Abstracts

Adelic quadratic spaces

Éric Gaudron
(joint work with Gaël Rémond)

We examine the links between linear and quadratic equations through the search of algebraic solutions of small heights.

0.1. The starting point is a theorem by Cassels (1955, [1]) and Davenport (1957, [3]) which asserts that if $q\colon \mathbb{Q}^n \to \mathbb{Q}$ is a non-zero isotropic quadratic form with integral coefficients $(a_{i,j})_{i,j}$ then there exists a vector $x = (x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{0\}$ such that $q(x) = 0$ and

$$\sum_{i=1}^{n} x_i^2 \leq \left(2\gamma_{n-1}^2 \sum_{i,j} a_{i,j}^2\right)^{(n-1)/2}$$

(γ_{n-1} is the Hermite constant). Our aim is to give a generalization of this statement in the context of rigid adelic spaces (introduced in the preceding talk by Gaël Rémond).

Let K be an algebraic extension of $\mathbb{Q}$ and n be a positive integer. We denote by $c_K(n)$ the supremum over all rigid adelic spaces E over K of the real numbers

$$\inf\left\{H_E(x)^n H(E)^{-1}\,;\ x \in E \setminus \{0\}\right\}$$

($H_E(x)$ and $H(E)$ are the heights of x and E with respect to the metrics on E). According to [6], the field K is called a *Siegel* field if $c_K(n) < +\infty$ for all $n \geq 1$. We have $c_{\mathbb{Q}}(n) = \gamma_n^{n/2}$,

$$c_K(n) \leq \left(n|\Delta_{K/\mathbb{Q}}|^{1/[K:\mathbb{Q}]}\right)^{n/2}$$

if K is a number field of absolute discriminant $\Delta_{K/\mathbb{Q}}$ and

$$c_{\overline{\mathbb{Q}}}(n) = \exp\left\{\frac{n}{2}\left(\frac{1}{2} + \cdots + \frac{1}{n}\right)\right\}$$

(see [6]).

An *adelic quadratic space* (E, q) over K is a rigid adelic space E/K endowed with a quadratic form $q\colon E \to K$. In this framework, several problems can be raised (here, small = of small height):

1) Existence of a small isotropic vector,
2) Existence of a small maximal totally isotropic subspace,
3) Existence of a basis of E composed of small isotropic vectors.

There exist between 25 and 30 articles in the literature dealing with these questions (essentially when K a number field or $\overline{\mathbb{Q}}$). A common divisor to these works is the notion of Siegel's lemma. We shall provide solutions to these three problems, which are optimal with respect to the height of q.

0.2. The following statement gives an answer to the problem 2.

Theorem 1. *Assume q is isotropic. Then, for all $\varepsilon > 0$, there exists a maximal totally isotropic subspace F of E of dimension $d \geq 1$ and height*

$$H(F) \leq (1+\varepsilon)c_K(n-d)\,(2H(q))^{(n-d)/2}\,H(E).$$

Here $H(q)$ is the height of q built from local operators norms (see [7]). For instance, in the context of Cassels and Davenport Theorem, one can prove that $H(q) \leq (\sum_{i,j} a_{i,j}^2)^{1/2}$. Theorem 1 generalizes and improves theorems by Schlickewei (1985, $K = \mathbb{Q}$, [9]), Vaaler (1987, K number field, [10]) and Fukshansky (2008, $K = \overline{\mathbb{Q}}$, [5]). Using a Siegel's lemma in such a subspace F, we obtain an answer to Problem 1:

Quadratic Siegel's lemma. *If q is isotropic then, for all $\varepsilon > 0$, there exists $x \in E \setminus \{0\}$ such that $q(x) = 0$ and*

$$H_E(x) \leq (1+\varepsilon)\left(c_K(n)\,(2H(q))^{(n-d)/2}\,H(E)\right)^{1/d}.$$

The proof of Theorem 1 follows from an estimate of the height of a suitable q-orthogonal symmetric of an almost minimal height subspace F (chosen among maximal totally isotropic subspaces of E) and from a Siegel's lemma used with the quotient E/F. To be interesting, Theorem 1 must be applied in a Siegel field ($c_K(n-d) < \infty$). But the converse is true: it can be also proved that to be a Siegel field is a necessary condition when a quadratic Siegel's lemma exists (take $q(x) = \ell(x)^2$ with $\ell\colon E \to K$ a linear form and use [6, § 4.8]).

