Proceedings of the Edinburgh Mathematical Society (1982) 25, 269–277 ©

SMALL FRACTIONAL PARTS OF QUADRATIC FORMS

by R. C. BAKER and G. HARMAN*

(Received 11th February 1981)

1. Introduction

Let $\|x\|$ denote the distance of x from the nearest integer. In 1948 H. Heilbronn proved [5] that for $\varepsilon>0$ and $N>c_1(\varepsilon)$ the inequality

$$\min_{1\leqq n\leqq N}\|\alpha n^2\|<N^{-(1/2)+\varepsilon}$$

holds for any real α. This result has since been generalised in many different directions, and we consider here extensions of the type: *For* $\varepsilon>0$, $N>c_2(\varepsilon,s)$ *and a quadratic form* $Q(x_1,\dots,x_s)$ *there exist integers* $n_1,\dots,n_s$ *not all zero with* $|n_1|,\dots,|n_s|\leqq N$ *and with*

$$\|Q(n_1,\dots,n_s)\|<N^{-c_3(s)+\varepsilon}. \tag{1}$$

Danicic obtained a result of this type [2] with $c_3(s)=s/(s+1)$. Cook was able to get (1) with $c_3(s)=1$ for an additive form in two variables [1]. More recently, Schinzel, Schlickewei and Schmidt have shown [7] that $c_3(s)$ may be taken as the maximum of

$$2\left(1+\frac{1}{h}+\frac{4}{s-h+1}\right)^{-1}$$

over odd h in $1\leqq h\leqq(s+5)/3$. Taking h asymptotically equal to $s/3$ gives

$$c_3(s)=2-(18/s)+O(1/s^2).$$

This result improves on Danicic's for $s\geqq7$ and, as is well known, the "limiting" exponent -2 is best possible. The new idea in [7] is the use of an auxiliary result on quadratic congruences. For a different approach to the limiting result $c_3(s)\to2$, see [9].

In the present note we refine the method of [7] to prove

Theorem. *Let* $s\geqq3$ *and let* $Q(x_1,\dots,x_s)$ *be a real quadratic form. Then there is a constant* $c_4(s)$ *such that for every integer* $N\geqq2$ *there are integers* $n_1,\dots,n_s$ *with*

$$0<\max(|n_1|,\dots,|n_s|)\leqq N, \tag{2}$$

*Written while the second author held a University of London postgraduate studentship.

having

$$\|Q(n_1,\ldots,n_s)\|<c_4(s)(N/\log N)^{-c_5(s)}. \tag{3}$$

Here

$$c_5(s)=\begin{cases} 2s/(s+5) & \textit{for odd } s,\\ 2s(s-1)/(s^2+4s-4) & \textit{for even } s. \end{cases} \tag{4}$$

Our exponent is the same as Danicic's for $s=3$, apart from the substitution of a power of $\log N$ for N^ε. For $s\geqq 4$, our exponent is better than that of [2] or [7], and (4) gives

$$c_5(s)=2-(10/s)+O(1/s^2).$$

The second author has refined the method further for diagonal quadratic forms; for example, one can take $c_5(5)=9/8$ and $c_5(11)=3/2$ in this special case.

The key to the improvement on [7] is Lemma 1, below. This is a straightforward extension of the congruence result of [7], but enables us to introduce successive minima explicitly. This is more economical; the procedure is analogous to that of Davenport and Ridout [4].

2. Quadratic congruences

Lemma 1. *Let $Q(\mathbf{x})=Q(x_1,\ldots,x_h)$ be a quadratic form in an odd number h of variables with integer coefficients. Let m be a natural number. Let $K_1,\ldots,K_h$ be positive reals with*

$$K_1\ldots K_h\geqq m^{(h+1)/2}. \tag{5}$$

Then there are integers $x_1,\ldots,x_h$ not all zero, with

$$Q(x_1,\ldots,x_h)\equiv 0 \qquad (\operatorname{mod} m), \tag{6}$$

and having

$$|x_i|\leqq K_i \qquad (i=1,\ldots,h). \tag{7}$$

The case $K_1=\ldots=K_h=m^{(1/2)+(1/2h)}$ is Theorem 1 of [7].

