ACTA ARITHMETICA
154.3 (2012)

Linear correlations amongst numbers represented by positive definite binary quadratic forms

by

Lilian Matthiesen (Bristol)

Contents

1. Introduction. The distribution of prime numbers shares many properties with the distribution of numbers that are representable as a sum of two squares, an analogy that is occasionally employed to obtain model problems for questions about the primes. Let us consider the distributions of the two sets in arithmetic progressions. Starting with the average orders, we have on the one hand the prime number theorem, asserting that $\pi(x) \sim x/\log x$. For the set S of sums of two squares on the other hand, Landau [17] proved

2010 *Mathematics Subject Classification*: Primary 11N37; Secondary 11E25, 11B30.
Key words and phrases: binary quadratic form, pseudorandomness, correlation.

DOI: 10.4064/aa154-3-2

an analogous asymptotic in 1908, namely

$$\sum_{n\le x} 1_S(n) \sim Bx/\sqrt{\log x}\ ,$$

where $B = \frac{1}{\sqrt{2}}\prod_{p\equiv 3\,(\mathrm{mod}\,4)}(1-p^{-2})^{-1/2}$.

Turning towards more general arithmetic progressions, let a and q be coprime integers; then the primes congruent to a modulo q satisfy $\pi(x;q,a)\sim x/(\phi(q)\log x)$. Building on Landau's result and the analogy to primes, Prachar [20] proved in the 1950s that, when furthermore $a\equiv 1 \pmod{\gcd(4,q)}$, sums of two squares show the following behaviour ([1]):

$$\sum_{\substack{n\le x\\ n\equiv a\,(\mathrm{mod}\,q)}} 1_S(n) \sim B_q\frac{x}{\sqrt{\log x}}\ ,$$

where

$$B_q = Bq^{-1}\frac{(4,q)}{(2,q)}\prod_{\substack{p\equiv 3\,(\mathrm{mod}\,4)\\ p\mid q}}(1+p^{-1}).$$

The factor $(4,q)/(2,q)$ describes that the density of sums of two squares is twice as high in the progression $n\equiv 1 \pmod 4$ as it is in $n\equiv 1 \pmod 2$. From pairs (a,q) that are not coprime, one needs to remove those choices from consideration that lead to whole progressions entirely lying outside the set S. Examples are integers n such that $n\equiv 3 \pmod{3^2}$, which are never a sum of two squares, or numbers of the form $(3\cdot 5)n+3^2$, which can only be a sum of two squares when $3\mid n$. When excluding such classes $a \pmod q$, the constant B_q only needs to be adapted by restricting the product over $p\equiv 3 \pmod 4$ to primes dividing $q/\gcd(a,q)$.

Thus, both sets, the primes and the sums of two squares, show some uniformity in the distribution in residue classes once one excludes residue classes that for obvious reasons contain too few elements.

It is natural to ask whether this uniformity carries further: is, for instance, the distribution uniform enough to determine asymptotically the density of solutions to linear equations within these sets? More precisely, we are interested in an asymptotic for correlations of the form

$$\sum_{n\in\mathbb{Z}^d\cap K}\prod_{i=1}^{t} f(\psi_i(n))\ ,$$

where the $\psi_i:\mathbb{Z}^d\to\mathbb{Z}$ are affine linear forms and where the arithmetic function $f:\mathbb{Z}\to\mathbb{R}$ is either the characteristic function 1_S of the sums of two squares, or the characteristic function of the primes.

[1] This compact formulation of the result is due to Iwaniec [15].

Green and Tao [8] studied these correlations in the case of the primes. They replaced for this purpose the sparse set of primes by a weighted version of asymptotic density 1 which is given by the von Mangoldt function. We shall *not* normalise the characteristic function 1_S in an analogous way, but instead consider the intrinsically weighted function that is given by the representation function of sums of two squares, $R(n) = |\{(x,y) \in \mathbb{Z} : x^2+y^2 = n\}|$. Counting lattice points in a circle of radius $\sqrt{N}$ immediately shows that the representation function has indeed an asymptotic density given by $\sum_{n\le N} R(n) \sim \pi N$. As we will see, the nilpotent Hardy–Littlewood method which Green and Tao developed to handle linear correlations among the primes can also be employed in the case of the representation function $R(n)$.

Instead of restricting attention to representations as sums of two squares, the slightly more general case of representation by a positive definite binary quadratic form $f(x,y) = ax^2+bxy+cy^2$ will be considered. The corresponding representation function is then given by

$$R_f(n) = |\{(x,y) : f(x,y) = n\}|.$$

Notation. Throughout the paper, we write $[m]$ for the set of numbers $\{1,\dots,m\}$ and $e(x)$ for $\exp(2\pi x)$. We let $v_p : \mathbb{N} \to \mathbb{N}_0$ denote the p-adic valuation. If T is a finite set, we use the expectation notation $\mathbb{E}_{t\in T}$ to abbreviate $|T|^{-1}\sum_{t\in T}$. A linear correlation is defined along a system $\Psi = (\psi_1,\dots,\psi_t) : \mathbb{Z}^d \to \mathbb{Z}^t$ of affine linear forms. Such a system may be written as $\Psi(n) = \Psi(0) + \dot{\Psi}(n)$, for a linear map $\dot{\Psi}$. We regard $\dot{\Psi}$ as fixed, while $\Psi(0)$ may, for instance, depend on K. Thus, all implicit constants in asymptotic notation, such as $O()$, $o()$ and $\ll$, are allowed to depend on the coefficients of the linear map $\dot{\Psi}$, the dimensions d and t of the domain and the target space of Ψ, and on the discriminants of the forms $f_1,\dots,f_t$.

Methods and results. The nilpotent Hardy–Littlewood method provides a scheme that allows one to obtain, for any given arithmetic function h with sufficiently quasirandom behaviour, an asymptotic for the expression

$$\sum_{n\in K\cap\mathbb{Z}^d} \prod_{i=1}^{t} h(\psi_i(n)),$$

where $K \subset [-N,N]^d$ is convex and satisfies $\psi_i(K) \subset [1,N]$ for each $i \in \{1,\dots,t\}$. We proceed to describe the basic set-up for the method. There are two main requirements on h. One is that h has small Gowers uniformity norms (see Section 10) and the other is that one can find a majorant $\nu : \{1,\dots,N\} \to \mathbb{R}_{>0}$ such that

1. (*majorant property*) the pointwise estimate $h(n) \le C\nu(n)$ is satisfied for an absolute constant C independent of N,

2. (*density condition*) h has positive relative density in ν in the sense that $\mathbb{E}_{n\leq N}h(n) \sim C'\mathbb{E}_{n\leq N}\nu(n)$,
3. (*pseudorandomness*) ν is a pseudorandom measure.

A *pseudorandom measure* resembles a true probability measure. Apart from requiring its total mass to be approximately 1, that is, $\mathbb{E}_{n\leq N}\nu(n) = 1 + o(1)$, there are two further defining conditions for a pseudorandom measure: the linear forms condition and the correlation condition. Each of them places some independence requirements upon ν. The linear forms condition for instance requires

$$\mathbb{E}_{n\in K\cap\mathbb{Z}^d}\prod_{i=1}^{t}\nu(\psi_i(n)) = 1 + o(1)$$

to hold for certain systems of affine linear forms. Once in possession of such a pseudorandom majorant, a number of tools are available. We will describe them as we encounter them.

