ACTA ARITHMETICA
158.3 (2013)

Correlations of representation functions of binary quadratic forms

by

Lilian Matthiesen (Bristol)

The purpose of this short note is to extend previous work on linear correlations of representation functions of positive definite binary quadratic forms to allow indefinite forms.

1. Introduction. The purpose of this note is to extend previous results from [9] on linear correlations of representation functions of positive definite binary quadratic forms to allow indefinite forms. Let $f : \mathbb{Z}^2 \to \mathbb{Z}$ be a primitive binary quadratic form whose discriminant is not a square. The latter assumption is equivalent to the assertion that f does not factor over $\mathbb{Q}$. Thus f is irreducible and there is no non-trivial representation of 0. Let $\mathcal{E}_f$ denote the group of automorphs of f and define the representation function $r_f : \mathbb{Z} \to \mathbb{N}_0$ by

$$r_f(n) = |\{(x,y) \in \mathbb{Z}^2/\mathcal{E}_f : f(x,y) = n\}|.$$

We shall assume familiarity with the notation from [9]. Generalising the main result from [9], our aim is to establish the following theorem.

Theorem 1.1. *Let $f_1, \dots, f_t$ be primitive irreducible binary quadratic forms. We further assume that every definite form is positive definite. For each f_i let r_{f_i} denote the representation function defined above, and let D_i be the discriminant of f_i. If $D_i < 0$, let $\mathrm{w}(D_i) = 6, 4, 2$ according as $D_i = -3, -4$ or $D_i < -4$. If $D_i > 0$, let ε_i denote the fundamental unit of $\mathbb{Q}(\sqrt{D_i})$.*

Let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \to \mathbb{Z}^t$ be a system of affine linear forms such that no two forms ψ_i and ψ_j are affinely dependent, and suppose that $K \subset [-N, N]^d \subset \mathbb{R}^d$ is a convex body such that $\psi_i(K) \geq 0$ whenever f_i is positive definite. Then

$$\sum_{n \in \mathbb{Z}^d \cap K} r_{f_1}(\psi_1(n)) \dots r_{f_t}(\psi_t(n)) = \beta_\infty \prod_p \beta_p + o(N^d),$$

2010 *Mathematics Subject Classification*: Primary 11N37; Secondary 11E25.
Key words and phrases: binary quadratic form, pseudorandomness, correlation.

DOI: 10.4064/aa158-3-4

where the implicit constant may depend on $D_1, \dots, D_t$ and the coefficients of Ψ. The local factors are given by

$$\beta_\infty = \mathrm{vol}(K) \prod_{i:D_i<0} \frac{2\pi}{\mathrm{w}(D_i)\sqrt{-D_i}} \prod_{j:D_j>1} \frac{\log \varepsilon_j}{\sqrt{D_j}},$$

$$\beta_p = \lim_{m\to\infty} \mathbb{E}_{a\in(\mathbb{Z}/p^m\mathbb{Z})^d} \prod_{i=1}^{t} \frac{\rho_{f_i,\psi_i(a)}(p^m)}{p^m},$$

with $\rho_{f,A}(q)$ denoting the local number of representations of $A \pmod q$ by f, that is,

$$\rho_{f,A}(q) := |\{(x,y) \in (\mathbb{Z}/q\mathbb{Z})^2 : f(x,y) \equiv A \pmod q\}|.$$

Theorem 1.1 provides a useful tool in the study of several Diophantine problems. It is instrumental, for example, in recent joint work [1] of the author with Browning and Skorobogatov on the Hasse principle and weak approximation for conic bundle surfaces. Generalising work of Heath-Brown [7, Theorem 2], it can also be used to study the set of $\mathbb{Q}$-rational points on varieties $X \subset \mathbb{P}^{2r+1}$ of the form

$$Q_i(Y_i, Z_i) = L_i(U,V)M_i(U,V), \qquad 1 \le i \le r.$$

Here each Q_i is an irreducible binary quadratic form over $\mathbb{Q}$, and L_i, M_i form a set of pairwise non-proportional linear forms defined over $\mathbb{Q}$. Mimicking the approach of Heath-Brown who dealt with the case $r = 2$ when $Q_i(Y,Z) = Y^2+Z^2$ for $i = 1, 2$, it would be straightforward to deduce from Theorem 1.1 that the set $X(\mathbb{Q})$ is Zariski dense in X as soon as there exists a non-singular $\mathbb{Q}$-rational point. It is worth stressing that very little is known about the arithmetic of intersections of $r \ge 3$ quadratics when the ambient projective dimension n is small. A notable exception is found in work of Skorobogatov [11] who handles the question of weak approximation when $r = 3$ and $n \ge 11$, under suitable hypotheses.

