the volume of the Euclidean unit ball in dimension $d \geq 1$.

The non–probabilistic case : the Hermite constant

- Recall that for $\Sigma \in \Sigma_d^{++}$,

$$M_d(\Sigma) := \min_{\boldsymbol{a} \in \mathbb{Z}^d \setminus \{\boldsymbol{0}\}} \boldsymbol{a}^T \cdot \Sigma \cdot \boldsymbol{a}$$

- Hermite proved that there exists a constant $\gamma_d > 0$ such that, for *any* $\Sigma \in \Sigma_d^{++}$,

$$M_d(\Sigma) \leq \gamma_d.$$

d (dimension)	1	2	3	4	5	6	7	8	24
γ_d^d	1	4/3	2	4	8	64/3	64	256	4^{24}

TABLE : Known values of the Hermite constant γ_d

- One can also prove for instance that

$$V_d^{-2/d} \leq \gamma_d \leq 4 \cdot V_d^{-2/d},$$

where V_d is the volume of the Euclidean unit ball in dimension $d \geq 1$.

How to tackle the Main Problem ?

- Two possible approaches :
  - a purely algebraic one :
    - essentially based on the Cholesky decomposition of an element in Σ_d^{++},
    - will provide an answer to the Initial Problem ;
  - a purely geometric one :
    - based on the spectral decomposition of an element in Σ_d^{++},
    - much more theoretical (only a few words in this talk).

How to tackle the Main Problem ?

- Two possible approaches :
  - a purely algebraic one :
    - essentially based on the Cholesky decomposition of an element in Σ_d^{++},
    - will provide an answer to the Initial Problem ;
  - a purely geometric one :
    - based on the spectral decomposition of an element in Σ_d^{++},
    - much more theoretical (only a few words in this talk).

Plan

Plan

Two preliminary remarks

- The problem is $SL_d(\mathbb{Z})$–invariant in the sense that for any $\Sigma \in \Sigma_d^{++}$ and any $A \in SL_d(\mathbb{Z})$,

$$M_d\left(A^T \cdot \Sigma \cdot A\right) = M_d(\Sigma)$$

- Any $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = L^T \cdot L,$$

where L belongs to the set of upper triangular matrices.
  - This decomposition is furthermore unique if one requires that L should have *strictly positive* diagonal entries (it is then known as the Cholesky decomposition of a positive definite matrix).

Two preliminary remarks

- The problem is $SL_d(\mathbb{Z})$–invariant in the sense that for any $\Sigma \in \Sigma_d^{++}$ and any $A \in SL_d(\mathbb{Z})$,

$$M_d\left(A^T \cdot \Sigma \cdot A\right) = M_d(\Sigma)$$

- Any $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = L^T \cdot L,$$

where L belongs to the set of upper triangular matrices.
  - This decomposition is furthermore unique if one requires that L should have *strictly positive* diagonal entries (it is then known as the Cholesky decomposition of a positive definite matrix).

Some heuristics with an abstract formulation of the problem

- The problem of estimating $M_d(\Sigma)$ for $\Sigma \in \Sigma_d^{++}$ is thus well–defined when Σ is seen as a element of the set

$$X_d := SO_d(\mathbb{R})\backslash SL_d(\mathbb{R})/SL_d(\mathbb{Z})$$

(a so–called *locally symmetric space*).

- The latter set can be equipped with a natural probability measure μ_{X_d} (coming from a so–called *Haar measure*).

Theorem (Kleinbock & Margulis, 1998)

Let $\delta > 0$. Denote by $p_{X_d}(\delta)$ the probability (w.r.t μ_{X_d}) of the event $M_d(\Sigma) \leq \delta$ in the space X_d. Then :

$$\frac{V_d}{2\zeta(d)}\delta^{d/2} - c_d\frac{V_d^2}{4}\delta^d \leq p_{X_d}(\delta) \leq \frac{V_d}{2\zeta(d)}\delta^{d/2}. \qquad (2)$$

Here, ζ denotes the Riemann zeta function, c_d is an explicit strictly positive constant and V_d denotes again the volume of the unit Euclidean ball in dimension d.

Some heuristics with an abstract formulation of the problem

- The problem of estimating $M_d(\Sigma)$ for $\Sigma \in \Sigma_d^{++}$ is thus well–defined when Σ is seen as a element of the set

$$X_d := SO_d(\mathbb{R})\backslash SL_d(\mathbb{R})/SL_d(\mathbb{Z})$$

(a so–called *locally symmetric space*).

- The latter set can be equipped with a natural probability measure μ_{X_d} (coming from a so–called *Haar measure*).

Theorem (Kleinbock & Margulis, 1998)

Let $\delta > 0$. Denote by $p_{X_d}(\delta)$ the probability (w.r.t μ_{X_d}) of the event $M_d(\Sigma) \leq \delta$ in the space X_d. Then :

$$\frac{V_d}{2\zeta(d)}\delta^{d/2} - c_d\frac{V_d^2}{4}\delta^d \leq p_{X_d}(\delta) \leq \frac{V_d}{2\zeta(d)}\delta^{d/2}. \qquad (2)$$

Here, ζ denotes the Riemann zeta function, c_d is an explicit strictly positive constant and V_d denotes again the volume of the unit Euclidean ball in dimension d.

Some heuristics with an abstract formulation of the problem

- The problem of estimating $M_d(\Sigma)$ for $\Sigma \in \Sigma_d^{++}$ is thus well–defined when Σ is seen as a element of the set

$$X_d := SO_d(\mathbb{R})\backslash SL_d(\mathbb{R})/SL_d(\mathbb{Z})$$

(a so–called *locally symmetric space*).

