Small Zeros of Quadratic Forms

with

Linear Conditions

Lenny Fukshansky

University of Texas at Austin

- Definitions and notation
- Motivation for searching for points of bounded height that satisfy arithmetic conditions
  - Lower bounds: Lehmer's Conjecture and Zhang's Theorem
  - Upper bounds: "Semi-effective" algorithm to search for solutions of polynomial equations
- Overview of the results on small zeros of quadratic forms
- D. W. Masser's result on small zeros of quadratic polynomials
- Generalization of Masser's result: Small Zeros of Quadratic Forms with Linear Conditions
- Further open questions and connections

Let K be a number field of degree d over $\mathbb{Q}$. Write $M(K)$ for the set of all places of K, and for each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, where K_v and $\mathbb{Q}_v$ are completions of K and $\mathbb{Q}$ respectively at the place v. Then if $u \in M(\mathbb{Q})$, let $M_u = \{v \in M(K) : v|u\}$, and we have

$$\sum_{v \in M_u} d_v = d.$$

We normalize our absolute values for $v \in M(K)$:

(1) if $v|p$ then $|p|_v = p^{-d_v/d}$,
(2) if $v|\infty$ then $|\alpha|_v = |\alpha|^{d_v/d}$, where $|\ |$ is the usual Euclidean absolute value on $\mathbb{R}$ or $\mathbb{C}$.

Then for every $\alpha \in K$, $\alpha \neq 0$, the product formula reads

$$\prod_v |\alpha|_v = 1.$$

Let $\boldsymbol{x} \in K_v^N$ for any $v \in M(K)$, then define:

$$|\boldsymbol{x}|_v = \max_{1 \leq i \leq N} |x_i|_v.$$

Then we have the following global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} |\boldsymbol{x}|_v.$$

For $\alpha \in K$, we also define the height of α to be

$$h(\alpha) = H(1, \alpha),$$

and finally for $\boldsymbol{x} \in K^N$, define the *inhomogeneous* height

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x}).$$

Let M, N be positive integers, and define

$$\mathcal{M} = \left\{ (i_1, ..., i_N) \in \mathbb{Z}_+^N : \sum_{j=1}^{N} i_j \leq M \right\},$$

where $\mathbb{Z}_+$ is the set of all *non-negative* integers. Let

$$F(X_1, ..., X_N) = \sum_{\boldsymbol{i} \in \mathcal{M}} f_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}} \in K[X_1, ..., X_N],$$

be a polynomial of degree M in N variables over K.
For every $v \in M(K)$, define

$$H_v(F) = \max_{\boldsymbol{i} \in \mathcal{M}} |f_{\boldsymbol{i}}|_v,$$

and then

$$H(F) = \prod_{v \in M(K)} H_v(F).$$

All the heights above are *multiplicative*. We also define the *additive* or *logarithmic* equivalents by taking log of each multiplicative height above. We denote this by writing h^+, H^+ instead of h, H respectively.

Lehmer's Conjecture, 1933. *There exists an absolute constant C_1 such that whenever $\alpha \neq 0$ or root of 1, is an algebraic number of degree d over $\mathbb{Q}$, then*

$$h^+(\alpha) > \frac{C_1}{d}.$$

The best known result in this direction is the following.

Theorem 1 (Dobrowolski, 1979). *Notation as in the conjecture, then if $d \geq 3$ there exists an absolute constant C_2 such that*

$$h^+(\alpha) > \frac{C_2}{d}\left(\frac{\log(\log(d))}{\log(d)}\right)^3.$$

Another direction to work in is try to place some arithmetic conditions on algebraic numbers and see if better lower bounds can be obtained.

Theorem 2 (Zhang, 1992). *There exists an absolute constant C_3 such that whenever x, y are algebraic numbers (not 0 or cube roots of 1) and $x + y + 1 = 0$, then*

$$h^+(x) + h^+(y) > C_3 > 0.$$

Theorem 3 (Zagier, 1993). *In Zhang's theorem,*

$$C_3 = \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right).$$

More generally than that, we have the following.