Regarding the first condition on h, which was the smallness of certain Gowers uniformity norms, there is an explicit (and quite strong) necessary condition that has to be satisfied: h must be equidistributed in residue classes to small moduli. The results quoted at the beginning of this introduction show that neither the characteristic function $1_S(n)$, nor its weighted version $r(n)$ meet this requirement. In such a situation, it may be possible to decompose the function h into a sum of functions that are more uniformly behaved and consider each of these functions separately. This decomposition is known as the W-trick and will be carried out in Section 7.

In Section 2 we construct a majorant for the representation function attached to a primitive form f. This majorant will be slightly modified in accordance to the W-trick in Section 7. In Section 9 we check that our majorant is indeed pseudorandom.

In the course of the minor arc analysis, which starts in Section 11, we observe that polynomial subsequences of δ-equidistributed linear nilsequences are still reasonably equidistributed (see Proposition 15.3 below). This result will be deduced from the quantitative equidistribution theory Green and Tao worked out in [10]. In connection with their factorisation theorem [10, Thm. 1.19], it could prove a useful tool for the minor arc analysis of a wider range of arithmetic problems.

Due to the quite complex foundations of the Green–Tao methods it proved not feasible to provide a self-contained account of it here. This paper therefore strongly depends on [8]. It furthermore relies on results about the divisor function from [18], which will be used in the construction of the pseudorandom majorants.

Results. In [18] a pseudorandom majorant for the normalised divisor function $\tilde{\tau}(n) = (\log N)^{-1} \sum_{d|n} 1$ has been constructed. Here we shall combine this majorant with a sieving majorant to obtain a pseudorandom majorant for the function $R_f(n)$ which counts the number of representations of n by a primitive positive definite binary quadratic form; results for the non-primitive case are immediate corollaries.

With this majorant at hand, we obtain, employing the machinery from [6, 8] in combination with the inverse theorem for the Gowers uniformity norms [11], an asymptotic for the representation function R_f evaluated along systems of linear equations:

THEOREM 1.1. *Let $f_1, \dots, f_t$ be primitive positive definite binary quadratic forms. 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. Suppose that the coefficients of the linear part $\dot{\Psi}$ are bounded and that $K \subset [-N, N]^d$ is a convex body such that $\Psi(K) \subset [0, N]^t$. Then*

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

where

$$\beta_\infty = \mathrm{vol}(K) \prod_{i=1}^{t} \frac{2\pi}{\sqrt{-D_i}},$$

and

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

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

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

Theorem 1.1 extends previous results by Heath-Brown [12] and improvements thereof by Browning and de la Bretèche [1], where the case of sums of two squares, $f_i(x, y) = x^2 + y^2$, for $i = 1, \dots, 4$, together with systems $\Psi : \mathbb{Z}^2 \to \mathbb{Z}^4$ was considered. We emphasise, however, that, in contrast to the results from [12] and [1], we unfortunately do not obtain explicit error terms in our asymptotic.

The most interesting case of correlation along a system of affine linear forms is certainly the 'infinite complexity' case of

$$\mathbb{E}_{n \le N} R_f(n + a_1) \dots R_f(n + a_d),$$

corresponding to the prime-tuples problem. In this case the linear forms involved are not independent and thus an asymptotic would give very strong information on the regularity of distribution of the function involved. Results of this type lie out of reach of the Green–Tao Hardy–Littlewood method.

It is worth mentioning at this point a recent related result of Henriot [13] which provides a correct order upper bound for $\mathbb{E}_{n\le N}F(|Q_1(n)|,\dots,|Q_t(n)|)$, where $F:\mathbb{N}^t\to\mathbb{R}_{\ge 0}$ belongs to a family of functions that does include $F(n_1,\dots,n_t)=\prod_{i=1}^{t}R_{f_i}(n_i)$, and where the Q_i are coprime irreducible polynomials. The bounds in this result are independent of the discriminant of the polynomial $Q_1\dots Q_t$.

Theorem 1.1 has some natural arithmetic consequences. Analysing the frequency of 4-term arithmetic progressions in sums of two squares (weighted by the representation function) may be viewed as a special case of studying the (average) number of simultaneous zeros of a pair of diagonal quadratic equations, namely solutions to

$$x_1^2+x_2^2-2x_3^2-2x_4^2+x_5^2+x_6^2=0,$$
$$x_3^2+x_4^2-2x_5^2-2x_6^2+x_7^2+x_8^2=0.$$

While the respective system for 3-term progressions may be easily handled by the circle method, Heath-Brown mentions in [12] that in order to give an asymptotic for the number of 4-term arithmetic progressions in sums of two squares "it would appear that one would require a version of the 'Kloosterman refinement' for a double integral". Browning and Munshi [2] have succeeded in showing that the circle method can in fact be employed to study any pair of quadratic equations in $n\ge 9$ variables that takes the form

$$F_1(x_3,\dots,x_n)=-c(x_1^2+x_2^2),\quad F_2(x_3,\dots,x_n)=0.$$

Previously, the classical Hardy–Littlewood method had been successfully applied to pairs of diagonal quadratic equations in at least nine variables:

Theorem 1.2 (Cook [3]). *Let $F,G:\mathbb{Z}^9\to\mathbb{Z}$ be integral diagonal quadratic forms such that for all real λ,μ, not both zero, $\lambda F+\mu G$ is an indefinite form in at least five variables. Then there is some positive constant K_0 such that the number of simultaneous integral zeros of F and G in the box*

$$P\le x_i\le CP,\qquad i=1,\dots,9,$$

is given by

$$\mathcal{N}(P)=K_0P^5+o(P^5)\qquad \text{as } P\to\infty.$$

Our result, which is in fact an analogue of [8, Thm. 1.8], considers certain highly singular systems of quadratic equations in eight or more variables.

Theorem 1.3. *Let $t\ge 4$ and let $f_1,\dots,f_t$ be primitive positive definite binary quadratic forms. For an integer $s\le t-2$, let $A\in M_{s\times t}(\mathbb{Z})$ be a full rank matrix whose row-span over $\mathbb{Q}$ contains no non-trivial element with* *less than three non-zero entries. Define a height function $H : \mathbb{Z}^{2t} \to \mathbb{R}_{\geq 0}$ by*

$$H(x) = \max_{j \in \{1,\dots,t\}} \sqrt{f_j(x_{2j-1}, x_{2j})}.$$

Then the simultaneous zeros of the system of quadratic forms

$$F_i(x_1, \dots, x_{2t}) = \sum_{j=1}^{t} a_{i,j} f_j(x_{2j-1}, x_{2j}), \quad i \in \{1, \dots, s\},$$

satisfy the following asymptotic:

$$\begin{aligned}|\{x \in \mathbb{Z}^{2t} : H(x) \leq N,\, F_1(x) = \cdots = F_s(x) = 0\}| \\ = \frac{(2\pi)^t}{\sqrt{|D_1 \dots D_t|}} \alpha_\infty \prod_p \alpha_p + o(N^{2t}),\end{aligned}$$

where

$$\alpha_p := \lim_{m \to \infty} \frac{|\{x \in (\mathbb{Z}/p^m\mathbb{Z})^{2t} : F_1(x) \equiv \cdots \equiv F_s(x) \equiv 0 \pmod{p^m}\}|}{(p^m)^{2t-s}}$$

and

$$\alpha_\infty := |\{z \in \{1, \dots, N^2\}^t : Az = 0\}|.$$

We conclude this introduction with the fairly short deduction of Theorem 1.3.