- The latter set can be equipped with a natural probability measure μ_{X_d} (coming from a so–called *Haar measure*).

Theorem (Kleinbock & Margulis, 1998)

Let $\delta > 0$. Denote by $p_{X_d}(\delta)$ the probability (w.r.t μ_{X_d}) of the event $M_d(\Sigma) \leq \delta$ in the space X_d. Then :

$$\frac{V_d}{2\zeta(d)}\delta^{d/2} - c_d\frac{V_d^2}{4}\delta^d \leq p_{X_d}(\delta) \leq \frac{V_d}{2\zeta(d)}\delta^{d/2}. \tag{2}$$

Here, ζ denotes the Riemann zeta function, c_d is an explicit strictly positive constant and V_d denotes again the volume of the unit Euclidean ball in dimension d.

Some heuristics with an abstract formulation of the problem (bis)

Theorem (Kleinbock & Margulis, 1998)

Let $\delta > 0$. Denote by $p_{X_d}(\delta)$ the probability (w.r.t μ_{X_d}) of the event $M_d(\Sigma) \leq \delta$ in the space X_d. Then :

$$\frac{V_d}{2\zeta(d)}\delta^{d/2} - c_d \frac{V_d^2}{4}\delta^d \leq p_{X_d}(\delta) \leq \frac{V_d}{2\zeta(d)}\delta^{d/2}.$$

Here, ζ denotes the Riemann zeta function, c_d is an explicit strictly positive constant and V_d denotes again the volume of the unit Euclidean ball in dimension d.

- Resulting heuristics : for a "typical measure", one should expect the probability of the event $M_d(\Sigma) \leq \delta$ to grow like the volume of the Euclidean ball of radius $\sqrt{\delta}$ in dimension d.

Strategy to tackle the Main Problem with the algebraic approach

- Assume that f is some density function on Σ_d^{++} : the problem boils down to estimating the integral :

$$\mathfrak{m}_f(\delta) \;:=\; \int_{\Sigma_d^{++}} \chi_{[M_d(\Sigma)>\delta]} \cdot f(\Sigma) \cdot \mathrm{d}\Sigma$$

for a given $\delta > 0$.

- If $\Sigma \in \Sigma_d^{++}$ is decomposed in its Cholesky form as $\Sigma = L^T \cdot L$, then :

$$(M_d(\Sigma) > \delta) \quad \Longleftrightarrow \quad \left(L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \sqrt{\delta}) = \{\mathbf{0}\}\right).$$

- The problem has thus been reduced to measure the probability that a lattice of the form $L \cdot \mathbb{Z}^d$, with L upper triangular with strictly positive diagonal entries, does not admit a short non–zero vector.

Strategy to tackle the Main Problem with the algebraic approach

- Assume that f is some density function on Σ_d^{++} : the problem boils down to estimating the integral :

$$\mathfrak{m}_f(\delta) \;:=\; \int_{\Sigma_d^{++}} \chi_{[M_d(\Sigma)>\delta]} \cdot f(\Sigma) \cdot \mathrm{d}\Sigma$$

  for a given $\delta > 0$.
- If $\Sigma \in \Sigma_d^{++}$ is decomposed in its Cholesky form as $\Sigma = L^T \cdot L$, then :

$$(M_d(\Sigma) > \delta) \quad\Longleftrightarrow\quad \left(L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \sqrt{\delta}) = \{\mathbf{0}\}\right).$$

- The problem has thus been reduced to measure the probability that a lattice of the form $L \cdot \mathbb{Z}^d$, with L upper triangular with strictly positive diagonal entries, does not admit a short non–zero vector.

Strategy to tackle the Main Problem with the algebraic approach

- Assume that f is some density function on Σ_d^{++} : the problem boils down to estimating the integral :

$$\mathfrak{m}_f(\delta) \ := \int_{\Sigma_d^{++}} \chi_{[M_d(\Sigma)>\delta]} \cdot f(\Sigma) \cdot \mathrm{d}\Sigma$$

  for a given $\delta > 0$.

- If $\Sigma \in \Sigma_d^{++}$ is decomposed in its Cholesky form as $\Sigma = L^T \cdot L$, then :

$$(M_d(\Sigma) > \delta) \quad \Longleftrightarrow \quad \left(L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \sqrt{\delta}) \ = \ \{\mathbf{0}\} \right).$$

- The problem has thus been reduced to measure the probability that a lattice of the form $L \cdot \mathbb{Z}^d$, with L upper triangular with strictly positive diagonal entries, does not admit a short non–zero vector.

A key–observation

- Denote by $\mathcal{T}_d^{++}$ the set of upper triangular matrices of determinant one with strictly positive diagonal entries.
- The diagonal entries of a generic elements $L \in \mathcal{T}_d^{++}$ will hereafter be denoted by $(\beta_1, \dots, \beta_d) \in (\mathbb{R}_{>0})^d$. In particular,

$$\beta_d = \left(\prod_{i=1}^{d-1} \beta_i \right)^{-1}.$$

Lemma

With the previous notation, the following hold :

- *if $\beta_i > \eta$ for all $i = 1, \dots, d$, then*

$$L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \eta) = \{\mathbf{0}\};$$

- *conversely, if $L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \eta) = \{\mathbf{0}\}$, then $\beta_1 > \eta$.*