Proof. We first observe that the result is trivial if $K_i\geqq m$ for some i; hence we suppose that

$$K_i<m \qquad (i=1,\ldots,h) \tag{8}$$

Clearly we may assume that $m>1$, and that m is square free. For any m may be written in the form

$$m=r^2a$$

where a is square free. If $K_1\dots K_h \geqq m^{(h+1)/2}$, then $(K_1/r)\dots(K_h/r)\geqq a^{(h+1)/2}$. A solution $(y_1,\dots,y_h)$ of $Q(\mathbf{y})\equiv 0 \pmod a$, with $|y_i|\leqq K_i/r$, yields a solution $x_i=ry_i$ of (5) satisfying (7).

Let $d=(h-1)/2$. According to [7], for every prime p dividing m there are integer vectors $\mathbf{r}_1^{(p)},\dots,\mathbf{r}_d^{(p)}$ which are linearly independent modulo p, and for which

$$Q(s_1\mathbf{r}_1^{(p)}+\dots+s_d\mathbf{r}_d^{(p)})\equiv 0 \qquad \pmod p$$

whenever $s_1,\dots,s_d$ are integers. By the Chinese remainder theorem there are integer vectors $\mathbf{r}_1,\dots,\mathbf{r}_d$ having

$$\mathbf{r}_i\equiv \mathbf{r}_i^{(p)} \qquad \pmod p$$

for each prime p dividing m. Write $\mathbf{r}_i=(r_{i1},\dots,r_{ih})$.

By Minkowski's linear forms theorem, and taking account of (5), there are integers $s_1,\dots,s_d$, $z_1,\dots,z_h$ not all zero, with

$$|s_i|<m, \qquad (i=1,\dots,d) \tag{9}$$

$$\left|\sum_{k=1}^{d} s_k r_{kj}+mz_j\right|\leqq K_j \quad (j=1,\dots,h). \tag{10}$$

Put $\mathbf{x}=s_1\mathbf{r}_1+\dots+s_d\mathbf{r}_d+m\mathbf{z}$, where $\mathbf{z}=(z_1,\dots,z_h)$. Then clearly (6) holds, and (7) follows from (10). Since $K_j<m$ we easily see that $(s_1,\dots,s_h)\neq\mathbf{0}$, say $s_1\neq 0$. Since m is square free, there is a prime factor p of m with $s_1\not\equiv 0 \pmod p$. Because $\mathbf{r}_1,\dots,\mathbf{r}_d$ are linearly independent $(\mathrm{mod}\, p)$, we have $\mathbf{x}\not\equiv 0 \pmod p$. Thus $\mathbf{x}\neq 0$.

3. A lemma on exponential sums

The following lemma was pointed out to us by H. L. Montgomery. Compared with the familiar Lemma 12 of [8], Chapter I, it saves a great deal of work, and a small power of $\log N$, farther on.

Lemma 2. *Let L, M be natural numbers and let $\alpha_1,\alpha_2,\dots,\alpha_M$ be real numbers such that $\|\alpha_n\|\geqq L^{-1}$ $(n=1,\dots,M)$. Then we have*

$$\sum_{l=1}^{L}\left|\sum_{n=1}^{M} e(l\alpha_n)\right|\geqq M/6.$$

Proof. Let $J=(L^{-1},1-L^{-1})$ with indicator function $X_J(x)$. According to Montgomery [**6**], p. 559, there is a function $b\in L^1(R)$ such that

$$b(x)\geqq X_J(x),\quad \hat{b}(0)=|J|+L^{-1} \tag{11}$$

$$\hat{b}(t)=0 \quad \text{for} \quad |t|\geqq L. \tag{12}$$

By an easy calculation, the function

$$B(x)=\sum_n b(x+n)$$

is in $L^1(0,1)$ with Fourier series $\sum_{|k|\leqq L}\hat{b}(k)e(kx)$, hence

$$B(x)=\sum_{|k|\leqq L}\hat{b}(k)e(kx). \tag{13}$$

Note that for integral $k\neq 0$, (13) implies

$$|\hat{b}(k)|\leqq\int_0^1|B(x)-1|\,dx\leqq\int_0^1\{(B(x)-1)+2(1-X_J(x))\}\,dx$$