Proof of Theorem 1.3 from Theorem 1.1. The number of simultaneous zeros of bounded height of the forms $F_1, \dots, F_t$ can be reinterpreted in terms of representation functions:

$$\begin{aligned}(1.1) \quad |\{x \in \mathbb{Z}^{2t} : F_1(x) = \cdots = F_t(x) = 0,\, H(x) \leq N\}| \\ = \sum_{z \in [N^2]^t :\, Az = 0} \prod_{j=1}^{t} r_{f_j}(z_j).\end{aligned}$$

To turn the latter expression into the form of a linear correlation, we may follow [8, §4]: Pick a basis for the integer lattice

$$\Gamma := \{z \in \mathbb{Z}^t : Az = 0\}.$$

Since A has full rank, Γ has rank $d := t - s$, and thus there are linear forms $\psi_1, \dots, \psi_t : \mathbb{Z}^d \to \mathbb{Z}$ such that

$$\Gamma = \{(\psi_1(n), \dots, \psi_t(n)) : n \in \mathbb{Z}^d\}.$$

This system of forms has finite complexity, as otherwise we would find $i \neq j$ such that $\alpha_i \psi_i = \alpha_j \psi_j$ for some non-zero integers α_i, α_j. Hence,

$$\Gamma = \{z \in \mathbb{Z}^t : Az = 0,\, \alpha_i z_i - \alpha_j z_j = 0\},$$

which implies by the full rank assumption on A that the row-space of A contains a non-trivial element with less than three non-zero entries, a contradiction.

Thus, (1.1) takes a form to which Theorem 1.1 applies and we obtain

$$\begin{aligned}|\{x \in \mathbb{Z}^{2t} : F_1(x) = \cdots = F_s(x) = 0,\ H(x) \le N\}|\\ &= \sum_{n \in \mathbb{N}^d \cap \Psi^{-1}([1,N^2]^t)} \prod_{j=1}^{t} r_{f_j}(\psi_j(n_j))\\ &= \operatorname{vol}(\mathbb{R}^d_{\ge 0} \cap \Psi^{-1}([0,N^2]^t)) \frac{(2\pi)^t}{\sqrt{|D_1 \ldots D_t|}} \prod_p \beta_p + o(N^{2d}).\end{aligned}$$

Note that

$$\begin{aligned}\operatorname{vol}(\mathbb{R}^d_{\ge 0} \cap \Psi^{-1}([0,N^2]^t)) &= |\{n \in \mathbb{Z}^d : \Psi(n) \in [0,N^2]^t\}| + o(N^{2d})\\ &= |\{z \in \{1,\ldots N^2\}^t : Az = 0\}| + o(N^{2d}),\end{aligned}$$

which justifies defining $\alpha_\infty := |\{z \in \{1,\ldots,N^2\}^t : Az = 0\}|$. It remains to interpret the local factors β_p in terms of $F_1,\ldots,F_t$. If m is sufficiently large, then the $\mathbb{Z}$-basis $(\psi_j)_{j\in[d]}$ of Γ gives rise to a basis of $\{z \in (\mathbb{Z}/p^m\mathbb{Z})^t : Az \equiv 0 \pmod{p^m}\}$, whence

$$\begin{aligned}\mathbb{E}_{a\in(\mathbb{Z}/p^m\mathbb{Z})^d} \prod_{j=1}^{t} \frac{\rho_{f_j,\psi_j(a)}(p^m)}{p^m} &= p^{-m(t+d)}\\ \times \sum_{a\in(\mathbb{Z}/p^m\mathbb{Z})^d} \prod_{j=1}^{t} |\{(x_{2j-1},x_{2j}) \in [p^m]^2 &: f_j(x_{2j-1},x_{2j}) \equiv \psi_j(a) \pmod{p^m}\}|\\ &= \frac{|\{x \in (\mathbb{Z}/p^m\mathbb{Z})^{2t} : F_1(x) \equiv \cdots \equiv F_s(x) \equiv 0 \pmod{p^m}\}|}{(p^m)^{2t-s}},\end{aligned}$$

which yields $\beta_p = \alpha_p$ for all primes p. ∎

2. A majorant for the representation function via the Kronecker sum

Preliminaries and notation. Recall that a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is *primitive* when $(a,b,c) = 1$ and that its discriminant is given by $D(f) = b^2 - 4ac$. Throughout this paper all binary quadratic forms will be assumed to be positive definite. The number of ways a form f represents an integer n is described by the *representation function* $R_f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$R_f(n) := |\{(x,y) : f(x,y) = n\}|.$$

In order to make use of some multiplicative properties of R_f, we introduce the function $r_f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$r_f(n) := R_f(n)/k(D),$$

where $k(D)$ denotes the number of automorphs of binary forms of discriminant D. We have $k(D) = 6, 4, 2$ according to whether $D = -3$, $D = -4$ or $D < -4$, respectively.

Closely related to r_f is the function $r_{D(f)} : \mathbb{Z} \to \mathbb{Z}$ which counts—up to the factor $k(D)$—the number of ways n is represented by any equivalence class of forms of discriminant $D = D(f)$. We define $r_{D(f)}$ by

$$r_{D(f)}(n) := \sum_{D(f')=D(f)} r_{f'}(n),$$

where f' runs through a complete system of representatives of primitive forms of discriminant equal to $D(f)$.

The function $r_{D(f)}$ majorises r_f and has some properties that suggest it may be a good candidate to start the construction of a pseudorandom majorant with: on the one hand, the number $h(D)$ of equivalence classes of primitive forms of discriminant D is finite, and thus the average order of $r_{D(f)}$ is comparable to the average order of r_f; on the other hand, $r_{D(f)}$ has an arithmetic representation as a divisor sum, a structure that proved to be well suited for the construction of a pseudorandom majorant in both [6] and [18].

Let f be a primitive positive definite form of discriminant D. Then $r_f(n) = 0$ for $n < 0$ and $r_f(0) = 1$. For positive integers n coprime to D, r_D has the representation

$$r_{D(f)}(n) = \sum_{d|n} \left(\frac{D}{d}\right)$$

as a character sum, where $(\frac{\cdot}{\cdot})$ is the Kronecker symbol. For general n, we pick up another factor which depends only on $\gcd(n, D)$ and the parities of the α in $\prod_{p|D,\, p^\alpha \| n} p^\alpha$. We will see in Corollary 5.1 that

$$r_{D(f)}(n) \ll_D \sum_{d|n} \left(\frac{D}{d}\right) \tag{2.1}$$

for all $n \in \mathbb{N}$.

Recall that the Kronecker symbol is only non-zero when its entries are coprime and that furthermore the following lemma holds (see for instance [4, Thm. 1.14]).

Lemma 2.1. *If $D \equiv 0, 1 \pmod 4$ is a non-zero integer, then there is a unique character $\chi_D : (\mathbb{Z}/D\mathbb{Z})^* \to \{-1, 1\}$ such that $\chi_D(p \pmod D) = \left(\frac{D}{p}\right)$ for odd p coprime to D.*

Let $\mathcal{Q}_D$ denote the set of primes for which $\chi_D(p) = -1$. Note that this is the union of the primes in a collection of progressions modulo D. By multiplicativity we have

$$\sum_{d|n}\left(\frac{D}{d}\right) = \sum_{d|n}\chi_D(d) = \prod_{p^a\|n}(1+\chi_D(p)+\cdots+\chi_D(p^a)) \tag{2.2}$$
$$= \tau_D(n)\prod_{p^\alpha\|n,\, p\in\mathcal{Q}_D}\frac{1}{2}(1+(-1)^\alpha),$$

where

$$\tau_D(m) = \prod_{p^a\|m,\,\chi_D(p)=1}(a+1).$$

We denote by $\mathcal{P}_D$ the set of primes for which $\chi_D(p) = 1$. Thus, a square-free number n is represented by some form of discriminant $D(f)$ only if all of its prime factors belong to $\mathcal{P}_D$ or divide $D(f)$.