A key–observation

- Denote by $\mathcal{T}_d^{++}$ the set of upper triangular matrices of determinant one with strictly positive diagonal entries.
- The diagonal entries of a generic elements $L \in \mathcal{T}_d^{++}$ will hereafter be denoted by $(\beta_1, \dots, \beta_d) \in (\mathbb{R}_{>0})^d$. In particular,

$$\beta_d = \left(\prod_{i=1}^{d-1} \beta_i \right)^{-1} .$$

Lemma

With the previous notation, the following hold :

- *if $\beta_i > \eta$ for all $i = 1, \dots, d$, then*

$$L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \eta) = \{\mathbf{0}\} ;$$

- *conversely, if $L \cdot \mathbb{Z}^d \cap B_2(\mathbf{0}, \eta) = \{\mathbf{0}\}$, then $\beta_1 > \eta$.*

Implication for the Main Problem

- By change of variables, given $\delta > 0$,

$$\mathfrak{m}_f(\delta) := \int_{\Sigma_d^{++}} \chi_{[M_d(\Sigma)>\delta]} \cdot f(\Sigma) \cdot \mathrm{d}\Sigma = \int_{\mathcal{T}_d^{++}} \chi_{[M_d(\varphi_{chol}(L))>\delta]} \cdot G_f(L) \cdot \mathrm{d}L,$$

with

$$G_f(L) := f(\varphi_{chol}(L)) \cdot \mathrm{Jac}_L(\varphi_{chol}).$$

Here, $\mathrm{Jac}_L(\varphi_{chol})$ is the Jacobian at $L \in \mathcal{T}_d^{++}$ of the Cholesky map

$$\varphi_{chol} : L \in \mathcal{T}_d^{++} \mapsto L^T L \in \Sigma_d^{++}.$$

- From the previous lemma, one has therefore

$$\int_{\mathcal{T}_d^{(1)}(\delta)} G_f(L) \cdot \mathrm{d}L \le \mathfrak{m}_f(\delta) \le \int_{\mathcal{T}_d^{(2)}(\delta)} G_f(L) \cdot \mathrm{d}L,$$

where :
  - $\mathcal{T}_d^{(1)}(\delta)$ is the set of matrices $L \in \mathcal{T}_d^{++}$ such that $\beta_i > \sqrt{\delta}$ for all $i = 1, \dots, d$.
  - $\mathcal{T}_d^{(2)}(\delta)$ is the set of matrices $L \in \mathcal{T}_d^{++}$ such that $\beta_1 > \sqrt{\delta}$.

Implication for the Main Problem

- By change of variables, given $\delta > 0$,

$$\begin{aligned}\mathfrak{m}_f(\delta) &:= \int_{\Sigma_d^{++}} \chi_{[M_d(\Sigma)>\delta]} \cdot f(\Sigma) \cdot \mathrm{d}\Sigma \\ &= \int_{\mathcal{T}_d^{++}} \chi_{[M_d(\varphi_{chol}(L))>\delta]} \cdot G_f(L) \cdot \mathrm{d}L,\end{aligned}$$

with

$$G_f(L) := f(\varphi_{chol}(L)) \cdot \mathrm{Jac}_L(\varphi_{chol}).$$

Here, $\mathrm{Jac}_L(\varphi_{chol})$ is the Jacobian at $L \in \mathcal{T}_d^{++}$ of the Cholesky map

$$\varphi_{chol} : L \in \mathcal{T}_d^{++} \mapsto L^T L \in \Sigma_d^{++}.$$

- From the previous lemma, one has therefore

$$\int_{\mathcal{T}_d^{(1)}(\delta)} G_f(L) \cdot \mathrm{d}L \leq \mathfrak{m}_f(\delta) \leq \int_{\mathcal{T}_d^{(2)}(\delta)} G_f(L) \cdot \mathrm{d}L,$$

where :
  - $\mathcal{T}_d^{(1)}(\delta)$ is the set of matrices $L \in \mathcal{T}_d^{++}$ such that $\beta_i > \sqrt{\delta}$ for all $i = 1, \ldots, d$.
  - $\mathcal{T}_d^{(2)}(\delta)$ is the set of matrices $L \in \mathcal{T}_d^{++}$ such that $\beta_1 > \sqrt{\delta}$.

Conclusions regarding the theoretical part of the algebraic approach

- Given a density function f on the space Σ_d^{++} and given $\delta > 0$, the probability $\mathfrak{m}_f(\delta)$ of the event $M_d(\Sigma) > \delta$ can be estimated both by above and by below.
- The lower bound for $\mathfrak{m}_f(\delta)$ is more accurate (can be seen as nearly optimal for "not too wild" density functions).

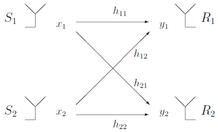
Conclusions regarding the theoretical part of the algebraic approach

- Given a density function f on the space Σ_d^{++} and given $\delta > 0$, the probability $\mathfrak{m}_f(\delta)$ of the event $M_d\,(\Sigma) > \delta$ can be estimated both by above and by below.
- The lower bound for $\mathfrak{m}_f(\delta)$ is more accurate (can be seen as nearly optimal for "not too wild" density functions).

Plan

Application to Signal Processing : the general set–up

- Assume that two *users* (or *transmitters*) S_1 and S_2 want to *transmit* messages (or *signals*) x_1 (for S_1) and x_2 (for S_2) along a communication channel (e.g., a cable or a radio channel) simultaneously to two *receivers* R_1 and R_2.