$$=\hat{b}(0)+1-2|J|=3L^{-1}. \tag{14}$$

Combining (11), (13) and (14) with the hypothesis $\|\alpha_n\|\geqq L^{-1}$, we obtain

$$M\leqq\sum_{n=1}^{M}B(\alpha_n)\leqq M\hat{b}(0)+\sum_{0<|k|\leqq L}|\hat{b}(k)|\left|\sum_{n=1}^{M}e(k\alpha_n)\right|$$

$$\leqq M\hat{b}(0)+6L^{-1}\sum_{k=1}^{L}\left|\sum_{n=1}^{M}e(k\alpha_n)\right|.$$

Since $1-\hat{b}(0)=L^{-1}$, the desired inequality follows.

4. Proof of the theorem

The proof will be by contradiction. Suppose that there are no integers $n_1,\dots,n_s$ satisfying (2) and (3). Let

$$S(l)=\sum_{n_1=1}^{N}\cdots\sum_{n_s=1}^{N}e(lQ(n_1,\dots,n_s)).$$

Let

$$L=[2c_4(s)^{-1}(N/\log N)^{c_5(s)}]$$

where $c_4(s)$ is sufficiently large, then from Lemma 2 with $M=N^s$ we have

$$\sum_{l=1}^{L} |S(l)| \geqq N^s/6.$$

Let l be a natural number, $1 \leqq l \leqq L$, having

$$|S(l)| \geqq N^s/6L. \tag{15}$$

We define linear forms $L_1, \ldots, L_s$ with symmetric coefficient matrix via the identity

$$Q(x_1, \ldots, x_s) = x_1 L_1(\mathbf{x}) + \ldots + x_s L_s(\mathbf{x}).$$

Let $M_1, \ldots, M_s$ be the first s successive minima of the convex body described by

$$\left.\begin{array}{r} |2lL_j(\mathbf{x}) - x_{s+j}| < N^{-1} \\ |x_j| < N \end{array}\right\} \qquad (j = 1, \ldots, s),$$

with respect to the integer lattice in $2s$-dimensional space. It is established in the proof of Lemma 5 of [3] that

$$|S(l)|^2 \leqq c_6(s)(M_1 \ldots M_s)^{-1} N^s (\log N)^s.$$

In view of (15), then,

$$(M_1 \ldots M_s)^{-1} \geqq c_7(s) L^{-2} N^s (\log N)^{-s}. \tag{16}$$

We now consider the cases of odd and even s separately.

Case I. Odd s. By the definition of successive minima, we can find s linearly independent integer vectors $\mathbf{r}'_\mu$ in $2s$-dimensional space with

$$|2lL_j(\mathbf{r}_\mu) - r_{j+s,\mu}| < N^{-1} M_\mu, \tag{17}$$

$$|r_{j\mu}| < NM_\mu \tag{18}$$

for $j = 1, \ldots, s$, $\mu = 1, \ldots, s$. Here $\mathbf{r}'_\mu = (r_{1\mu}, \ldots, t_{2s,\mu})$ and $\mathbf{r}_\mu = (r_{1\mu}, \ldots, r_{s\mu})$.