Theorem 4 (Schmidt, 1996). *Let $F(X_1, ..., X_N)$ be a polynomial of degree M in N variables with integer coefficients. Let $x_1, ..., x_N$ be non-zero algebraic numbers such that*

$$F(x_1, ..., x_N) = 0, \quad F(1/x_1, ..., 1/x_N) \neq 0.$$

Then

$$\sum_{i=1}^{N} h^+(x_i) \geq \frac{1}{2^{4M+2N} H(F)}.$$

These results provide certain motivation for studying lower bounds of algebraic points that satisfy various arithmetic conditions.

What about upper bounds?

Property of Heights. *Let K be a number field, C a positive constant, N a positive integer. Then the set*

$$S_C^N(K) = \left\{ \boldsymbol{x} \in K^N : H(\boldsymbol{x}) \leq C \right\},$$

has finite cardinality.

Suppose one can show that if a polynomial $F(X_1, ..., X_N)$ with coefficients in a number field K has a zero in K, then it has such a zero of bounded height, and determine an explicit upper bound on height of such a zero in terms of $H(F)$. This would produce an explicit "search bound" on zeros of F in K due to the above property of heights. This approach is not entirely effective, although various bounds on the cardinality of the set $S_C^N(K)$ are known: for instance, asymptotic results due to Schanuel (1963, 1979).

There was a large amount of work done in this direction, starting from the celebrated Siegel's Lemma, which answers a similar question for a system of M linear forms in N variables, $N > M$.

Siegel's Lemma (Bombieri, Vaaler, 1983). *Let $L_1, ..., L_M$ be M linear forms in N variables with coefficients in a number field K. Then there exists $\mathbf{0} \neq \boldsymbol{x} \in K^N$ such that $L_i(\boldsymbol{x}) = 0$ for each $1 \leq i \leq M$, and*

$$H(\boldsymbol{x}) \leq C(K, N, M) \left\{ \prod_{i=1}^{M} H(L_i) \right\}^{1/(N-M)}.$$

Remark. The actual result of Bombieri and Vaaler is considerably stronger than this. Among other things, they produce an explicit constant $C(K, N, M)$. Other (more recent) important results along the lines of Siegel's Lemma include an "absolute version" over $\overline{\mathbb{Q}}$ by Roy and Thunder (1996), where the solution is searched for in any algebraic extensions of K, and the constant does not depend on K, and another version over a number field by Vaaler (2002), where the best possible constant is produced: the exponent in the upper bound is best possible in the Bombieri-Vaaler original result.

Next we consider quadratic forms and quadratic polynomials. Let

$$F(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i Y_j,$$

be a symmetric bilinear form, and let

$$F(\boldsymbol{X}) = F(\boldsymbol{X}, \boldsymbol{X}),$$

be the associated quadratic form in N variables. First suppose the coefficients f_{ij} are in $\mathbb{Z}$.

Theorem 5 (Cassels, 1955). *Suppose F is isotropic over $\mathbb{Q}$. Then there exists $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^N$ such that $F(\boldsymbol{x}) = 0$, and*

$$H(\boldsymbol{x}) \leq \left(3N^2 H(F)\right)^{\frac{N-1}{2}}.$$

This result of Cassels has been generalized to number fields by S. Raghavan (1975). There was quite a number of further extensions and generalizations over the years, in particular by Birch, Davenport, Chalk, Schmidt, Schlikewei, Vaaler, and others.

Now suppose that the coefficients of our quadratic (bilinear) form F come from a number field K, and let O_K be the ring of integers of K. The following version of Cassels' original theorem in the number field case follows from a result of Vaaler.