Following the strategy from [8, 9], we deduce Theorem 1.1 by means of the machinery Green and Tao developed in [3, 4, 5], in connection with Green, Tao and Ziegler's inverse theorem for the uniformity norms [6]. In fact, it will be possible to modify the approach from [9], adapting only few parts. We therefore restrict attention to these changes, referring the reader to [9] for details regarding the remaining parts.

Our main tasks in establishing Theorem 1.1 are then to construct a pseudorandom majorant for r_f when f is indefinite, to show that a suitably W-tricked version r'_f of this function is Gowers-uniform, and to check that the linear forms and correlation estimates are valid across the different majorants from the definite and indefinite cases.

Theorem 1.1 can be extended to reducible forms. If f is a form of discriminant 1, then the representation function of f is given by $\frac{1}{2}\tau(n) = \frac{1}{2}\sum_{d\in\mathbb{N}} 1_{d|n}$

for non-zero integers n. If the discriminant is a square greater than 1, then the representation function is a restricted divisor function. In both cases, the majorant function from [8] can be employed. The W-trick is compatible with the one used for irreducible forms. The proof of the linear forms condition can be adapted without difficulties (although this is a tedious task and will not be treated here).

All implicit constants in this paper are allowed to depend on the discriminants $D_1, \dots, D_t$ and the coefficients of Ψ.

2. Representation by indefinite forms. Let $f(x,y) = ax^2 + bxy + cy^2 = \langle a,b,c\rangle$ be a primitive indefinite form whose discriminant is not a square. In order to obtain a more explicit expression for r_f than that given in the introduction, we proceed to fix a fundamental domain $K_0 \subset \mathbb{R}^2$ for the action of the group of automorphs. This will allow us to write

$$r_f(n) = |\{(x,y) \in K_0 : f(x,y) = n\}|.$$

Let $D = b^2 - 4ac$ denote the discriminant of f and let $\varepsilon = \frac{1}{2}(t_0 + u_0\sqrt{D})$ be the fundamental unit of $\mathbb{Q}(\sqrt{D})$, that is, (t_0, u_0) is the solution of $t^2 - Du^2 = 4$ for which u_0 is minimal under the condition $t_0, u_0 > 0$. Then (cf. [10, §9.3]) the automorph

$$T_0 := \frac{1}{2}\begin{pmatrix} t_0 - bu_0 & 2au_0 \\ -2cu_0 & t_0 + bu_0 \end{pmatrix}$$

generates the group $\mathcal{E}_f = \{\pm T_0^n : n \in \mathbb{Z}\}$. In what follows we restrict attention to positive n; on replacing f by $-f$, this also covers the case of representation of negative integers by f. Since equivalent forms have identical representation functions, we may assume that $f = \langle a,b,c\rangle$ satisfies $|b| \le \min(|a|,|c|) \le \frac{1}{2}\sqrt{D}$ and $a > 0 > c$. Thus, either $\langle a,b,c\rangle$ or $\langle c,b,a\rangle$ is reduced. The automorph T_0 takes the line $\{y = 0\}$ to $\{y = \theta x\}$ for $\theta = -2cu_0/(t_0 - bu_0)$. Observe that θ is bounded in terms of D, and satisfies $\theta > 0$ since $c < 0$ and $t_0 - bu_0 > t_0 - \sqrt{D}u_0 > 0$. Let

$$K_0 \subset \{(x,y) \in \mathbb{R}^2 : x > 0,\ y \ge 0\}$$

be the cone defined by the lines $\{y = 0\}$ and $\{y = \theta x\}$. Then

$$r_f(n) = |\{(x,y) \in K_0 \cap \mathbb{N}^2 : f(x,y) = n\}|$$

for $n > 0$.

If $K_0(N) := \{(x,y) \in K_0 : f(x,y) \le N\}$, then (cf. [10, §10, Lemma 3.5])

$$\mathrm{vol}(K_0(N)) = N\frac{\log \varepsilon}{\sqrt{D}}.$$

Thus, the analogue of [9, Lemma 4.1] is the following.