- In the simplest case that they use an additive channel, the message y_i received by R_i ($i \in \{1, 2\}$) is represented by the system of equations

$$\begin{cases} y_1 = h_{11}x_1 + h_{12}x_2 + z_1 \\ y_2 = h_{21}x_1 + h_{22}x_2 + z_2, \end{cases} \tag{3}$$

where z_1 and z_2 are the noise and h_{ij} ($1 \leq i, j \leq 2$) the *channel coefficients* representing a certain degree of *fading* in the transmission.

The general set–up (bis)

- In the case of $m \geq 1$ users and $n \geq 1$ receivers, the model generalises in an obvious way :

$$\boldsymbol{y} \; = \; H \cdot \boldsymbol{x} + \boldsymbol{z},$$

where $H \in \mathbb{R}^{n \times m}$, $\boldsymbol{x} \in \mathbb{R}^m$ and $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{R}^n$.

- The input $\boldsymbol{x}$ (seen as a random variable) satisfies a power constraint of the form :

$$\mathbb{E}\left(\boldsymbol{x}^T \cdot \boldsymbol{x}\right) \; \leq \; m \cdot SNR,$$

where SNR stands for the *Signal–to–Noise Ratio* (expressed in *decibels*).

The general set–up (bis)

- In the case of $m \geq 1$ users and $n \geq 1$ receivers, the model generalises in an obvious way :

$$\boldsymbol{y} \;=\; H \cdot \boldsymbol{x} + \boldsymbol{z},$$

where $H \in \mathbb{R}^{n \times m}$, $\boldsymbol{x} \in \mathbb{R}^m$ and $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{R}^n$.

- The input $\boldsymbol{x}$ (seen as a random variable) satisfies a power constraint of the form :

$$\mathbb{E}\left(\boldsymbol{x}^T \cdot \boldsymbol{x}\right) \;\leq\; m \cdot SNR,$$

where SNR stands for the *Signal–to–Noise Ratio* (expressed in *decibels*).

The general set–up (ter)

- Basic problem : to determine whether the received information is reliable.
- Naive solution : to reduce the rate of new data sent by the users (for instance, by repeating each string of message several times).
- In 1948, Shannon proved that this intuition is surprisingly incorrect :
  - It is actually possible to exchange information at a *strictly positive* data rate keeping at the same time the error probability as small as desired.
  - There is nevertheless a maximal rate, the *capacity of the channel*, above which this cannot be done any more. The latter quantity is usually expressed in bits.

The general set–up (ter)

- Basic problem : to determine whether the received information is reliable.
- Naive solution : to reduce the rate of new data sent by the users (for instance, by repeating each string of message several times).
- In 1948, Shannon proved that this intuition is surprisingly incorrect :
  - It is actually possible to exchange information at a *strictly positive* data rate keeping at the same time the error probability as small as desired.
  - There is nevertheless a maximal rate, the *capacity of the channel*, above which this cannot be done any more. The latter quantity is usually expressed in bits.

The general set–up (ter)

- Basic problem : to determine whether the received information is reliable.
- Naive solution : to reduce the rate of new data sent by the users (for instance, by repeating each string of message several times).
- In 1948, Shannon proved that this intuition is surprisingly incorrect :
  - It is actually possible to exchange information at a *strictly positive* data rate keeping at the same time the error probability as small as desired.
  - There is nevertheless a maximal rate, the *capacity of the channel*, above which this cannot be done any more. The latter quantity is usually expressed in bits.

The general set–up (quater)

- A crucial remark : the performances of a channel depends heavily on whether or not the transmitter knows the channel coefficients matrix H.
  - => If such information is available, they can for instance allocate more power to the stronger antennas to minimise the effect of fading.
  - => If this information is not known to the transmitter a reasonable strategy is to allocate equal power to each of the sub–channels. In this situation, the capacity of the channel is rather referred to as the *mutual information*.

The general set–up (quater)

- A crucial remark : the performances of a channel depends heavily on whether or not the transmitter knows the channel coefficients matrix H.
  - => If such information is available, they can for instance allocate more power to the stronger antennas to minimise the effect of fading.
  - => If this information is not known to the transmitter a reasonable strategy is to allocate equal power to each of the sub–channels. In this situation, the capacity of the channel is rather referred to as the *mutual information*.

The general set–up (quater)

- A crucial remark : the performances of a channel depends heavily on whether or not the transmitter knows the channel coefficients matrix H.
  - => If such information is available, they can for instance allocate more power to the stronger antennas to minimise the effect of fading.
  - => If this information is not known to the transmitter a reasonable strategy is to allocate equal power to each of the sub–channels. In this situation, the capacity of the channel is rather referred to as the *mutual information*.

The general set–up (quinquies)

- There is no single expression for the capacity/mutual information C of a channel, but in all the cases we will be interested in :

$$C = \log\det\left(I_m + SNR \cdot H^T \cdot H\right).$$

- In the more specific case of a channel where a so–called Integer Forcing Technique is applied at the Receiver, the “quality” of the channel is determined by the so–called Effective–Signal–to–Noise Ratio SNR_{eff} which satisfies the estimates (Erez & Ordentlich, 2015) :

$$\frac{1}{4m^2} \cdot M_m\left(I_m + \mathrm{SNR} \cdot H^T \cdot H\right) < \mathrm{SNR}_{\mathrm{eff}} \leq M_m\left(I_m + \mathrm{SNR} \cdot H^T \cdot H\right).$$

The general set–up (quinquies)

- There is no single expression for the capacity/mutual information C of a channel, but in all the cases we will be interested in :

$$C \;=\; \log\det\left(I_m + SNR\cdot H^T\cdot H\right).$$

- In the more specific case of a channel where a so–called Integer Forcing Technique is applied at the Receiver, the "quality" of the channel is determined by the so–called Effective–Signal–to–Noise Ratio SNR_{eff} which satisfies the estimates (Erez & Ordentlich, 2015) :

$$\frac{1}{4m^2}\cdot M_m\left(I_m+\mathrm{SNR}\cdot H^T\cdot H\right)\;<\;\mathrm{SNR}_{\mathrm{eff}}\;\le\;M_m\left(I_m+\mathrm{SNR}\cdot H^T\cdot H\right).$$

A possible Interpretation of the Initial Problem

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}$$

and

Initial Problem

Assume that the set $\mathcal{H}_{m,n}(\gamma, c)$ is equipped with a "uniform" probability measure. Let $s \geq 0$.
What is the cumulative distribution function of the quantity $M_m\left(\gamma I_m + H^T \cdot H\right)$ seen as a random variable ?