Let us write

$$K_\mu = c_7(s)^{-1/s} L^{2/s} (2l)^{(s+1)/2s} M_\mu^{-1} (\log N) N^{-1}, \tag{19}$$

then

$$K_1 \ldots K_s \geqq (2l)^{(s+1)/2} \tag{20}$$

from (16). We also write

$$\theta_{\mu\nu}=2l\sum_{j=1}^{s} r_{j\mu}L_j(\mathbf{r}_\nu) \qquad (\mu, \nu=1,\dots,s),$$

so that

$$\|\theta_{\mu\nu}\|<sM_\mu M_\nu \tag{21}$$

from (17) and (18). Let $b_{\mu\nu}$ be integers with

$$\|\theta_{\mu\nu}\|=|\theta_{\mu\nu}-b_{\mu\nu}| \qquad (\mu, \nu=1,\dots,s). \tag{22}$$

By Lemma 1 and (20) there are integers $x_1,\dots,x_s$ not all zero, with

$$|x_\mu|\leqq K_\mu \qquad (\mu=1,\dots,s) \tag{23}$$

and

$$\sum_{\mu=1}^{s}\sum_{\nu=1}^{s} b_{\mu\nu}x_\mu x_\nu\equiv 0 \qquad (\mathrm{mod}\ 2l). \tag{24}$$

Put $n_i=\sum_{\mu=1}^{s} r_{i\mu}x_\mu$ for $i=1,\dots,s$. Then

$$\begin{aligned}Q(n_1,\dots,n_s)&=\sum_{\mu=1}^{s}\sum_{\nu=1}^{s}\left(\sum_{i=1}^{s} L_i(\mathbf{r}_\mu)r_{i\nu}\right)x_\mu x_\nu\\&=(2l)^{-1}\sum_{\mu=1}^{s}\sum_{\nu=1}^{s}\theta_{\mu\nu}x_\mu x_\nu\\&=(2l)^{-1}\sum_{\mu=1}^{s}\sum_{\nu=1}^{s} b_{\mu\nu}x_\mu x_\nu+(2l)^{-1}\sum_{\mu=1}^{s}\sum_{\nu=1}^{s}(\theta_{\mu\nu}-b_{\mu\nu})x_\mu x_\nu.\end{aligned} \tag{25}$$

The first sum on the right-hand side of (25) is an integer, in view of (24). Thus

$$\begin{aligned}\|Q(n_1,\dots,n_s)\|&\leqq(2l)^{-1}\sum_{\mu=1}^{s}\sum_{\nu=1}^{s}\|\theta_{\mu\nu}\||x_\mu||x_\nu|\\&<\frac{s}{2l}\sum_{\mu=1}^{s}\sum_{\nu=1}^{s} M_\mu M_\nu K_\mu K_\nu\\&=\frac{s^3}{2l}(c_7(s))^{-2/s}L^{4/s}(2l)^{(s+1)/s}(\log N)^2N^{-2}\end{aligned}$$

https://doi.org/10.1017/S0013091500016758 Published online by Cambridge University Press

from (21) and (23). For sufficiently large $c_4(s)$, we have

$$\|Q(n_1,\ldots,n_s)\| < 2s^3(c_7(s))^{-2/s}L^{5/s}(N/\log N)^{-2}$$
$$< L^{-1}.$$

Moreover, we have

$$|n_i| = \left|\sum_{\mu=1}^{s} r_{i\mu}x_\mu\right| \leqq sM_\mu NK_\mu$$
$$\leqq sc_7(s)^{-1/s}L^{2/s}(2l)^{(s+1)/2s}\log N$$
$$\leqq 2sc_7(s)^{-1/s}L^{(s+5)/2s}\log N < N.$$

By hypothesis, then, we must have

$$(n_1,\ldots,n_s) = \mathbf{0},$$

so that $\sum_{\mu=1}^{s} x_\mu \mathbf{r}_\mu = \mathbf{0}$ and consequently

$$\sum_{\mu=1}^{s} x_\mu L_j(\mathbf{r}_\mu) = \mathbf{0} \qquad (j=1,\ldots,s). \tag{26}$$

Combining (26) with (17) we obtain

$$\left|\sum_{\mu=1}^{s} x_\mu r_{j+s,\mu}\right| < N^{-1}\sum_{\mu=1}^{s} M_\mu |x_\mu|$$
$$\leqq N^{-1}\sum_{\mu=1}^{s} M_\mu K_\mu < 1$$

as we already saw above. Hence

$$\sum_{\mu=1}^{s} x_\mu r_{j\mu} = 0$$

is true not only for $j=1,\ldots,s$ but for $j=s+1,\ldots,2s$ also. This contradicts the linear independence of $\mathbf{r}'_1,\ldots,\mathbf{r}'_\mu$.