We can say a little more about the sets $\mathcal{P}_D$ and $\mathcal{Q}_D$: Since χ is a non-principal character taking values ±1, the fact that $\sum_{a\in(\mathbb{Z}/D\mathbb{Z})^*}\chi(a) = 0$ implies that both $\mathcal{P}_D$ and $\mathcal{Q}_D$ are the union of the primes in exactly $\phi(D)/2$ progressions modulo D. Thus, the square-free numbers that are coprime to D and representable by some form of discriminant D are those numbers whose prime factors belong to a set comprising asymptotically half the prime numbers.

As a last piece of notation, given any set $\mathcal{P}$ of primes, let $\langle\mathcal{P}\rangle$ denote the set of natural numbers all of whose prime factors belong to $\mathcal{P}$. Thus we may write

$$\tau_D(n) = \sum_{d\in\langle\mathcal{P}_D\rangle}1_{d|n}.$$

Construction of the majorant. The key observation for the construction of our majorant for r_f is that according to (2.1) and (2.2) it suffices to find two majorants separately: one for a divisor-type function related to τ_D, and one for the characteristic function of the set of numbers without $\mathcal{Q}_D$-prime factors. Writing $\mathcal{P}_D^* = \mathcal{P}_D\cup\{p : p \mid D\}$, the characteristic function of interest is $1_{\langle\mathcal{P}_D^*\rangle}$. The shifts by square factors of the form $\prod_{p\in\mathcal{Q}_D}p^{2\alpha}$ only influence the asymptotic density by a constant factor and may be taken care of separately. If ν is a majorant for τ_D and if β is a majorant for $1_{\langle\mathcal{P}_D^*\rangle}$, then $r_f(n)$ is majorised by

$$O_D(1)\nu(n)\sum_{m\in\langle\mathcal{Q}_D\rangle}\beta(n/m^2)1_{m^2|n}.$$

The majorant β for $1_{\langle\mathcal{P}_D^*\rangle}$ will be chosen as a sieving majorant. In fact, the approach via sieve weights in [8] proves universal enough to apply here too without much change. Concerning ν, we make use of the results on the divisor function from [18].

Since neither τ_D nor $1_{\langle \mathcal{P}_D^* \rangle}$ has asymptotic density, we proceed to determine the average order of τ_D and show that $\mathbb{E}_{n\leq N}\tau_D(n) \asymp (\log N)^{1/2}$. This suggests renormalising the factors in the bound on $r_{D(f)}$ as follows:

$$r_{D(f)}(n) \ll_D \frac{\tau_D(n)}{(\log N)^{1/2}} \sum_{\substack{m\in\langle \mathcal{Q}_D\rangle \\ m^2 | n}} 1_{\langle \mathcal{P}_D^* \rangle}(n/m^2)(\log N)^{1/2}.$$

Iwaniec [15] proves via sieve theory that it is indeed the case that $1_{\langle \mathcal{P}_D^* \rangle}$ is of average order $(\log N)^{-1/2}$. This bound, however, is not needed here.

Lemma 2.2. *τ_D satisfies the asymptotic bounds*

$$\mathbb{E}_{n\leq N}\tau_D(n) \asymp (\log N)^{1/2},$$

where the implicit constants may depend on D.

Proof. We have

$$\mathbb{E}_{n\leq N}\tau_D(n) = \frac{1}{N} \sum_{\substack{d\in\langle \mathcal{P}_D\rangle \\ d\leq N}} \left[\frac{N}{d}\right] = \sum_{\substack{d\in\langle \mathcal{P}_D\rangle \\ d\leq N}} \frac{1}{d} + O(1).$$

To estimate the last sum, observe that on the one hand

$$\sum_{\substack{d\in\langle \mathcal{P}_D\rangle \\ d\leq N}} \frac{1}{d} \leq \prod_{\substack{p\in\mathcal{P}_D \\ p\leq N}} (1-p^{-1})^{-1} \ll (\log N)^{1/2},$$

where the last step follows from the prime number theorem in arithmetic progressions in the form

$$\sum_{\substack{p\equiv a \,(\mathrm{mod}\, q) \\ p\leq N}} p^{-1} = \frac{1}{\phi(q)} \log\log(N) + O(1).$$

The above remains true when replacing $\mathcal{P}_D$ by $\langle \mathcal{Q}_D^* \rangle := \mathcal{Q}_D \cup \{p : p \,|\, D\}$ and $O(1)$ by $O_D(1)$. On the other hand the following chain of inequalities allows us to deduce a matching lower bound:

$$\log N + O(1) = \sum_{n\leq N}\frac{1}{n} \leq \Bigg(\sum_{\substack{m_1\in\langle \mathcal{P}_D\rangle \\ m_1\leq N}} \frac{1}{m_1}\Bigg)\Bigg(\sum_{\substack{m_2\in\langle \mathcal{Q}_D^*\rangle \\ m_2\leq N}} \frac{1}{m_2}\Bigg)$$

$$\ll \Bigg(\sum_{\substack{m_1\in\langle \mathcal{P}_D\rangle \\ m_1\leq N}} \frac{1}{m_1}\Bigg)(\log N)^{1/2}. \ \blacksquare$$

The divisor-type majorant. To start with, we recall the divisor function majorant that was constructed in [18] based on Erdős's work [5]. For any $\gamma > 0$ define the truncated divisor function $\tau_\gamma : [N] \to \mathbb{Z}$ by

$$\tau_\gamma(n) := \sum_{d \leq N^\gamma} 1_{d|n}$$

and the truncated restricted divisor function $\tau_{D,\gamma} : [N] \to \mathbb{Z}$ by

$$\tau_{D,\gamma}(n) := \sum_{\substack{d \in \langle \mathcal{P}_D \rangle \\ d \leq N^\gamma}} 1_{d|n}.$$

Proposition 2.3 ([18], majorant for the divisor function). *Let $\xi = 2^{-m}$ for some $m \in \mathbb{N}$. Let C_0 be a parameter and write $X_0 = X_0(C_1, N)$ for the exceptional set of all $n \leq N$ satisfying either*

1. *n is excessively "rough" in the sense that it is divisible by some prime power p^a, $a \geq 2$, with $p^a > \log^{C_1} N$, or*
2. *n is excessively "smooth" in the sense that if $n = \prod_p p^a$ then*

$$\prod_{p \leq N^{1/(\log\log N)^3}} p^a \geq N^{\xi/\log\log N}.$$

Further, define $U(i, 2/\xi) := \{1\}$ for $i = \log_2(2/\xi) - 2$, and $U(i, 2/\xi) := \emptyset$ else. If $s > 2/\xi$, write $U(i,s)$ for the set of all products of $m_0(i,s) := \lceil \xi s(i + 3 - \log_2 s)/100 \rceil$ distinct primes from the interval $[N^{1/2^{i+1}}, N^{1/2^i}]$. Define $\tilde{\nu}_\xi : [N] \to \mathbb{R}_+$ by

$$\tilde{\nu}_\xi(n) := \sum_{s \geq 2/\xi}^{(\log\log N)^3} \sum_{i \geq \log_2 s - 2}^{6 \log\log\log N} \sum_{u \in U(i,s)} 2^s 1_{u|n} \tau_\xi(n) + 1_{n \in X_0} \tau(n).$$

Then $\tau(n) \leq \tilde{\nu}_\xi(n)$ for all $n \leq N$, provided N is sufficiently large.