- For the channel under consideration and up to an elementary change of variables, this Initial Problem can be interpreted as the determination of the cumulative distribution function of SNR_{eff} under the assumption that the transmitter has no knowledge of the channel coefficients matrix H.

A possible Interpretation of the Initial Problem

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{H \in \mathbb{R}^{n\times m} : \det\left(\gamma I_m + H^T \cdot H\right) = c\right\}$$

and

Initial Problem

Assume that the set $\mathcal{H}_{m,n}(\gamma, c)$ is equipped with a "uniform" probability measure. Let $s \geq 0$.
What is the cumulative distribution function of the quantity $M_m\left(\gamma I_m + H^T \cdot H\right)$ seen as a random variable ?

- For the channel under consideration and up to an elementary change of variables, this Initial Problem can be interpreted as the determination of the cumulative distribution function of SNR_{eff} under the assumption that the transmitter has no knowledge of the channel coefficients matrix H.

Strategy to tackle the Initial Problem

1/ Define properly the concept of a "uniform" probability measure on $\mathcal{H}_{m,n}(\gamma, c)$.

2/ Push this measure forward to the space of positive definite matrices of determinant one Σ_d^{++} with the help of the map

$$f \ : H \in \mathcal{H}_{m,n}(\gamma, c) \ \mapsto \ c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++}.$$

=> This essentially requires a change of variables $\Sigma = f(H)$ and the calculation of the corresponding Jacobian.

$$\mathcal{H}_{m,n}(\gamma, c) \xrightarrow{f} \Sigma_m^{++} \xrightarrow{\widetilde{\varphi}_{chol}^{-1}} \mathcal{T}_m^{++}$$

3/ The general theory developed previously can be applied with the probability density function in the space Σ_m^{++} obtained in Step 2.

- Conclusion : It only remains to solve Step 1.

Strategy to tackle the Initial Problem

1/ Define properly the concept of a "uniform" probability measure on $\mathcal{H}_{m,n}(\gamma, c)$.

2/ Push this measure forward to the space of positive definite matrices of determinant one Σ_d^{++} with the help of the map

$$f \ : H \in \mathcal{H}_{m,n}(\gamma, c) \ \mapsto \ c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++}.$$

=> This essentially requires a change of variables $\Sigma = f(H)$ and the calculation of the corresponding Jacobian.

$$\mathcal{H}_{m,n}(\gamma, c) \xrightarrow{f} \Sigma_m^{++} \xrightarrow{\widetilde{\varphi}_{chol}^{-1}} \mathcal{T}_m^{++}$$

3/ The general theory developed previously can be applied with the probability density function in the space Σ_m^{++} obtained in Step 2.

- Conclusion : It only remains to solve Step 1.

Strategy to tackle the Initial Problem

1/ Define properly the concept of a “uniform” probability measure on $\mathcal{H}_{m,n}(\gamma, c)$.

2/ Push this measure forward to the space of positive definite matrices of determinant one Σ_d^{++} with the help of the map

$$f \; : H \in \mathcal{H}_{m,n}(\gamma, c) \; \mapsto \; c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++}.$$

=> This essentially requires a change of variables $\Sigma = f(H)$ and the calculation of the corresponding Jacobian.

$$\mathcal{H}_{m,n}(\gamma, c) \xrightarrow{f} \Sigma_m^{++} \xrightarrow{\widetilde{\varphi}_{chol}^{-1}} \mathcal{T}_m^{++}$$

3/ The general theory developed previously can be applied with the probability density function in the space Σ_m^{++} obtained in Step 2.

- Conclusion : It only remains to solve Step 1.

Strategy to tackle the Initial Problem

1/ Define properly the concept of a "uniform" probability measure on $\mathcal{H}_{m,n}(\gamma, c)$.

2/ Push this measure forward to the space of positive definite matrices of determinant one Σ_d^{++} with the help of the map

$$f\ : H \in \mathcal{H}_{m,n}(\gamma, c) \ \mapsto\ c^{-1/m} \cdot \left(\gamma I_m + H^T \cdot H\right) \in \Sigma_m^{++}.$$

=> This essentially requires a change of variables $\Sigma = f(H)$ and the calculation of the corresponding Jacobian.

$$\mathcal{H}_{m,n}(\gamma, c) \xrightarrow{f} \Sigma_m^{++} \xrightarrow{\widetilde{\varphi}_{chol}^{-1}} \mathcal{T}_m^{++}$$

3/ The general theory developed previously can be applied with the probability density function in the space Σ_m^{++} obtained in Step 2.

- Conclusion : It only remains to solve Step 1.