Theorem 6 (Vaaler, 1987). *If F has a nontrivial zero in K^N, then there exists $\mathbf{0} \neq \boldsymbol{x} \in O_K^N$ such that $F(\boldsymbol{x}) = 0$, and*

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) \leq A_K(N-1)H(F)^{(N-1)/2},$$

where for every positive integer j,

$$A_K(j) = \left\{2^{5j}(j+1)^j |\Delta_K|^{\frac{j+1}{d}}\right\}^{1/2} \prod_{v \in M(K)} r_v(j)^{\frac{jd_v}{d}}.$$

In the theorem above some notation needs to be clarified. First of all, Δ_K is the discriminant of K and d is the degree of K.
Now for each $v \in M(K)$, and a positive integer j define

(1) $r_v(j) = \pi^{-1/2}\Gamma(j/2+1)^{1/j}$, if $v|\infty$ is real,
(2) $r_v(j) = (2\pi)^{-1/2}\Gamma(j+1)^{1/2j}$, if $v|\infty$ is complex,
(3) $r_v(j) = 1$, if $v \nmid \infty$.

where Γ is the Gamma-function.

Next, Masser generalized Cassels' result over rationals to inhomogeneous quadratic polynomials. Let

$$P(X_1, ..., X_N) = \sum_{i=1}^{N}\sum_{j=1}^{N} f_{ij}X_iX_j + \sum_{i=1}^{N} f_{0j}X_j + f_{00}$$

be an inhomogeneous quadratic polynomial in N variables with rational coefficients. Let

$$F(X_0, ..., X_N) = \sum_{i=0}^{N}\sum_{j=0}^{N} f_{ij}X_iX_j$$

be a quadratic form in $N+1$ variables with rational coefficients.

Then

$$H(P) = H(F),$$

and P vanishes at some $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Q}^N$ if and only if F vanishes at $(1, \boldsymbol{x})$, where

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}) = H(1, \boldsymbol{x}).$$

Therefore Masser proves the existence of rational zeros of P of small height by means of proving the following theorem.

Theorem 7 (Masser, 1998). *Suppose F is a quadratic form in $N+1$ variables with rational coefficients, and assume that there exists $\boldsymbol{x} = (x_0, ..., x_N) \in \mathbb{Q}^{N+1}$ with $x_0 \neq 0$ such that $F(\boldsymbol{x}) = 0$. Then there exists such a point $\boldsymbol{x}$ with*

$$H(\boldsymbol{x}) \leq \left(3(N+1)^2 H(F)\right)^{(N+1)/2}.$$

Notice that the condition $X_0 \neq 0$ is a non-vanishing condition on a very simple linear form. We generalize Masser's result in the following way. For positive integers M, N and number field K, define

$$B_K(N, M) = \frac{1}{1152}(N+1)^2 A_K(N) \left\{ \frac{27}{2}(N+1)^6 A_K(N)^2 \right\}^{M-1} \times$$
$$\times (M+2)! \{(M+3)!\}^2,$$

with $A_K(N)$ as in Theorem 6 above. Then we have the following.

Theorem 8 (F., 2003). *Let M, N be positive integers. Let*

$$F(X_0, ..., X_N) = \sum_{i=0}^{N} \sum_{j=0}^{N} f_{ij} X_i X_j$$

be a quadratic form in $N+1$ variables with coefficients in a number field K of degree d over $\mathbb{Q}$, and

$$L_1(X_0, ..., X_N), ..., L_M(X_0, ..., X_N)$$

be linear forms in $N+1$ variables with coefficients in K. Suppose that there exists $\mathbf{0} \neq \boldsymbol{x} \in K^{N+1}$ such that $F(\boldsymbol{x}) = 0$, and $L_i(\boldsymbol{x}) \neq 0$ for each $1 \leq i \leq M$. Then there exists such a point in O_K^{N+1} with

$$H(\boldsymbol{x}) \leq B_K(N, M) H(F)^{\frac{N+2M}{2}+(M-1)(N+2)}, \tag{1}$$

as well as

$$H(\boldsymbol{x}) \leq B_K(N, M) H(F)^{\frac{N+1}{2}+(M-1)(N+2)} \prod_{i=1}^{M} H(L_i)^{\frac{(2M-1)N}{M}}, \tag{2}$$

and finally

$$H(\boldsymbol{x}) \leq B_K(N, M) H(F)^{\frac{2N+2M+1}{4}+(M-1)(N+2)} \prod_{i=1}^{M} H(L_i)^{\frac{(2M-1)N}{2M}}. \tag{3}$$