Note that the main term of $\tilde{\nu}_\xi$ has low complexity in that it only involves small divisors since all $u \leq N^\xi$. Restricting all occurrences of divisor functions in $\tilde{\nu}_\xi$ to only count divisors in $\langle \mathcal{P}_D \rangle$, yields a majorant for τ_D of the same order of magnitude as τ_D. We make one further modification and replace the cut-off in the definition of $\tau_{D,\gamma}$ by a smooth cut-off of the form which appears in Green and Tao's Λ-majorant. This turns out to be advantageous when establishing the linear forms condition. Thus, let $\chi : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be a smooth, even function that is supported on $[-1, 1]$ and has the property $\chi(x) = 1$ for $x \in [-1/2, 1/2]$. Define $\tau^*_{D,\gamma} : [N] \to \mathbb{Z}$ by

$$\tau^*_{D,\gamma}(n) := \sum_{\substack{d \in \langle \mathcal{P}_D \rangle \\ d \leq N^\gamma}} 1_{d|n} \chi\left(\frac{\log d}{\log N^\gamma}\right).$$

Then $\tau_{D,\gamma/2} \leq \tau^*_{D,\gamma}(n) \leq \tau_{D,\gamma}(n)$. With this definition we have the following lemma.

Lemma 2.4 (A majorant for τ_D). *Let the sets $U(i,s)$ be those which Proposition* 2.3 *produces for $\xi = \gamma/2$. Let $\nu_{D,\gamma} : [N] \to \mathbb{R}$ be defined by*

$$C\nu_{D,\gamma}(n) \\ := \frac{1}{\sqrt{\log N}}\Big(\sum_{s\geq 4/\gamma}^{(\log\log N)^3} \sum_{i\geq \log_2 s-2}^{6\log\log\log N} \sum_{u\in U(i,s)} 2^s 1_{u|n}\tau^*_{D,\gamma}(n) + 1_{n\in X_0}\tau_D(n)\Big).$$

Then $\tau_D(n)/(\log N)^{1/2} \leq C\nu_{D,\gamma}(n)$ for all $n \in [N]$ and there is some constant C bounded independently of N such that $\mathbb{E}_{n\leq N}\nu_{D,\gamma}(n) = 1 + o(1)$.

Proof. We begin by checking the majorisation property. For any $n \in [N]$, write $n = n_{\mathcal{P}}m$ where $n_{\mathcal{P}}$ is the largest factor of n that belongs to $\langle \mathcal{P}_D\rangle$. Then

$$\tau_D(n) = \tau(n_{\mathcal{P}}) \leq \tilde{\nu}_{\gamma/2}(n_{\mathcal{P}}) \leq C(\log N)^{1/2}\nu_{D,\gamma}(n_{\mathcal{P}}) = C(\log N)^{1/2}\nu_{D,\gamma}(n),$$

as required. The existence of C follows as in the proof of [18, Prop. 4.2], taking into account that $\mathbb{E}_{m\leq N}\tau_{D,\gamma/2}(m) \asymp (\log N)^{1/2}$, which is proved in much the same way as Lemma 2.2. ∎

The sieving type majorant. The next task is to give a majorant $\beta : \mathbb{N} \to \mathbb{R}^+$ for the characteristic function of the set $\langle \mathcal{P}^*_D\rangle$ of numbers without $\mathcal{Q}_D$-prime factors. Adapting the Selberg-sieve majorant for primes from [8] to the set $\langle \mathcal{P}^*_D\rangle$, we aim to remove all integers that have prime factors p from $\mathcal{Q}_D$ with $p \leq N^\gamma$. Let $\chi : \mathbb{R} \to \mathbb{R}$ be a smooth, even function that is supported on $[-1,1]$ and satisfies $\chi(0) = 1$. Define, in analogy to [8, App. D],

$$\beta(n) := \Lambda_{D,\chi,\gamma}(n) := C'(\log N)^{1/2}\Big(\sum_{d|n,\, d\in\langle \mathcal{Q}_D\rangle} \mu(d)\chi\Big(\frac{\log d}{\log N^\gamma}\Big)\Big)^2$$

for some constant C'. The results from [8] show that C' may be chosen such that $\mathbb{E}_{n\leq N}\beta(n) = 1 + o(1)$. This will play a role in Section 9. Note that $\beta(m) = C'(\log N)^{1/2}$ at every $\mathcal{Q}_D$-prime-free integer $m \leq N$, and thus we have the pointwise majorisation

$$1_{\langle \mathcal{P}^*_D\rangle}(n)(\log N)^{1/2} \leq C'^{-1}\beta(n), \quad n \in [N].$$

3. A reduction of the main theorem. While it is possible to apply the nilpotent Hardy–Littlewood method to the representation function r_f itself, it is the aim of this section to show that we can deduce the main theorem from a similar statement about a smoothed version of r_f, that is, a function that agrees with r_f everywhere except on a sparse set where the restricted divisor function τ_D shows exceptionally irregular behaviour.

First note that the pointwise bound $r_f(n) \leq r_{D(f)}(n) \leq \tau(n)$ for $n \in \mathbb{N}$ of the representation function of any primitive positive definite quadratic form f by the divisor function gives the following second moment estimate.

Lemma 3.1 (Second moment estimate). *Let $f_1, \dots, f_t$ be primitive positive definite binary quadratic forms and let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^m \to \mathbb{Z}^t$ be a system of affine-linear forms whose linear coefficients are bounded by L. If $K \subset [-N, N]^d$ is a convex body such that $\Psi(K) \subseteq [0, N]^t$, then*

$$\mathbb{E}_{n \in \mathbb{Z}^m \cap K} \prod_{i \in [t]} r_{f_i}^2(\psi_i(n)) \ll_{t,m,L} (\log N)^{O_t(1)}.$$

Proof. Let $K' := \{x \in K : \Psi(x) \in [1, N]^t\}$. Then Hölder's inequality yields

$$\begin{aligned}\mathbb{E}_{n \in \mathbb{Z}^m \cap K} \prod_{i \in [t]} r_{f_i}^2(\psi_i(n)) &\leq \prod_{i \in [t]} \big(1 + \mathbb{E}_{n \in \mathbb{Z}^m \cap K'} r_{f_i}^{2t}(\psi_i(n))\big)^{1/t} \\ &\leq \prod_{i \in [t]} \big(1 + \mathbb{E}_{n \in \mathbb{Z}^m \cap K'} \tau^{2t}(\psi_i(n))\big)^{1/t}\end{aligned}$$

The remaining steps are standard; cf. the proof of [18, Lemma 3.1] for details. ∎

The next lemma, which is a combination of some technical lemmas from [5], describes an exceptional set for the divisor function, i.e. a sparse set containing those numbers on which the divisor function behaves particularly irregularly.