Some topological properties of the set $\mathcal{H}_{m,n}(\gamma, c)$

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}$$

- From Sylvester's determinant identity, for any $H \in \mathbb{R}^{n\times m}$,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_n + H \cdot H^T\right).$$

=> It may be assumed *without loss of generality* that

$$d := \min\{m, n\} = m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is empty if $c < \gamma^m$ and reduced to the zero matrix if $c = \gamma^m$. Assume therefore from now on that

$$c > \gamma^m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is compact.

Some topological properties of the set $\mathcal{H}_{m,n}(\gamma, c)$

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}$$

- From Sylvester's determinant identity, for any $H \in \mathbb{R}^{n\times m}$,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_n + H \cdot H^T\right).$$

=> It may be assumed *without loss of generality* that

$$d := \min\{m, n\} = m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is empty if $c < \gamma^m$ and reduced to the zero matrix if $c = \gamma^m$. Assume therefore from now on that

$$c > \gamma^m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is compact.

Some topological properties of the set $\mathcal{H}_{m,n}(\gamma, c)$

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}$$

- From Sylvester's determinant identity, for any $H \in \mathbb{R}^{n\times m}$,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_n + H \cdot H^T\right).$$

=> It may be assumed *without loss of generality* that

$$d := \min\{m, n\} = m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is empty if $c < \gamma^m$ and reduced to the zero matrix if $c = \gamma^m$. Assume therefore from now on that

$$c > \gamma^m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is compact.

Some topological properties of the set $\mathcal{H}_{m,n}(\gamma, c)$

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c\right\}$$

- From Sylvester's determinant identity, for any $H \in \mathbb{R}^{n\times m}$,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_n + H \cdot H^T\right).$$

=> It may be assumed *without loss of generality* that

$$d := \min\{m, n\} = m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is empty if $c < \gamma^m$ and reduced to the zero matrix if $c = \gamma^m$. Assume therefore from now on that

$$c > \gamma^m.$$

- The set $\mathcal{H}_{m,n}(\gamma, c)$ is compact.

On uniform measures

Definition

A measure is uniform (if it is Borelian and) if the measure of a ball depends only on its radius but not on the position of its center.

Theorem (Kirchheim & Preiss, 2002)

A bounded subset in $\mathbb{R}^k$ ($k \geq 1$) carries a uniform measure only if it is contained in a sphere.

On uniform measures

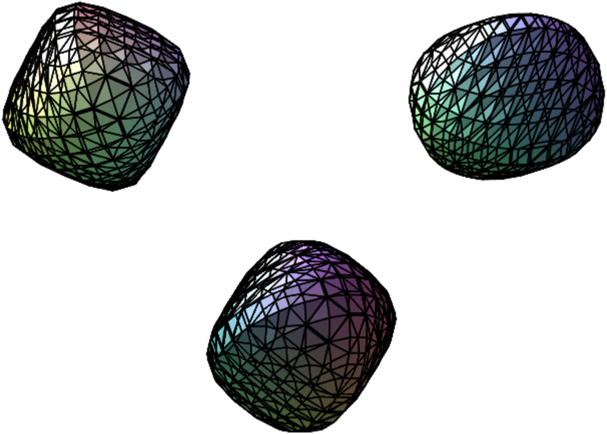
Definition

A measure is uniform (if it is Borelian and) if the measure of a ball depends only on its radius but not on the position of its center.

Theorem (Kirchheim & Preiss, 2002)

A bounded subset in $\mathbb{R}^k$ ($k \geq 1$) carries a uniform measure only if it is contained in a sphere.

Projection of the manifold $\mathcal{H}_{2,2}(1,2)$ in $\mathbb{R}^3$ (various angles of view)



=> This manifold cannot be contained in a sphere. This holds for the more general manifold $\mathcal{H}_{m,n}(\gamma, c)$ as soon as $\min\{m, n\} \geq 2$.

How to render the idea of a uniform measure ?

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \;:\; \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Clearly, given any $U \in \mathcal{O}_m(\mathbb{R})$, this set is invariant under the map $H \mapsto U \cdot H$ — this is just saying that

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_m + (UH)^T \cdot (UH)\right).$$

- From the QR decomposition, for each $H \in \mathcal{H}_{m,n}(\gamma, c)$, there exists an (essentially unique) orthogonal matrix $U \in \mathcal{O}_m(\mathbb{R})$ such that

$$UH = \begin{pmatrix} T \\ \mathbf{0} \end{pmatrix}$$

with T lying in the set $\Theta_d(\mathbb{R})$ of upper triangular matrices with size $d = m$. Furthermore, in this case,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ?

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Clearly, given any $U \in \mathcal{O}_m(\mathbb{R})$, this set is invariant under the map $H \mapsto U \cdot H$ — this is just saying that

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_m + (UH)^T \cdot (UH)\right).$$

- From the QR decomposition, for each $H \in \mathcal{H}_{m,n}(\gamma, c)$, there exists an (essentially unique) orthogonal matrix $U \in \mathcal{O}_m(\mathbb{R})$ such that

$$UH = \begin{pmatrix} T \\ \mathbf{0} \end{pmatrix}$$

with T lying in the set $\Theta_d(\mathbb{R})$ of upper triangular matrices with size $d = m$. Furthermore, in this case,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ?

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Clearly, given any $U \in \mathcal{O}_m(\mathbb{R})$, this set is invariant under the map $H \mapsto U \cdot H$ — this is just saying that

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_m + (UH)^T \cdot (UH)\right).$$

- From the QR decomposition, for each $H \in \mathcal{H}_{m,n}(\gamma, c)$, there exists an (essentially unique) orthogonal matrix $U \in \mathcal{O}_m(\mathbb{R})$ such that

$$UH = \begin{pmatrix} T \\ \mathbf{0} \end{pmatrix}$$

with T lying in the set $\Theta_d(\mathbb{R})$ of upper triangular matrices with size $d = m$. Furthermore, in this case,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ?

