J. Math. Pures Appl. ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal de Mathématiques Pures et Appliquées

www.elsevier.com/locate/matpur

On the minimum of a positive definite quadratic form over non-zero lattice points. Theory and applications

Faustin Adiceam *,[1], Evgeniy Zorin

Department of Mathematics, University of York, York, YO10 5DD, UK

ARTICLE INFO

Article history:
Received 15 July 2016
Available online xxxx

In honorem Henriettae Dickinsonis apud Manutium in Hibernia

MSC:
11H55
11H06
94A15
11Z05

Keywords:
Quadratic forms
Lattice points
Information theory

ABSTRACT

Let Σ_d^{++} be the set of positive definite matrices with determinant 1 in dimension $d \geqslant 2$. Identifying any two $SL_d(\mathbb{Z})$-congruent elements in Σ_d^{++} gives rise to the space of reduced quadratic forms of determinant one, which in turn can be identified with the locally symmetric space $X_d := SL_d(\mathbb{Z})\backslash SL_d(\mathbb{R})/SO_d(\mathbb{R})$. Equip the latter space with its natural probability measure coming from a Haar measure on $SL_d(\mathbb{R})$. In 1998, Kleinbock and Margulis established sharp estimates for the probability that an element of X_d takes a value less than a given real number $\delta > 0$ over the non-zero lattice points $\mathbb{Z}^d\backslash\{\mathbf{0}\}$.

In this article, these estimates are extended to a large class of probability measures arising either from the spectral or the Cholesky decomposition of an element of Σ_d^{++}. The sharpness of the bounds thus obtained are also established (up to multiplicative constants) for a subclass of these measures.

Although of an independent interest, this theory is partly developed here with a view towards application to Information Theory. More precisely, after providing a concise introduction to this topic fitted to our needs, we lay the theoretical foundations of the study of some manifolds frequently appearing in the theory of Signal Processing. This is then applied to the recently introduced Integer-Forcing Receiver Architecture channel whose importance stems from its expected high performance. Here, we give sharp estimates for the probabilistic distribution of the so-called *Effective Signal-to-Noise Ratio*, which is an essential quantity in the evaluation of the performance of this model.

RÉSUMÉ

Soit Σ_d^{++} l'ensemble des matrices définies positives de déterminant 1 en dimension $d \geqslant 2$. L'espace des formes quadratiques réduites de déterminant 1 s'en déduit en identifiant les matrices $SL_d(\mathbb{Z})$-congruentes. Cet espace peut à son tour être identifié à l'ensemble localement symétrique $X_d := SL_d(\mathbb{Z})\backslash SL_d(\mathbb{R})/SO_d(\mathbb{R})$ sur lequel peut être définie une mesure de probabilité obtenue à partir d'une mesure de Haar de $SL_d(\mathbb{R})$. En 1998, Kleinbock et Margulis estimèrent de manière optimale la probabilité qu'un élément de X_d prenne une valeur inférieure à un réel $\delta > 0$ sur l'ensemble des points non nuls du réseau $\mathbb{Z}^d$.

* Corresponding author.
E-mail addresses: fadiceam@gmail.com (F. Adiceam), evgeniy.zorin@york.ac.uk (E. Zorin).
[1] Present address: Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L3G1, Canada.

https://doi.org/10.1016/j.matpur.2018.08.009

Dans cet article, ces estimations sont étendues à une large classe de mesures de probabilité définies, soit à partir de la décomposition spectrale d'un élément de Σ_d^{++}, soit à partir de sa décomposition de Cholesky. L'optimalité des bornes ainsi obtenues est également établie (à une constante multiplicative près) pour une sous-classe des mesures considérées.

Bien qu'intéressante en soi, cette théorie est en partie développée ici en considération de ses applications à la théorie de l'information. Plus précisément, à la suite d'une présentation concise et adaptée à nos besoins du sujet en question, nous posons les fondements théoriques de l'étude de quelques variétés apparaissant fréquemment en théorie du traitement du signal. Ceci est ensuite utilisé pour décrire l'*architecture du réseau à forçage aux entiers auprès du receveur* récemment élaboré et dont l'importance réside dans les hautes performances qui en sont attendues. Nous estimons ici de manière optimale la distribution probabilistique dudit *rapport signal sur bruit effectif*, qui est une grandeur fondamentale dans l'évaluation de la performance de ce modèle.

1. Introduction

Fix once and for all an integer $d \geqslant 2$. Let Q be a non-degenerate symmetric matrix in dimension d. Throughout, the matrix Q will be identified with the corresponding quadratic form $\boldsymbol{x} \in \mathbb{R}^d \mapsto {}^t\boldsymbol{x} \cdot Q \cdot \boldsymbol{x}$.

If Q is indefinite, the Oppenheim conjecture solved by Margulis states that the set of values taken by this quadratic form at non-zero integral points, viz.

$$\left\{ {}^t\boldsymbol{a} \cdot Q \cdot \boldsymbol{a} \ : \ \boldsymbol{a} \in \mathbb{Z}^d \backslash \{\boldsymbol{0}\} \right\},$$

is dense in the real line whenever $d \geqslant 3$. When $d = 2$ however (i.e. for indefinite binary quadratic forms), this set may exhibit very different structures: it may be dense or else closed and discrete, but it may also be not closed and/or not dense. For further details on the theory of values taken by an indefinite quadratic form, the reader is referred to [6,7] and to the references therein.

In the case that Q is definite, say positive definite without loss of generality, it is easy to see that the quantity

$$M_d(Q) := \min_{\boldsymbol{a} \in \mathbb{Z}^d \backslash \{\boldsymbol{0}\}} {}^t\boldsymbol{a} \cdot Q \cdot \boldsymbol{a} \tag{1}$$

is well-defined. It is a result due to Hermite (see [2, p. 43] for a proof) that one has always

$$M_d(Q) \leqslant \left(\frac{4}{3}\right)^{(d-1)/2} |Q|^{1/d}, \tag{2}$$

where $|Q|$ denotes the determinant of Q. It is known that the constant $(4/3)^{(d-1)/2}$ on the right-hand side of (2) is optimal only when $d = 2$. Denoting by $\mathcal{S}_d^{++}$ the set of positive definite matrices in dimension $d \geqslant 2$, this leads one to the definition of the *Hermite constant* γ_d:

$$\gamma_d := \frac{\sup_{Q \in \mathcal{S}_d^{++}} M_d(Q)}{|Q|^{1/d}}.$$

The supremum in this definition can actually be replaced with a maximum. Only the values of γ_d for $d = 2, 3, 4, 5, 6, 7, 8$ and $d = 24$ are exactly known. For other d's, several estimates have been established. See, e.g., [5] for proofs and further details on the Hermite constants. See also [4] for an algorithm to approximate $M_d(Q)$ for a *given* $Q \in \mathcal{S}_d^{++}$.

Please cite this article in press as: F. Adiceam, E. Zorin, On the minimum of a positive definite quadratic form over non-zero lattice points. Theory and applications, J. Math. Pures Appl. (2018), https://doi.org/10.1016/j.matpur.2018.08.009