Lemma 3.2. *Let $C_1 > 1$ be a parameter and write X_0 for the set of all positive $n \leq N$ satisfying either of the following:*

(1) *n is excessively "rough" in the sense that it is divisible by some prime power p^a, $a \geq 2$, with $p^a > \log^{C_1} N$,*
(2) *n is excessively "smooth" in the sense that if $n = \prod_p p^a$ then*

$$\prod_{p \leq N^{1/(\log\log N)^3}} p^a \geq N^{\gamma/\log\log N},$$

(3) *n has a large square divisor $m^2 \mid n$, $m > N^\gamma$.*

Then

$$\mathbb{E}_{n \in K \cap \mathbb{Z}^d} \sum_{i=1}^{t} 1_{\psi_i(n) \in X_0} \ll (\log N)^{-C_1/2}.$$

Proof. See [5] for the original results or [18, §3] for their adaptation to this situation. ∎

The previous two lemmas allow us to deduce the main theorem from an equivalent statement about smoothed versions of the representation functions r_{f_i}. The particular smoothed functions we shall work with will be chosen in Section 7.

LEMMA 3.3. *Let $f_1, \dots, f_t$ be primitive positive definite binary quadratic forms. For each $i \in [t]$, let $\bar{r}_{f_i} : \{0, \dots, N\} \to \mathbb{R}$ denote a function that agrees with r_{f_i} on $[N] \setminus X_0$, that is, outside the exceptional set of the divisor function, and which further satisfies $0 \leq \bar{r}_{f_i}(n) \leq r_{f_i}(n)$ for all $n \in X_0 \cup \{0\}$. If the parameter C_1 of the exceptional set is sufficiently large, then the main theorem holds if and only if under the same conditions*

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

Proof. This follows by the Cauchy–Schwarz inequality from the previous two lemmas and the bound

$$\sum_{n \in K \cap \mathbb{Z}^d} \sum_{i=1}^{t} 1_{\psi_i(n)=0} \ll N^{d-1}. \blacksquare$$

The above lemma in particular shows that a pseudorandom majorant used in the proof only needs to majorise the function r_f (or $\bar{r}_f$) on the set of positive unexceptional integers. We can therefore truncate the summation over dilates of m^2, $m \in \langle \mathcal{Q}_D \rangle$, in the majorant to those m with $m < N^\gamma$. Furthermore, we may restrict attention to the case where $\Psi(K) \subseteq [1, N]^t$.

4. Distribution in residue classes.

The transference principle from [6, 8], which we shall employ later, only works with functions h that are sufficiently quasirandom in the sense that all U^k-norms $\|h - \mathbb{E}h\|_{U^k}$ up to some order k, determined by the specific system Ψ one is working with, are small. A necessary condition for the uniformity norms to be small is that the function h at hand is equidistributed in residue classes to small moduli. This condition is in fact equivalent to requiring that h does not correlate with periodic nilsequences of short period (cf. Section 11).

As seen at the start of the introduction, the representation function r_f does not have this property. To remove these obstructions to uniformity, one can try to split the function r_f into a sum of functions each of which does not detect a difference between residue classes to small moduli. This strategy is known as the W-trick. In order to find a suitable decomposition, we shall investigate the quantities

$$\mathbb{E}_{n \leq N} 1_{n \equiv \beta \,(\mathrm{mod}\, q)} \; r_f(n)$$

for fixed period q and fixed residue class β. Define

$$\rho_{f,\beta}(q) := |\{(x, y) \in [q]^2 : f(x, y) \equiv \beta \pmod{q}\}|$$

to be the number of representations of $\beta \pmod q$, and let

$$K(N) = f^{-1}([0,N]) \subseteq \mathbb{R}^2.$$

This is the area enclosed by the ellipse $f(x,y) = N$ and hence a convex set of volume

$$\operatorname{vol} K(N) = \frac{2\pi N}{\sqrt{-D}}.$$

A volume packing argument (cf. [8, App. A]) yields

$$\sum_{\substack{n \leq N \\ n \equiv \beta \,(\mathrm{mod}\, q)}} r_f(n) k(D) = \sum_{\substack{(x,y) \in K(N) \cap \mathbb{Z}^2 \\ f(x,y) \equiv \beta \,(\mathrm{mod}\, q)}} 1 = \frac{\rho_{f,\beta}(q)}{q^2} \operatorname{vol}(K) + O(\sqrt{N}\, q),$$

which proves the following lemma.

Lemma 4.1. *Let $P := \{n \leq N : n \equiv \beta \pmod q\}$ be an arithmetic progression. Then the average of the representation function of f along P satisfies*

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

In view of this lemma it is not surprising that we will make use of several further observations on the densities $\rho_{f,\beta}(q) q^{-1}$, which will be established in Section 6.

Lemma 4.2. *$\rho_{f,\beta}(q)$ only depends on the genus class of f.*

Proof. Two forms f_1 and f_2 belong to the same genus if and only if they are locally equivalent in the following sense: for every non-zero integer m there exists $\sigma_m \in Gl_2(\mathbb{Z}/m\mathbb{Z})$ such that

$$f_1(x,y) \equiv f_2((x,y)\sigma_m) \pmod m.$$

Thus, $\rho_{f_1,\beta}(q) = \rho_{f_2,\beta}(q)$ for all positive integers q and all $\beta \in [q]$. ∎

The reason this lemma is important to us is that it allows us to consider instead of r_f the following more regularly behaved function in all questions regarding the distribution in residue classes. Let the genus class representation function $r_g : \mathbb{N} \to \mathbb{N}$ be defined by

$$r_g(n) = \mathbb{E}(r_f(n) \mid f \in g),$$

where f runs through a system of representatives of classes in the genus g. Under the assumptions of Lemma 4.1 we then have

$$\mathbb{E}_{n \in P} r_f(n) = \mathbb{E}_{n \in P} r_{g(f)}(n) + O(|P|^{-1/2} q^2), \tag{4.1}$$

where $g(f)$ denotes the genus that contains f.

5. Results from the theory of binary quadratic forms.

The aim of this section is to prove the bound (2.1) on the number of representations of a positive integer n by a form of discriminant D, which was used to construct the majorant function in Section 2.

5.1. Representation by primitive forms of fixed discriminant.

The question of whether or not m is properly representable by a primitive form of discriminant D is linked to the solubility in x of the congruence

$$x^2 \equiv D \pmod{4m}; \tag{5.1}$$

see [16, p. 506] or [21, p. 172]. If f is a form of discriminant D that represents m properly, then f is equivalent to $\langle m, n, *\rangle = mX^2 + nXY + *Y^2$, where $D = n^2 - 4mk$ for some integer k.

Claim 1. *Consider the solutions $x = n$ to (5.1) that satisfy $0 < n \le 2m$. These form a complete set of incongruent solutions modulo $2m$. Those solutions among them for which $\langle m, n, (D - n^2)/4m\rangle$ is primitive are in one-to-one correspondence with the distinct classes of primitive forms that represent m properly.*

Proof. Let f be a primitive form and suppose there are coprime u and v such that $f(u, v) = m$. Choose a solution (z_0, w_0) to $1 = uz_0 - vw_0$. Then

$$f'(X,Y) := f\left((X,Y)\begin{pmatrix} u & v \\ w_0 & z_0 \end{pmatrix}\right) = mX^2 + nXY + \frac{D - n^2}{4m}Y^2$$

is an equivalent form with leading coefficient m. Choosing different solutions $w = w_0 + w'$ and $z = z_0 + z'$ to $1 = uz - vw$, we have $w' = tu$ and $z' = tv$ for some non-zero integer t, which implies that the middle coefficient n is unique modulo $2m$. In particular $\langle m, n_1, *\rangle \sim \langle m, n_2, *\rangle$ if and only if $n_1 \equiv n_2 \pmod{2m}$.