- Recall that

$$\mathcal{H}_{m,n}(\gamma, c) := \left\{ H \in \mathbb{R}^{n\times m} \ : \ \det\left(\gamma I_m + H^T \cdot H\right) = c \right\}.$$

- Clearly, given any $U \in \mathcal{O}_m(\mathbb{R})$, this set is invariant under the map $H \mapsto U \cdot H$ — this is just saying that

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_m + (UH)^T \cdot (UH)\right).$$

- From the QR decomposition, for each $H \in \mathcal{H}_{m,n}(\gamma, c)$, there exists an (essentially unique) orthogonal matrix $U \in \mathcal{O}_m(\mathbb{R})$ such that

$$UH = \begin{pmatrix} T \\ \mathbf{0} \end{pmatrix}$$

with T lying in the set $\Theta_d(\mathbb{R})$ of upper triangular matrices with size $d = m$. Furthermore, in this case,

$$\det\left(\gamma I_m + H^T \cdot H\right) = \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ? (bis)

- Idea : defining equivalently the "uniform" measure taking into account the geometric properties of the manifold

$$\mathcal{H}'_{m,n}(\gamma, c) := \left\{ T \in \Theta_d(\mathbb{R}) \; : \; \det\left(\gamma I_d + T^T \cdot T\right) = c \right\}.$$

- This is precisely the idea behind the concept of *volume element* $\mathrm{d}\,\mathrm{vol}(T)$ on a manifold : it defines a probability measure ν_d deduced from the formula

$$\nu_d(\mathcal{B}) = \int_{\mathcal{B}} \mathrm{d}\,\mathrm{vol}(T)$$

valid for any (measurable set) $\mathcal{B} \subset \mathcal{H}'_{m,n}(\gamma, c)$.

- Explicitely, the density $\mathrm{d}\,\mathrm{vol}(T)$ is given by

$$\mathrm{d}\,\mathrm{vol}(T) = \|(\nabla g)(T)\|_2 \cdot \left(\left(\frac{\partial g}{\partial t_{dd}} \right)(T) \right)^{-1} \cdot \mathrm{d}T,$$

where

$$g \; : T \in \Theta_d(\mathbb{R}) \mapsto \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ? (bis)

- Idea : defining equivalently the "uniform" measure taking into account the geometric properties of the manifold

$$\mathcal{H}'_{m,n}(\gamma, c) := \left\{ T \in \Theta_d(\mathbb{R}) \;:\; \det\left(\gamma I_d + T^T \cdot T\right) = c \right\}.$$

- This is precisely the idea behind the concept of *volume element* $\mathrm{d}\,\mathrm{vol}(T)$ on a manifold : it defines a probability measure ν_d deduced from the formula

$$\nu_d(\mathcal{B}) = \int_{\mathcal{B}} \mathrm{d}\,\mathrm{vol}(T)$$

valid for any (measurable set) $\mathcal{B} \subset \mathcal{H}'_{m,n}(\gamma, c)$.

- Explicitely, the density $\mathrm{d}\,\mathrm{vol}(T)$ is given by

$$\mathrm{d}\,\mathrm{vol}(T) = \|(\nabla g)(T)\|_2 \cdot \left(\left(\frac{\partial g}{\partial t_{dd}}\right)(T)\right)^{-1} \cdot \mathrm{d}T,$$

where

$$g : T \in \Theta_d(\mathbb{R}) \mapsto \det\left(\gamma I_d + T^T \cdot T\right).$$

How to render the idea of a uniform measure ? (bis)

- Idea : defining equivalently the “uniform” measure taking into account the geometric properties of the manifold

$$\mathcal{H}'_{m,n}(\gamma, c) := \left\{ T \in \Theta_d(\mathbb{R}) \ : \ \det\left(\gamma I_d + T^T \cdot T\right) = c \right\}.$$

- This is precisely the idea behind the concept of *volume element* $\mathrm{d}\,\mathrm{vol}(T)$ on a manifold : it defines a probability measure ν_d deduced from the formula

$$\nu_d\left(\mathcal{B}\right) = \int_{\mathcal{B}} \mathrm{d}\,\mathrm{vol}(T)$$

valid for any (measurable set) $\mathcal{B} \subset \mathcal{H}'_{m,n}(\gamma, c)$.

- Explicitely, the density $\mathrm{d}\,\mathrm{vol}(T)$ is given by

$$\mathrm{d}\,\mathrm{vol}(T) = \|(\nabla g)(T)\|_2 \cdot \left(\left(\frac{\partial g}{\partial t_{dd}}\right)(T)\right)^{-1} \cdot \mathrm{d}T,$$

where

$$g \ : T \in \Theta_d(\mathbb{R}) \mapsto \det\left(\gamma I_d + T^T \cdot T\right).$$

Some numerical values

- In the case that there are $d = m = 2$ users and $n = 2$ receivers, assume that the capacity of the channel is $C = 30$ bits and that $SNR = 5$ db.
- Let $\mathfrak{m}_2(s)$ denote the probability that $SNR_{eff} \geq s$:

s	1	3/2	2
$\mathfrak{m}_2(s) \geq$	0.672723	0.560289	0.489859

s	5	10	30
$\mathfrak{m}_2(s) \geq$	0.314961	0.223899	0.12972

- For instance, the initial SNR value is recovered with probability at least 31%.