Thus Theorem 8 assumes the existence of a zero of F outside of a collection of N-dimensional subspaces in K^{N+1}, and proves the existence of such a zero of *bounded height*.

Notice that if $M = 1$ and $L_1(\boldsymbol{X}) = X_0$, then (2) reduces to

$$H(\boldsymbol{x}) \leq 3(N+1)^2 A_K(N) H(F)^{(N+1)/2},$$

which is a direct generalization of Masser's Theorem 7 over K.

Another interesting consequence of Theorem 8 in case $M = 1$ is the following.

Corollary 9. *Let $F(\boldsymbol{X})$ be a quadratic form in $N+1$ variables with coefficients in the number field K, as above. Let*

$$\mathcal{V}_K(F) = \left\{ \boldsymbol{t} \in K^{N+1} : F(\boldsymbol{t}) = 0 \right\}.$$

Suppose that there exists a non-singular point $\mathbf{0} \neq \boldsymbol{x} \in \mathcal{V}_K(F)$. Then there exists a non-singular point $\mathbf{0} \neq \boldsymbol{u} \in \mathcal{V}_K(F)$ such that

$$H(\boldsymbol{u}) \leq \max\{3, A_K(N)\} \; H(F)^{\frac{N}{2}}.$$

Proof of this is a little involved. However, a weaker bound

$$H(\boldsymbol{u}) \leq \left(3(N+1)^2 H(F)\right)^{(N+1)/2}$$

follows directly from Theorem 8 as follows.

Proof. For each $0 \leq i \leq N$, define a linear form

$$L_i(\boldsymbol{X}) = \frac{\partial F}{\partial X_i}(\boldsymbol{X}) \in K[X_0, ..., X_N].$$

Let $\mathbf{0} \neq \boldsymbol{x}$ be a non-singular point in $\mathcal{V}_K(F)$.
Then $F(\boldsymbol{x}) = 0$, $L_i(\boldsymbol{x}) \neq 0$ for some $0 \leq i \leq N$.
Hence let $M = 1$, and the result follows by (1) of Theorem 8. $\square$

Sketch of the proof of Theorem 8. We argue by induction on M.

If $M = 1$, then our argument is a generalization of Masser's argument:

- Argue by induction on N. The case $N = 1$ is simple.
- Start with a point $\boldsymbol{x}$ of small height at which F vanishes - the existence of such a point is guaranteed by Theorem 6. Assume that $L_1(\boldsymbol{x}) = 0$.
- If $\boldsymbol{x}$ is a non-singular point in the variety of F, then construct a point $\boldsymbol{t}$ with coordinates $0, \pm 1$ such that $L_1(\boldsymbol{t}), F(\boldsymbol{x}, \boldsymbol{t}) \neq 0$, and let

$$\boldsymbol{y} = F(\boldsymbol{t})\boldsymbol{x} - 2F(\boldsymbol{x}, \boldsymbol{t})\boldsymbol{t}.$$

  It is easy to check that $F(\boldsymbol{y}) = 0$, $L_1(\boldsymbol{y}) \neq 0$.
  It is also not difficult to estimate the height of $\boldsymbol{y}$, since $H(\boldsymbol{t}) = 1$, and we have an upper bound on $H(\boldsymbol{x})$.
- If $\boldsymbol{x}$ is a singular point in the variety of F, then reduce to fewer variables and use induction hypothesis.