Observe that in the other direction every solution $x = n$ to $x^2 \equiv D \pmod{4m}$ yields an equivalence class $\langle m, n, *\rangle$ of forms of discriminant D that represents m properly. ■

In order to determine the number of classes of forms that represent m, we are interested in two pieces of information:

1. the number of solutions x to $x^2 \equiv D \pmod{4m}$, and
2. how many of these solutions yield *primitive* forms $(m, x, *)$ of discriminant D.

A third necessary piece of information regards the number of proper representations by a fixed class of forms: any two proper representations of m by a fixed form f are related by an automorph. Thus each class $C(f)$ of forms equivalent to f represents m properly in $k(D)$ different ways, where $k(D)$ is the number of automorphs of forms of discriminant D.

In order to analyse the number of solutions to (5.1), we introduce the related irreducible quadratic polynomial $P(x) = x^2 - D$, which has discriminant $4D$.

Let $\rho(a) := |\{k \in [a] : P(k) \equiv 0 \pmod{a}\}|$ denote the number of zeros modulo a. The counting function ρ is multiplicative by the Chinese remainder theorem, which leaves us to determine ρ at prime powers. If $p \nmid D$, then (cf. [14, Thm. 12.3.4])

$$\rho(p^\alpha) = \begin{cases} 2 & \text{if } p = 2,\ \alpha = 2, \\ 2(1 + \chi_D(p)) & \text{if } p = 2,\ \alpha > 2, \\ 1 + \chi_D(p) & \text{if } p > 2. \end{cases}$$

In the remaining case of primes $p \mid D$, Hensel's lemma implies that

$$\rho(p^\alpha) = \rho(p^{v_p(4D)+1}) \quad \text{if } \alpha > v_p(4D).$$

For $p \mid D$ we will show below that, in fact, there are no primitive forms that properly represent an integer m with $v_p(m) > v_p(D)$ for some prime p.

If m is coprime to D, then each solution to $x^2 \equiv D \pmod{4m}$ yields a primitive form, and $\rho(4m)$ is directly linked to the number $r_D^*(m)$ of classes of primitive forms that represent m *properly*: $r_D^*(m) = \frac{1}{2}\rho(4m)$.

We turn to the case where $\gcd(D, m) > 1$. If there is a prime p dividing $\gcd(D, 4m)$ to an odd power, then solutions to $D = n^2 - 4mk$ yield primitive forms if and only if each such p divides both D and $4m$ to the same power.

Considering the set of forms arising from solutions to (5.1), we can, if $\gcd(m, 4D) > 1$, retrieve the number of primitive forms among them via an inclusion-exclusion argument. Indeed, when $d = \gcd(m, n, k)$, then m/d is properly represented by the form $\langle m/d, n/d, k/d\rangle$ of discriminant Dd^{-2}. Note that automorphs of forms of the first kind are also automorphs of forms of the second kind and vice versa.

Let $p^\alpha \parallel m$ and suppose that $p^\sigma \parallel D$, $\sigma > 1$.

We begin by analysing the largest range for α, $\alpha > \sigma > 1$. When σ is odd, then there are, as seen above, no primitive forms that represent p^α properly. Suppose next that σ is even and define

$$\rho'(p^\alpha) := |\{x : x^2 \equiv D \pmod{p^\alpha}\}| - |\{x : x^2 \equiv Dp^{-2} \pmod{p^{\alpha-1}}\}|.$$

This quantity counts the number of solutions to $x^2 \equiv D \pmod{p^\alpha}$ for which $x^2 = D + kp^\alpha$ for some k not divisible by p. The expression for $\rho'(p^\alpha)$ simplifies to

$$\begin{aligned} \rho'(p^\alpha) = |\{x : x^2 \equiv Dp^{-\sigma} &\pmod{p^{\alpha-\sigma}}\}| \\ &- |\{x : x^2 \equiv Dp^{-\sigma} \pmod{p^{\alpha-1-(\sigma-2)}}\}|, \end{aligned}$$

which is seen to be 0 by Hensel's lemma (note that $p \nmid Dp^{-\sigma}$). Thus, no power $p^\alpha \nmid D$ of a discriminant-prime with $p^2 \mid D$ is properly representable by a primitive form.

What remains are even powers $p^\alpha \mid D$, $\alpha < \sigma$, and the case $p^\alpha \parallel D$. In the former case, any solution to $D = n^2 + 4mk$ with $p^{\alpha/2} \parallel n$ satisfies $p \nmid k$. Hence there are $p^{\alpha/2}(1 - p^{-1})$ choices for $n \pmod{p^\alpha}$. In the latter case, $p \nmid k$ if and only if $p^{\lceil \alpha/2 \rceil} \mid n$, hence there are $p^{\lfloor \alpha/2 \rfloor}$ choices in this case.

In total, the number $r^*(m)$ of primitive forms properly representing m is given by

$$\frac{1}{2}(1 + 1_{2\nmid D}) \prod_{\substack{p\mid m\\ p\nmid D}} (1 + \chi_D(p)) \prod_{\substack{q\mid D\\ q^\alpha \parallel 4m\\ q^\sigma \parallel 4D}} \big(q^{\alpha/2}(1 - q^{-1}) 1_{\alpha<\sigma} 1_{\alpha \text{ even}} + q^{\lfloor \alpha/2 \rfloor} 1_{\alpha=\sigma}\big),$$

where p and q run over primes, and where the factor $1/2$ takes account of the fact that for every solution $x \in [4m]$, $x + 2m$ is the unique other solution determining the same class of forms.

Collecting everything together, we obtain the following explicit expression for r_D:

Corollary 5.1. *The total number of representations* (*proper and improper*) *of an integer m by classes of primitive forms of discriminant D satisfies*

$$\begin{aligned} r_D(m) &= \sum_{\delta^2 \mid m} r_D^*(m/\delta^2) \\ &= \frac{1 + 1_{2\nmid D}}{2} \sum_{\substack{\delta^2\mid m\\ (\delta,D)=1}} \prod_{\substack{p\nmid D\\ p^\alpha \parallel m\delta^{-2}}} (1 + \chi_D(p)) \\ &\quad \times \prod_{\substack{q\mid (D,m)\\ q^\alpha \parallel 4m\\ q^\sigma \parallel 4D}} \big(q^{\lfloor \min(\alpha,\sigma-1)/2 \rfloor} 1_{\alpha\,\text{even}} + q^{\lfloor \sigma/2 \rfloor} 1_{\alpha \equiv \sigma \,(\mathrm{mod}\, 2)} 1_{\alpha \geq \sigma}\big) \\ &\ll \sqrt{D} \sum_{d\mid m} \chi_D(d), \end{aligned}$$

where p, q run over primes.

5.2. Representation by genera. Recall that the representation function $r_g : \mathbb{N} \to \mathbb{N}$ of a genus class g was defined to be $r_g(n) = \mathbb{E}(r_{f'}(n) \mid f' \in g)$, where f' runs through a system of representatives. This function is of interest since by Lemmas 4.1 and 4.2, it has the same distribution in residue classes as any function r_f with $f \in g$. We aim to reduce the problem of determining the number of representations of an integer n by a specific genus class to that of counting certain representations of the factor n' of n that is coprime to D.