0.3. Now, let us tackle the problem of a small isotropic basis of an adelic quadratic space (E,q) over a Siegel field K. Assume that there exists a nondegenerate isotropic vector in E. It is well known then that there exists a basis $(e_1,\dots,e_n)$ of E such that $q(e_i) = 0$ for all $1 \leq i \leq n$. Our goal is to have also the heights of e_i's *small.* An obvious approach rests on an induction process, choosing $e_i \in E \setminus K.e_1 \oplus \cdots \oplus K.e_{i-1}$ with small height and $q(e_i) = 0$. That leads us to the following variant of the quadratic Siegel's lemma:

1a) Let I be an ideal of the ring of polynomials of E and denote by $Z(I)$ the set of zeros $\{x \in E\,;\ \forall\, P \in I,\ P(x) = 0\}$. How to bound

$$\inf\{H_E(x)\,;\ q(x) = 0 \text{ and } x \notin Z(I)\}\ ?$$

(Quadratic Siegel's lemma avoiding an algebraic set.)

To simplify, we state our result only for the standard adelic space $E = K^n$.

Theorem 2. *Let $q\colon K^n \to K$ be a quadratic form and let I be an ideal of $K[X_1,\dots,X_n]$ generated by polynomials of (total) degree $\leq M$. Assume (i) $q \neq 0$ and (ii) $\exists\, x \notin Z(I)\,;\ q(x) = 0$. Then there exists a constant $c(n,K) \geq 1$, which depends only on n and K, such that the vector x in condition (ii) can also be chosen with height*

$$H_{K^n}(x) \leq c(n,K)M^3H(q)^{(n-d+1)/2}$$

where d is the dimension of maximal totally isotropic subspaces of (K^n, q).

The constant $c(n, K)$ can be made fully explicit (see [7, § 7]). This statement generalizes and improves previous results by Masser (1998, $K = \mathbb{Q}$, $Z(I)$ hyperplane, [8]), Fukshansky (2004, K number field, $Z(I)$ union of hyperplanes, [4]) and Chan, Fukshansky & Henshaw (2014, [2]). Moreover the exponent $(n - d + 1)/2$ of $H(q)$ is best possible: take $E = \mathbb{Q}^n$, $a, d \geq 1$ integers, $Z(I) = \{x_d = 0\}$ and

$$q(x) = 2x_{d+1}x_d - a^2x_d^2 - (x_{d+2} - ax_{d+1})^2 - \cdots - (x_n - ax_{n-1})^2.$$

We have $H(q) = \mathrm{O}_{a\to+\infty}(a^2)$ and if x is isotropic then $|x_n| \geq a^{n-d+1}|x_d|/4$. The proof of Theorem 2 relies on an avoiding Siegel's lemma and a geometric lemma. From Theorem 2 can easily be deduced a small-height isotropic basis of E.

Complete proofs and further results are given in [7].

References

[1] J. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **51** (1955), 262–264.

[2] W.K. Chan, L. Fukshansky and G. Henshaw, *Small zeros of quadratic forms outside a union of varieties*, Trans. Amer. Math. Soc. **366** (2014), 5587–5612.

[3] H. Davenport, *Note on a theorem of Cassels*, Proc. Cambridge Philos. Soc. **53** (1957), 539–540.

[4] L. Fukshansky, *Small zeros of quadratic forms with linear conditions*, J. Number Theory **108** (2004), 29–43.

[5] L. Fukshansky, *Small zeros of quadratic forms over* $\overline{\mathbb{Q}}$, Int. J. Number Theory **4** (2008), 503–523.

[6] É. Gaudron and G. Rémond, *Corps de Siegel*, J. reine angew. Math. to appear, 61 pages. `DOI: 10.1515/crelle-2014-0096`

[7] É. Gaudron and G. Rémond, *Espaces adéliques quadratiques*, 34 pages, preprint available on `http://math.univ-bpclermont.fr/~gaudron`

[8] D. Masser, *How to solve a quadratic equation in rationals*, Bull. London Math. Soc. **30** (1998), 24–28.

[9] H.P. Schlickewei, *Kleine Nullstellen homogener quadratischer Gleichungen*, Monatsh. Math. **100** (1985), 35–45.

[10] J. Vaaler, *Small zeros of quadratic forms over number fields*, Trans. Amer. Math. Soc. **302** (1987), 281–296.