Suppose $M \geq 2$, and that theorem has been proved for any subset of $L_1, ..., L_M$ of k linear forms, where $1 \leq k \leq M - 1$.
Then there exist points $\boldsymbol{x}, \boldsymbol{y} \in K^{N+1}$ such that

$$F(\boldsymbol{x}) = F(\boldsymbol{y}) = 0, \quad L_i(\boldsymbol{x}) \neq 0 \ \ \forall\ 1 \leq i \leq M - 1,\ L_M(\boldsymbol{y}) \neq 0,$$

and $h(\boldsymbol{x}), h(\boldsymbol{y})$ are bounded. The existence of these points is guaranteed by induction hypothesis.
If $L_M(\boldsymbol{x}) \neq 0$ or $L_i(\boldsymbol{y}) \neq 0$ for all $1 \leq i \leq M - 1$, then we are done. So assume it is not so. Then there exists a k, such that $1 \leq k < M - 1$ and, by reordering the linear forms if necessary, we have

(1) $L_i(\boldsymbol{x}) \neq 0$, $L_i(\boldsymbol{y}) \neq 0$, for all $1 \leq i \leq k$,
(2) $L_i(\boldsymbol{x}) \neq 0$, $L_i(\boldsymbol{y}) = 0$, for all $k < i \leq M - 1$,
(3) $L_M(\boldsymbol{x}) = 0$, $L_M(\boldsymbol{y}) \neq 0$.

There exists a positive integer β such that for all $1 \leq i \leq M$,

$$L_i(\boldsymbol{x} \pm \beta \boldsymbol{y}) \neq 0,$$

for the same choice of $\pm$. For this, β needs to be such that for the same choice of $\pm$ none of the linear equations in β

$$L_i(\boldsymbol{x}) \pm \beta L_i(\boldsymbol{y}) = 0, \quad 1 \leq i \leq k \leq M-2,$$

are true. There are at most $M-2$ such equations, and since we can also choose $\pm$, there exists such a β so that

$$1 \leq \beta \leq \left[\frac{M-2}{2}\right] + 1 \leq \frac{M}{2}. \tag{4}$$

Define

$$\boldsymbol{u} = \boldsymbol{x} \pm \beta \boldsymbol{y},$$

for this choice of $\pm$ and β.

Case 1. Suppose $F(\boldsymbol{x}, \boldsymbol{y}) = 0$. Then

$$F(\boldsymbol{u}) = F(\boldsymbol{x}) + \beta^2 F(\boldsymbol{y}) \pm 2\beta F(\boldsymbol{x}, \boldsymbol{y}) = 0,$$

and

$$L_i(\boldsymbol{u}) \neq 0, \quad \forall\ 1 \leq i \leq M.$$

Case 2. Suppose $F(\boldsymbol{x}, \boldsymbol{y}) \neq 0$. We need the following auxiliary result.

Lemma 10. *Let $U(\boldsymbol{X})$ be a polynomial in $l \geq 1$ variables of degree $j \geq 1$ with coefficients in a number field K. Suppose that $U(\boldsymbol{X})$ is not identically 0. Then there exists a point $\boldsymbol{w} \in \mathbb{Z}^l$ such that $U(\boldsymbol{w}) \neq 0$, and*

$$h(\boldsymbol{w}) \leq |\boldsymbol{w}| \leq \left[\frac{j}{2}\right] + 1.$$

Proof. Induction on l. The idea for an argument was suggested to me by Professor S. David. □

We can take $l = N + 1$, $j = M$,

$$U(\boldsymbol{X}) = \prod_{i=1}^{M} L_i(\boldsymbol{X}),$$

and conclude that there exists $\boldsymbol{w} \in K^{N+1}$ such that $L_i(\boldsymbol{w}) \neq 0$ for each $1 \leq i \leq M$ and

$$h(\boldsymbol{w}) \leq \frac{M+2}{2}.$$

If $F(\boldsymbol{w}) = 0$, we are done. Assume it is not so. Let β be a positive integer, and define

$$\boldsymbol{u} = F(\boldsymbol{y} \pm \beta\boldsymbol{w})\boldsymbol{x} - 2F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w})(\boldsymbol{y} \pm \beta\boldsymbol{w}).$$

