Canad. Math. Bull. Vol. **52** (1), 2009 pp. 63–65

Small Zeros of Quadratic Forms Avoiding a Finite Number of Prescribed Hyperplanes

Rainer Dietmann

Abstract. We prove a new upper bound for the smallest zero $\mathbf{x}$ of a quadratic form over a number field with the additional restriction that $\mathbf{x}$ does not lie in a finite number of m prescribed hyperplanes. Our bound is polynomial in the height of the quadratic form, with an exponent depending only on the number of variables but not on m.

In 1955, Cassels [2] proved his famous result on small zeros of quadratic forms:

If $Q(X_1, \dots, X_s)$ is an integral quadratic form having an integer zero $\mathbf{x} \neq 0$, then there is such a zero $\mathbf{x}$ where $|\mathbf{x}| \ll_s |Q|^{(s-1)/2}$.

Here $|\cdot|$ denotes the maximum norm for vectors, or the largest modulus of the coefficients of Q (the 'height'), respectively. Recently, Masser [6] obtained the following generalization about small zeros avoiding a prescribed hyperplane:

If there is an integer zero $\mathbf{x}$ of Q with $x_1 \neq 0$, then there is such a zero $\mathbf{x}$ with $|\mathbf{x}| \ll_s |Q|^{s/2}$.

Both Masser's and Cassels' results are best possible, apart from the implied O-constant. More recently, Fukshansky [4] obtained a further generalization by allowing for a finite number of linear conditions, and also by allowing for a general number field K. His result is that if $L_1, \dots, L_m$ are K-linear forms and there is a K-rational $\mathbf{x}$ with $Q(\mathbf{x}) = 0$ and $L_i(\mathbf{x}) \neq 0$ $(1 \leq i \leq m)$, then there is such an $\mathbf{x}$ with

$$H(\mathbf{x}) \ll \min \Big\{ H(Q)^{\frac{s-1+2m}{2}+(m-1)(s+1)}, \quad H(Q)^{\frac{s}{2}+(m-1)(s+1)} \prod_{i=1}^{m} H(L_i)^{\frac{(2m-1)(s-1)}{m}}, \quad H(Q)^{\frac{2s+2m-1}{4}+(m-1)(s+1)} \prod_{i=1}^{m} H(L_i)^{\frac{(2m-1)(s-1)}{2m}} \Big\},$$

where the implied O-constant can be explicitly given and depends only on s, m, and the number field K, and where H denotes the homogeneous global height (for the definition of H and the inhomogeneous height h see [4] or [7]). For $m = 1$ and $L_1(X_1, \dots, X_s) = X_1$, Fukshansky's bound reduces to Masser's apart from O-constants, but for $m > 1$ one might ask if stronger bounds are possible.

Received by the editors July 31, 2006; revised December 3, 2006.
AMS subject classification: Primary: 11D09; secondary: 11E12, 11H46, 11H55.

https://doi.org/10.4153/CMB-2009-007-7 Published online by Cambridge University Press

Theorem *Let $Q(X_1, \dots, X_s) \in K[X_1, \dots, X_s]$ be a quadratic form, and let*

$$L_i(X_1, \dots, X_s) \in K[X_1, \dots, X_s] \ (1 \leq i \leq m)$$

be linear forms. Suppose that there is an $\mathbf{x} \in K^s$ with $Q(\mathbf{x}) = 0$ and $L_i(\mathbf{x}) \neq 0$ $(1 \leq i \leq m)$. Then there is such an $\mathbf{x}$ with $H(\mathbf{x}) \ll H(Q)^{(s+1)/2}$. The implied O-constant depends only on s, m, and the number field K.

This improves Fukshansky's result for $m > 1$. Moreover, one obtains a bound which depends on m only as far as the implied O-constant is concerned, and which could easily be calculated by some extra work.

To prove the theorem we distinguish three different cases.