Thus the theorem is proved in Case I.

Case II. Even s. From (16) and $M_1 \leqq \ldots \leqq M_s$, we obtain

$$(M_1 \ldots M_{s-1})^{-1} \geqq c_7(s)^{(s-1)/s}L^{-2(s-1)/s}(N/\log N)^{s-1}. \tag{27}$$

Let $\mathbf{r}'_\mu$, $\mathbf{r}_\mu$, $\theta_{\mu\nu}$, $b_{\mu\nu}$ be as in Case I. By repeating the argument of Case I, with $s-1$ instead of s, we obtain integers $x_1, \ldots, x_{s-1}$ such that

$$\sum_{\mu=1}^{s-1} \sum_{\nu=1}^{s-1} b_{\mu\nu} x_\mu x_\nu \equiv 0 \qquad (\bmod 2l)$$

and

$$|x_\mu| \leqq H_\mu = c_8(s) L^{2/s} (2l)^{s/2(s-1)} M_\mu^{-1} (\log N) N^{-1}.$$

After all,

$$H_1 \ldots H_{s-1} \geqq (2l)^{((s-1)/2)+1/2}$$

provided that $c_8(s)$ is sufficiently large. Let

$$(n_1, \ldots, n_s) = \sum_{\mu=1}^{s-1} x_\mu \mathbf{r}_\mu.$$

Continuing as before, we obtain for $\|Q(n_1, \ldots, n_s)\|$ the upper bound

$$\frac{s^3}{2l} \left(\max_{1 \leqq \mu \leqq s-1} H_\mu M_\mu \right)^2 \leqq c_9(s) L^{(4/s)+(1/(s-1))} (\log N)^2 N^{-2}$$

$$< L^{-1}, \tag{28}$$

and

$$\max(|n_1|, \ldots, |n_s|) \leqq s \max_{1 \leqq \mu \leqq s-1} H_\mu M_\mu N$$

$$\leqq c_{10}(s) L^{(2/s)+(s/2(s-1))} \log N < N, \tag{29}$$

for a suitable choice of $c_4(s)$. The argument used in Case I can be repeated to obtain

$$\sum_{\mu=1}^{s-1} x_\mu \mathbf{r}'_\mu = \mathbf{0},$$

which is a contradiction. This proves the theorem in Case II.

REFERENCES

1. R. J. Cook, On the fractional parts of an additive form, *Proc. Camb. Philos. Soc.* **72** (1972), 209–212.

2. I. Danicic, An extension of a theorem of Heilbronn, *Mathematika* **5** (1958), 30–37.

3. H. Davenport, Indefinite quadratic forms in many variables (II), *Proc. London Math. Soc.* (3) **8** (1958), 109–126.

4. H. DAVENPORT and D. RIDOUT, Indefinite quadratic forms, *Proc. London Math. Soc.* (3) **9** (1959), 544–555.

5. H. HEILBRONN, On the distribution of the sequence $\theta n^2 \pmod 1$, *Quart. J. Math.* **19** (1948), 249–256.

6. H. L. MONTGOMERY, The analytic principle of the large sieve, *Bull. Amer. Math. Soc.* **84** (1978), 547–567.

7. A. SCHINZEL, H.-P. SCHLICKEWEI and W. M. SCHMIDT, Small solutions of quadratic congruences and small fractional parts of quadratic forms, *Acta Arithmetica* **37** (1980), 241–248.

8. I. M. VINOGRADOV, *The Method of Trigonometric Sums in the Theory of Numbers* (Wiley–Interscience, New York, 1954).

9. R. J. COOK, Small fractional parts of quadratic forms in many variables, *Mathematika* **27** (1980), 25–29.

ROYAL HOLLOWAY COLLEGE
EGHAM
SURREY