LEMMA 2.1. *Let $q > 0$ and A be integers and let $P := \{n \le N : n \equiv A \pmod q\}$ be an arithmetic progression. Then the average of r_f along P satisfies*

$$\mathbb{E}_{n\in P}\, r_f(n) = \frac{\log\varepsilon}{\sqrt{D}}\,\frac{\rho_{f,A}(q)}{q} + O(|P|^{-1/2}q^2).$$

3. W-trick and pseudorandom majorant. As in the definite case, r_f has the arithmetic representation

$$r_f(n) = \sum_{d|n} \chi_D(d)$$

for non-zero n which are coprime to D. All non-archimedean results that are recorded in [9, §§5–6] carry over to indefinite forms directly, as is to be expected since definiteness and indefiniteness are archimedean properties. In particular,

$$r_f(n) \ll \sum_{d|n} \chi_D(d)$$

holds for any non-zero integer n. This allows us to employ a majorant of the exact same form as in the definite case (see [9, §2, §7.2]).

Let $C_1 > 1$ be the parameter that appears in the divisor function majorant [9, Proposition 2.3] and assume it to be sufficiently large for the conclusion of [9, Lemma 3.3] to hold. We then define, as in the definite case, $\overline{W} := \prod_{p<w(N)} p^{\alpha(p)}$, where $w(N) = \log\log N$ and $p^{\alpha(p)-1} < \log^{C_1+1} N \le p^{\alpha(p)}$. For integers $0 \le A < \overline{W}$, write $r_{f,A}(n) := r_f(\overline{W}n+A)$. If $\rho_{f,A}(\overline{W}) > 0$, we may in view of Lemma 2.1 define the normalised function $r'_{f,A} : \mathbb{N} \to \mathbb{R}_{\ge 0}$ by

$$r'_{f,A}(n) := \left(\frac{\log\varepsilon}{\sqrt{D}}\,\frac{\rho_{f,A}(\overline{W})}{\overline{W}}\right)^{-1} r_{f,A}(n).$$

Since the major arc estimate [9, Proposition 7.4] only builds on non-archimedean properties, it continues to hold for indefinite forms f:

LEMMA 3.1. *Let $P \subseteq [N/\overline{W}]$ be a progression of $w(N)$-smooth common difference q_1 and let $0 < A < \overline{W}$ be such that $\rho_{f,A}(\overline{W}) > 0$ and $A \not\equiv 0 \pmod{p^{\alpha(p)}}$ for all primes $p < w(N)$. If $P = \{q_1 m + q_0 : 0 \le m < M\}$ has length M, then*

$$\mathbb{E}_{n\in P}\, r'_{f,A}(n) = \mathbb{E}_{0\le m<M}\, r'_{f,A}(q_1 m + q_0) = 1 + O\left(\frac{\overline{W}(\overline{W}q_1)^2}{M^{1/2}}\right).$$

Lemma 3.1 shows that the same W-trick works for definite and indefinite forms and reduces matters to studying the functions $r'_{f,A}$ and their majorants $\nu'_{D,\gamma}(\overline{W}n + A)$ defined in [9, §7.2].

If all forms in the collection $f_1, \dots, f_t$ are irreducible, then the required linear forms and correlation estimates for the corresponding $\overline{W}$-tricked versions of the majorants follow word by word the proofs in [9, §9]. Some minor changes would be required if reducible forms are included.

4. The non-correlation estimate. Let $h : \mathbb{N} \to \mathbb{C}$ be an arithmetic function. In order to prove that

$$\mathbb{E}_{n \le N}\, h(n) F(g(n)\Gamma) = o_{s,d,G/\Gamma,\|F\|_{\mathrm{Lip}}}(1)$$

for all s-step nilmanifolds G/Γ and polynomial nilsequences $(F(g(n)\Gamma))_{n\in\mathbb{N}}$ of degree d on it, it usually suffices to show that such an estimate holds when $\int_{G/\Gamma} F = 0$ and when the nilsequence is equidistributed in some quantitative sense. This strategy was introduced by Green and Tao in [4] and employed in [9], although several modifications were necessary in the latter case. The strategy that was used for $h(n) = r'_{f,A}(n)$ in the case of definite forms f continues to apply in the indefinite case with the only changes concerning the final part of the argument carried out in [9, §18]. Let $0 < q \ll N^{o(1)}$ be a $w(N)$-smooth integer, let $r \in \{0, \dots, q\}$ and set $N'' := [(N - \overline{W}r - b)/q\overline{W}]$. In [9, §18] we split the summation