Case I The quadratic form Q has rank at least three, and Q has a non-singular K-rational zero. Then by [4, Corollary 1.2] (see also its proof) there is such a non-singular zero $\mathbf{x} \in K^s$ with $h(\mathbf{x}) \ll H(Q)^{(s-1)/2}$. In particular, the linear form $\mathbf{y} \mapsto Q(\mathbf{x}, \mathbf{y})$ is not identically zero (here we used the notation Q also for the bilinear form associated to Q). Now it is easily seen (compare [3, page 89]) that for any $\mathbf{y} \in \mathbb{Z}^s$ the vector $\mathbf{z} = Q(\mathbf{y})\mathbf{x} - 2Q(\mathbf{x}, \mathbf{y})\mathbf{y}$ is again a zero of Q. Fix i; then $L_i(\mathbf{z})$ cannot be zero, for all possible choices of $\mathbf{y}$. Indeed, if $L_i(\mathbf{x}) \neq 0$, then $L_i(\mathbf{z})$ cannot be zero for all $\mathbf{y}$, for otherwise we would have

$$Q(\mathbf{y}) = \frac{2Q(\mathbf{x}, \mathbf{y})L_i(\mathbf{y})}{L_i(\mathbf{x})}$$

for all $\mathbf{y}$, thus the quadratic form $Q(\mathbf{y})$ could be written as a product of the two linear forms $\mathbf{y} \mapsto 2Q(\mathbf{x}, \mathbf{y})/L_i(\mathbf{x})$ and $L_i(\mathbf{y})$, contrary to our assumption that Q has rank at least three. On the other hand, if $L_i(\mathbf{x}) = 0$, then again $L_i(\mathbf{z}) = -2Q(\mathbf{x}, \mathbf{y})L_i(\mathbf{y})$ cannot be zero for all $\mathbf{y}$ because $\mathbf{y} \mapsto Q(\mathbf{x}, \mathbf{y})$ is not the zero linear form, and the same is clearly true for $L_i(\mathbf{y})$. So since the two linear forms are not identically zero, both of their nullspaces have co-dimension one in K^s, and hence we can always pick a point in K^s outside of their union. Consequently, $F(\mathbf{y}) := L_1(\mathbf{z}) \cdots L_m(\mathbf{z})$ is not the zero polynomial in $\mathbf{y}$. Thus by [4, Theorem 3.1] there is an $\mathbf{y} \in \mathbb{Z}^s$ with $F(\mathbf{y}) \neq 0$ and $|\mathbf{y}| \ll 1$. Hence $\mathbf{z}$ is a zero of Q with $L_i(\mathbf{z}) \neq 0$ $(1 \leq i \leq m)$, and using [4, Lemma 2.3] we conclude that $H(\mathbf{z}) \ll H(Q)h(\mathbf{x})h(\mathbf{y})^2 \ll H(Q)^{(s+1)/2}$, which completes the proof in Case I.

Case II All K-rational zeros of Q are singular. Then the set of K-rational zeros of Q is a K-linear space V, because if $\mathbf{x}, \mathbf{y} \in K^s$ are singular zeros of Q, then $Q(\mathbf{x}, \mathbf{y}) = 0$, hence $Q(\mathbf{x} + \mathbf{y}) = Q(\mathbf{x}) + 2Q(\mathbf{x}, \mathbf{y}) + Q(\mathbf{y}) = 0$, so $\mathbf{x} + \mathbf{y}$ is again a zero of Q. Let n be the dimension of V. Now by [7, Corollary 2] there is a basis $\mathbf{x}_1, \dots, \mathbf{x}_n \in K^s$ of V where

$$\prod_{i=1}^{n} h(\mathbf{x}_i) \ll H(Q)^{(s-1)/2}.$$

(Note that if Q is identically zero, then by [4, Theorem 3.1] there exists $\mathbf{x} \in K^s$ with $H(\mathbf{x}) \ll 1$ such that $\prod_{i=1}^{m} L_i(\mathbf{x}) \neq 0$ since the linear forms are not identically zero, and we are done. Hence we may assume that Q is not identically zero, so $L < M$

https://doi.org/10.4153/CMB-2009-007-7 Published online by Cambridge University Press