Some numerical values

- In the case that there are $d = m = 2$ users and $n = 2$ receivers, assume that the capacity of the channel is $C = 30$ bits and that $SNR = 5$ db.
- Let $\mathfrak{m}_2(s)$ denote the probability that $SNR_{eff} \geq s$:

s	1	$3/2$	2
$\mathfrak{m}_2(s) \geq$	0.672723	0.560289	0.489859

s	5	10	30
$\mathfrak{m}_2(s) \geq$	0.314961	0.223899	0.12972

- For instance, the initial SNR value is recovered with probability at least 31%.

Plan

A summary of the geometric approach

- Idea : Any matrix $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = P^T \cdot D \cdot P,$$

where $P \in \mathcal{O}_d(\mathbb{R})$ and D is diagonal with determinant 1 (spectral decomposition).

- Defining a suitable class of probability measures on the set of orthogonal matrices and (above all) on the set of diagonal matrices with determinant 1 thus determines a class of probability measures in Σ_d^{++}.
- The problem amounts to determining whether a random ellipsoid centered at the origin contains a non–zero lattice points.
- The results obtained are sharp in the sense that we recover the growth in $\delta^{d/2}$ from the Theorem of Kleinbock & Margulis.
- The key problem in the proof is to evaluate the measure of the intersection between an ellipsoid and the unit sphere.

A summary of the geometric approach

- Idea : Any matrix $\Sigma \in \Sigma_d^{++}$ can be decomposed as
$$\Sigma = P^T \cdot D \cdot P,$$
where $P \in \mathcal{O}_d(\mathbb{R})$ and D is diagonal with determinant 1 (spectral decomposition).
- Defining a suitable class of probability measures on the set of orthogonal matrices and (above all) on the set of diagonal matrices with determinant 1 thus determines a class of probability measures in Σ_d^{++}.
- The problem amounts to determining whether a random ellipsoid centered at the origin contains a non–zero lattice points.
- The results obtained are sharp in the sense that we recover the growth in $\delta^{d/2}$ from the Theorem of Kleinbock & Margulis.
- The key problem in the proof is to evaluate the measure of the intersection between an ellipsoid and the unit sphere.

A summary of the geometric approach

- Idea : Any matrix $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = P^T \cdot D \cdot P,$$

where $P \in \mathcal{O}_d(\mathbb{R})$ and D is diagonal with determinant 1 (spectral decomposition).

- Defining a suitable class of probability measures on the set of orthogonal matrices and (above all) on the set of diagonal matrices with determinant 1 thus determines a class of probability measures in Σ_d^{++}.
- The problem amounts to determining whether a random ellipsoid centered at the origin contains a non–zero lattice points.
- The results obtained are sharp in the sense that we recover the growth in $\delta^{d/2}$ from the Theorem of Kleinbock & Margulis.
- The key problem in the proof is to evaluate the measure of the intersection between an ellipsoid and the unit sphere.

A summary of the geometric approach

- Idea : Any matrix $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = P^T \cdot D \cdot P,$$

where $P \in \mathcal{O}_d(\mathbb{R})$ and D is diagonal with determinant 1 (spectral decomposition).

- Defining a suitable class of probability measures on the set of orthogonal matrices and (above all) on the set of diagonal matrices with determinant 1 thus determines a class of probability measures in Σ_d^{++}.
- The problem amounts to determining whether a random ellipsoid centered at the origin contains a non–zero lattice points.
- The results obtained are sharp in the sense that we recover the growth in $\delta^{d/2}$ from the Theorem of Kleinbock & Margulis.
- The key problem in the proof is to evaluate the measure of the intersection between an ellipsoid and the unit sphere.

A summary of the geometric approach

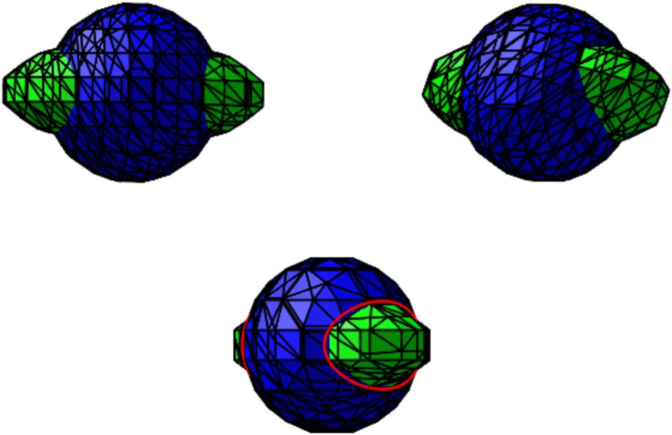
- Idea : Any matrix $\Sigma \in \Sigma_d^{++}$ can be decomposed as

$$\Sigma = P^T \cdot D \cdot P,$$

where $P \in \mathcal{O}_d(\mathbb{R})$ and D is diagonal with determinant 1 (spectral decomposition).

- Defining a suitable class of probability measures on the set of orthogonal matrices and (above all) on the set of diagonal matrices with determinant 1 thus determines a class of probability measures in Σ_d^{++}.
- The problem amounts to determining whether a random ellipsoid centered at the origin contains a non–zero lattice points.
- The results obtained are sharp in the sense that we recover the growth in $\delta^{d/2}$ from the Theorem of Kleinbock & Margulis.
- The key problem in the proof is to evaluate the measure of the intersection between an ellipsoid and the unit sphere.

Intersection of an ellipsoid with the unit sphere



- **Goal :** To compute the area (on the unit sphere) of this intersection.


Thank you