$$\mathbb{E}_{n \le N''}\, r_f(\overline{W}(qn + r) + b) F(g(n)\Gamma) = \frac{1}{N''} \sum_{\substack{x,y\ge 0:\, f(x,y)\le N,\\ f(x,y)\equiv \overline{W}r+b \,(\mathrm{mod}\, q\overline{W})}} F\left(g\left(\frac{f(x,y) - \overline{W}r - b}{q\overline{W}}\right)\Gamma\right)$$

into ranges where either x or y is fixed, while the free variable varies over a long enough interval for an analogue of Weyl's inequality to apply.

If f is indefinite, this part needs to be adapted since the region

$$K_0 \cap \{(x, y) : f(x, y) \le \overline{W}qN'' + \overline{W}r + b\},$$

which we are summing over, has a different shape. Let (x_0, y_0) be the point of intersection of $\{y = \theta x, x > 0\}$ and $\{f(x, y) = \overline{W}qN'' + \overline{W}r + b\}$, and let $x_1 > 0$ be the positive solution to $f(x_1, 0) = \overline{W}qN'' + \overline{W}r + b$. Observe that x_1 exists since we assumed that $a > 0$. Let $\kappa = 2\max(x_0, x_1)$, and consider the region

$$K_1 = \{(x, y) : 0 \le x \le \kappa,\ 0 \le y \le \min(\theta x, y_0)\}.$$

Introducing the notation

$$H(x, y) := 1_{f(x,y)\equiv \overline{W}r+b \,(\mathrm{mod}\, q\overline{W})} F\left(g\left(\frac{f(x,y) - \overline{W}r - b}{q\overline{W}}\right)\Gamma\right),$$

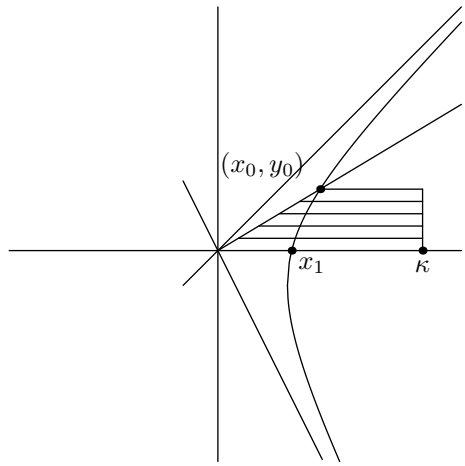

Fig. 1. The summation is split into individual sums for fixed y. Each such sum is expressed as the difference of two sums over a longer range.

we may now split our given summation as follows:

$$\begin{aligned}
&\frac{1}{N''}\sum_{\substack{(x,y)\in K_0:\\ f(x,y)\le N}} H(x,y)\\
&\qquad = \frac{1}{N''}\Bigg(\sum_{(x,y)\in K_1} H(x,y) - \sum_{\substack{(x,y)\in K_1:\\ f(x,y)>\overline{W}qN''+\overline{W}r+b}} H(x,y)\Bigg)\\
&\qquad = \frac{1}{N''}\sum_{0\le y\le y_0}\Bigg(\sum_{y/\theta<x\le\kappa} H(x,y) - \sum_{\substack{y/\theta<x\le\kappa\\ f(x,y)>\overline{W}qN''+\overline{W}r+b}} H(x,y)\Bigg).
\end{aligned}$$

The next aim is to apply Weyl's inequality for nilsequences to the latter sums over x for fixed y. The automorph T_0 carries $(x_1, 0)$ to (x_0, y_0), hence $x_0 \asymp_D x_1$. The relevant nilsequences therefore arise as polynomial subsequences of $(g(n)\Gamma)_{n\le CN}$ for some $C = O_D(1)$. In [9] we only considered equidistribution properties of the sequence $(g(n)\Gamma)_{n\le N}$ and polynomial subsequences thereof. For an application of Weyl's inequality, analogous to the one carried out in [9, §18], it thus remains to justify that for any $C = O(1)$ there exists a positive integer $C' = O(1)$ such that $(g(n)\Gamma)_{n\le CN}$ is totally $\delta^{1/C'}$-equidistributed if $(g(n)\Gamma)_{n\le N}$ is totally δ-equidistributed. We shall deduce this assertion from Green and Tao's quantitative Leibman theorem [5, Theorem 2.9].