Notice that $F(\boldsymbol{u}) = 0$. We want to choose $\pm\beta$ in such a way that the following is true:

(1) $F(\boldsymbol{y} \pm \beta\boldsymbol{w}) = \beta(\beta F(\boldsymbol{w}) \pm 2F(\boldsymbol{y}, \boldsymbol{w})) \neq 0$,
(2) $F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w}) = F(\boldsymbol{x}, \boldsymbol{y}) \pm \beta F(\boldsymbol{x}, \boldsymbol{w}) \neq 0$,
(3) $L_i(\boldsymbol{u}) = F(\boldsymbol{y} \pm \beta\boldsymbol{w})L_i(\boldsymbol{x}) - 2F(\boldsymbol{x}, \boldsymbol{y} \pm \beta\boldsymbol{w})(L_i(\boldsymbol{y}) \pm \beta L_i(\boldsymbol{w})) \neq 0$, for each $1 \leq i \leq M$.

It is not difficult to see that (1), (2), (3) amount to a total of 2 linear and M quadratic expressions in β. Selecting $\pm$ appropriately we see that there exists a positive integer β such that (1), (2), (3) are satisfied, and

$$\beta \leq M + 2.$$

Finally we need the following two lemmas to estimate heights of the points we constructed.

Lemma 11. *Let $\boldsymbol{x}, \boldsymbol{y} \in K^N$, and α, β be positive integers, then*

$$H(\alpha\boldsymbol{x} \pm \beta\boldsymbol{y}) \leq h(\alpha\boldsymbol{x} \pm \beta\boldsymbol{y}) \leq (\alpha + \beta)h(\boldsymbol{x})h(\boldsymbol{y}).$$

Lemma 12. *If $\boldsymbol{t}, \boldsymbol{w} \in K^{N+1}$, and $\boldsymbol{u} = F(\boldsymbol{t})\boldsymbol{w} - 2F(\boldsymbol{t}, \boldsymbol{w})\boldsymbol{t}$, then*

$$H(\boldsymbol{u}) \leq h(\boldsymbol{u}) \leq 3(N+1)^2 H(F)h(\boldsymbol{w})h(\boldsymbol{t})^2.$$

Proofs of these lemmas are not difficult. Also, while approximating the heights of our points, we keep in mind that the ordering of the linear forms is arbitrary, hence we take an average over a subgroup of M-cycles in the permutation group S_M. This completes the argument. $\square$

What is the next step in the same direction?

- Let $F(\boldsymbol{X})$ and $G(\boldsymbol{X})$ be two quadratic forms in N variables with coefficients in a number field K, and suppose they have a simultaneous non-trivial zero over K. Prove that they have one of bounded height.
- Let $F(\boldsymbol{X})$ be a homogeneous polynomial of degree $M > 2$ in N variables with coefficients in a number field K, and suppose it has a non-trivial zero over K. Prove that it has one of bounded height. How do we do it for any $M > 2$, say for $M = 3$?

Both of these seem to be very difficult questions. To the best of my knowledge, nothing has yet been done in any of these directions.

This sort of questions also seems to have a certain analogy with the arithmetic version of Bezout's Theorem (as stated, for instance, by Bost, Gillet, Soule, or by Laurent and Roy). This is a theorem that provides an upper bound on the height of the intersection cycle of two varieties in terms of the heights of these varieties (for an appropriately defined notion of height for a variety and a cycle). Our problems, however, are about providing an upper bound for the height of a point in a projective variety in terms of the height of this variety. This seems to be a considerably more difficult question in general.

Aknowledgement. I would like to thank my advisor, Professor J. D. Vaaler, for suggesting this problem to me, and for his many valuable comments and conversations on the subject of this work.