in the notation of [7] and [7, Corollary 2] is applicable.) By assumption, there is an $\mathbf{x} \in K^s$ with $L_i(\mathbf{x}) \neq 0$ $(1 \leq i \leq m)$, so the polynomial

$$F(\xi_1, \dots, \xi_n) = \prod_{i=1}^{m} L_i(\xi_1 \mathbf{x}_1 + \dots + \xi_n \mathbf{x}_n)$$

is not the zero polynomial in $\xi_1, \dots, \xi_n$. Again by [4, Theorem 3.1] we conclude that there are $\xi_1, \dots, \xi_n \in \mathbb{Z}$ with $|\xi| \ll 1$ and $F(\xi_1, \dots, \xi_n) \neq 0$. Consequently, $\mathbf{x} = \xi_1 \mathbf{x}_1 + \dots + \xi_n \mathbf{x}_n$ is a K-rational zero of Q since $\mathbf{x} \in V$, and $L_i(\mathbf{x}) \neq 0$ $(1 \leq i \leq m)$ since $F(\xi_1, \dots, \xi_n) \neq 0$, and finally $H(\mathbf{x}) \leq h(\mathbf{x}) \ll h(\mathbf{x}_1) \cdots h(\mathbf{x}_n) \ll H(Q)^{(s-1)/2}$. This proves the theorem in Case II. Note that we only introduced the inhomogeneous height h because the inequality $h(\mathbf{x}) \ll h(\mathbf{x}_1) \cdots h(\mathbf{x}_n)$ we were using would not be true if h were replaced by H.

Case III The quadratic form Q has rank at most two, and Q has a non-singular K-rational zero. Then Q is of the form $Q(X_1, \dots, X_s) = M_1(X_1, \dots, X_s) M_2(X_1, \dots, X_s)$ for two K-linear forms M_1 and M_2, which are not identically zero because we assume that Q has a non-singular K-rational zero. So the set of K-rational zeros of Q is the union of V_1 and V_2 where $V_i = \{\mathbf{x} \in K^s : M_i(\mathbf{x}) = 0\}$ $(1 \leq i \leq 2)$. By assumption, there is an $\mathbf{x} \in K^s$ with $Q(\mathbf{x}) = 0$, but $L_i(\mathbf{x}) \neq 0$ $(1 \leq i \leq m)$. Without loss of generality we may assume that $\mathbf{x} \in V_1$. Now by [5, Chapter 3, Proposition 2.4] we have $H(M_1)H(M_2) \ll H(M_1 M_2)$ where $M_1 M_2 = Q$. Hence $H(M_1) \ll H(Q)$. By Siegel's Lemma (see [1, Theorem 9]) there is a basis $\mathbf{x}_1, \dots, \mathbf{x}_{s-1}$ for the K-linear space of K-rational zeros of the linear form M_1 such that

$$\prod_{i=1}^{s-1} h(\mathbf{x}_i) \ll H(M_1) \ll H(Q).$$

We can now continue analogously to Case II. This completes the proof of the theorem.

Acknowledgment The author wants to thank the referee for carefully reading the manuscript.

References

[1] E. Bombieri and J. Vaaler, *On Siegel's lemma.* Invent. Math. **73**(1983), no. 1, 11–32.

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

[3] ———, *Rational quadratic forms.* London Mathematical Society Monographs 13, Academic Press, London-New York, 1978.

[4] L. Fukshansky, *Small zeros of quadratic forms with linear conditions.* J. Number Theory **108**(2004), no. 1, 29–43.

[5] S. Lang, *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[6] D. W. Masser, *How to solve a quadratic equation in rationals.* Bull. London Math. Soc. **30**(1998), no. 1, 24–28.

[7] J. D. Vaaler, *Small zeros of quadratic forms over number fields.* Trans. Amer. Math. Soc. **302**(1987), no. 1, 281–296.

Institut für Algebra und Zahlentheorie, Pfaffenwaldring 57, D-70550 Stuttgart, Germany
e-mail: dietmarr@mathematik.uni-stuttgart.de