Let m be the dimension of G/Γ and let d be the degree of the filtration $G_\bullet$ with respect to which the polynomial sequence g is defined. Suppose that

$(g(n)\Gamma)_{n\le N}$ is totally δ-equidistributed, where $\delta = \delta(N) \in (0,1)$ satisfies $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. By [9, Proposition 14.3] there is $B > 0$, $B = O_{m,d}(1)$, such that $(\eta \circ g(n))_{n\le N}$ is totally $\delta^{1/B}$-equidistributed for every horizontal character η of modulus $|\eta| \le \delta^{-1/B}$. By [9, Proposition 14.2(b)] and the definition of the smoothness norm [5, Definition 2.7], there is a positive integer $B' = O_{m,d}(1)$ such that

$$\|k\eta \circ g\|_{C^\infty[N]} \ge \delta^{-1/B'}$$

for all positive integers $k \le \delta^{-1/B'}$. Suppose that $k\eta \circ g : \mathbb{N}_0 \to \mathbb{R}/\mathbb{Z}$ has the representation $(k\eta \circ g)(n) = \sum_{j=0}^{d} \alpha_j n^j$. Then

$$\|k\eta \circ g\|_{C^\infty[N]} = \sup_{1\le j\le d} N^j \|\alpha_j\| \asymp_C \sup_{1\le j\le d} (CN)^j \|\alpha_j\| = \|k\eta \circ g\|_{C^\infty[CN]}.$$

Thus $\|k\eta \circ g\|_{C^\infty[CN]} \gg \delta^{-1/B'}$ for all $k \le \delta^{-1/B'}$. By [5, Theorem 2.9], there therefore is some integer $B'' > 0$, $B'' = O_{m,d}(1)$, such that $(g(n)\Gamma)_{n\le CN}$ is totally $\delta^{1/B''}$-equidistributed. This completes the proof of the assertion.

Acknowledgements. The author is grateful to Tim Browning for comments on an earlier draft of this paper.

While working on this paper the author was supported by EPSRC grant number EP/E053262/1.

References

[1] T. D. Browning, L. Matthiesen and A. N. Skorobogatov, *Rational points on pencils of conics and quadrics with many degenerate fibres*, arXiv:1209.0207.

[2] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. 167 (2008), 481–547.

[3] B. Green and T. Tao, *Linear equations in primes*, Ann. of Math. 171 (2010), 1753–1850.

[4] B. Green and T. Tao, *The Möbius function is strongly orthogonal to nilsequences*, Ann. of Math. 175 (2012), 541–566.

[5] B. Green and T. Tao, *The quantitative behaviour of polynomial orbits on nilmanifolds*, Ann. of Math. 175 (2012), 465–540.

[6] B. Green, T. Tao and T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$ norm*, Ann. of Math. 176 (2012), 1231–1372.

[7] D. R. Heath-Brown, *Linear relations amongst sums of two squares*, in: Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser. 303, Cambridge Univ. Press, Cambridge, 2003, 133–176.

[8] L. Matthiesen, *Correlations of the divisor function*, Proc. London Math. Soc. 104 (2012), 827–858.

[9] L. Matthiesen, *Linear correlations amongst numbers represented by positive definite binary quadratic forms*, Acta Arith. 154 (2012), 235–306.

[10] H. E. Rose, *A Course in Number Theory*, 2nd ed., Oxford Sci. Publ., Clarendon Press, Oxford, 1994.

[11] A. N. Skorobogatov, *On the fibration method for proving the Hasse principle and weak approximation*, in: Séminaire de théorie des nombres, Paris 1988–1989, Progr. Math. 91, Birkhäuser Boston, Boston, MA, 1990, 205–219.

Lilian Matthiesen
School of Mathematics
University Walk
Bristol, BS8 1TW, United Kingdom
E-mail: l.matthiesen@bristol.ac.uk

Received on 18.5.2012
and in revised form on 31.12.2012 (7069)