This is advantageous for the following reason. The values in $(\mathbb{Z}/D\mathbb{Z})^*$ that are represented by a form f with $D(f) = D$ form a *coset* of the subgroup in $(\mathbb{Z}/D\mathbb{Z})^*$ that is generated by the values the principal form represents (cf. [4, Lemma 2.24]). Thus, different genera represent disjoint sets of values in $(\mathbb{Z}/D\mathbb{Z})^*$. This means that the character sum expression of the function $r_{D(f)}$ which counts representations of all classes in $h(D)$ yields an arithmetic expression for the function r_g which just considers those classes of genus g. Indeed, let $\mathcal{R}_g$ denote the non-zero residues modulo D that are represented by forms in g. Then for n' *coprime* to D we have

$$r_g(n') = \frac{1}{|g|} \sum_{b \in \mathcal{R}_g} 1_{n' \equiv b \pmod{D}} \sum_{d | n'} \chi_D(d).$$

For an arbitrary positive integer n, let $n = n_D \tilde{n}^2 n'$ be the factorisation for which n' is coprime to D and n_D is the largest divisor $n_D \mid (n, D)$ such that $n/(n' n_D) = \tilde{n}^2$ is a square. This factorisation is chosen in such a way that Corollary 5.1 implies $r_D(n) = r_D(n' n_D)$, which is of interest because in $n' n_D$ the factor that is not coprime to D is bounded.

Let $\langle n' n_D, b, c\rangle$ be a primitive form properly representing $n' n_D$. Then, since $n_D \mid D$, we have $(n_D, b) > 1$ and hence $(n_D, c) = 1$ by primitiveness of the form. Since further $(n_D, n') = 1$, we have

$$\begin{aligned} \langle n' n_D, b, c\rangle &\simeq \langle c, -b, n_D n'\rangle \simeq \langle c, -b, n_D n'\rangle * \langle n_D, -b, n'c\rangle * \langle n'c, -b, n_D\rangle \\ &\simeq \langle c n_D, -b, n'\rangle * \langle n'c, -b, n_D\rangle \simeq \langle n', b, c n_D\rangle * \langle n_D, b, n'c\rangle. \end{aligned}$$

Note that all forms involved are primitive.

Thus, we can decompose the representation into separate ones for the coprime factors n' and n_D. We aim to use this multiplicative property of representation by primitive forms of fixed discriminant in conjunction with the following lemma.

Lemma 5.2. *The principle genus $\mathcal{G}_0$ is a subgroup of the class group* (*a finite abelian group*). *The genera form cosets of $\mathcal{G}_0$ in the class group.*

Proof. See e.g. [21, p. 197, Thm. 2.8]. ∎

With the help of this lemma we have

$$r_g(n) = |g| \sum_{g'} r_{g * g'^{-1}}(n_D) r_{g'}(n').$$

If the residue $n' \pmod{D}$ is representable by a form of discriminant D, then let $g_{n'}$ denote the unique genus class that represents $n' \pmod{D}$. We may use the arithmetic representation of $r_{g_{n'}}$ to obtain the following lemma.

Lemma 5.3. *Given $n = n_D n' \tilde{n}^2$ as above and a genus class g, then*

$$r_g(n) = r_{g * g_{n'}^{-1}}(n_D) \sum_{d | n'} \chi_D(d).$$

6. Representation in $\mathbb{Z}/q\mathbb{Z}$. This section contains several results on the densities $\rho_{f_i,\beta}(p^\alpha)p^{-\alpha}$, which will be established using results from the previous section and the following proposition.

PROPOSITION 6.1. *Let $P = \{q_0 m + \beta_0 : m \le M\}$ be a progression such that $D \mid q_0$ and $\beta_0 \not\equiv 0 \pmod{p^\alpha}$ for any $p^\alpha \parallel q_0$. Then*

$$\mathbb{E}_{n\in P}\sum_{d\mid n}\chi_D(d) = C\prod_{p\mid q_0}(1-\chi_D(p)p^{-1})\sum_{\alpha\ge 0}1_{p^\alpha\mid\beta_0}\chi_D(p^\alpha) + O\bigg(\frac{q_0^{1/2-\varepsilon}}{M^{1/2}}\bigg),$$

where $C = (1+\chi_D(\beta_0/(\beta_0,q_0)))L(1,\chi_D) = O(1)$.

We defer the proof to the end of the section. The following lemma is a rather immediate consequence.

LEMMA 6.2. *Let q be a positive integer that is divisible by D and let $\beta \in [q]$ be such that $\beta \not\equiv 0 \pmod{p^\alpha}$ for any $p^\alpha \parallel q$. Then*

$$\frac{\rho_{f,\beta}(q)}{q} = C'\prod_{p\mid q}(1-\chi_D(p)p^{-1})\sum_{\alpha\ge 0}1_{p^\alpha\mid\beta}\chi_D(p^\alpha),$$

where $C' = r_{g*g_{\beta'}^{-1}}(\beta_D)(1+\chi_D(\beta/(\beta,q)))h(D) = O(1)$.

Proof. By Lemmas 4.1 and 5.3 we have, for $P(M) = \{m \equiv \beta \pmod q : m \le M\}$,

$$\begin{aligned}\frac{\rho_{f,\beta}(q)}{q}\,\frac{2\pi}{k(D)\sqrt{-D}} &= \lim_{M\to\infty}\mathbb{E}_{n\in P(M)}r_f(n) = \lim_{M\to\infty}\mathbb{E}_{n\in P(M)}r_{g(f)}(n)\\ &= r_{g*g_{\beta'}^{-1}}(\beta_D)\lim_{M\to\infty}\mathbb{E}_{n\in P(M)}\sum_{d\mid n}\chi_D(d).\end{aligned}$$

By Proposition 6.1 and the class number formula the result follows. ∎

With the help of the previous lemma and a result of Stewart [22], we obtain the following more explicit information on the densities $\rho_{f_i,\beta}(p^\alpha)p^{-\alpha}$.

LEMMA 6.3.

(a) *Let p_0 be a prime that divides D and suppose that $\beta \not\equiv 0 \pmod{p_0^\alpha}$. Then*

$$\rho_{f,\beta}(p_0^\alpha)p_0^{-\alpha} = O(1)$$

as β and α vary. If $\alpha \ge v_{p_0}(D)$ and $\beta \not\equiv 0 \pmod{p_0^\alpha}$, then

$$\rho_{f,\beta}(p_0^\alpha)p_0^{-\alpha} = \rho_{f,\beta+kp_0^\alpha}(p_0^{\alpha+1})p_0^{-(\alpha+1)} \quad \text{for any } k \in \mathbb{Z}/p_0\mathbb{Z}.$$

(b) *If $p_0 \nmid D$ then for $\beta \not\equiv 0 \pmod{p_0^\alpha}$,*

$$\rho_{f,\beta}(p_0^\alpha)p_0^{-\alpha} = (1-\chi_D(p_0)p_0^{-1})\sum_{j\ge 0}1_{p_0^j\mid\beta}\chi_D(p_0^j).$$

(c) *Let p be any prime. Then $\rho_{f,0}(p^\alpha)p^{-\alpha} \ll \alpha$.*

Proof. (a) We may assume $\alpha > v_{p_0}(D)$. Let $\beta_0 \in (\mathbb{Z}/D\mathbb{Z})^*$ be a residue representable by f and let β_1 be such that $\beta_1 \equiv \beta \pmod{p_0^\alpha}$ and $\beta_1 \equiv \beta_0 \pmod{p^{v_p(D)}}$ for any prime divisor $p \neq p_0$ of D. By choice of β_0 we have $\rho_{f,\beta_1}(p^{v_p(D)}) \geq 1$ for $p \neq p_0$. The previous lemma yields

$$\frac{\rho_{f,\beta_1}(p_0^\alpha \prod_{p\mid D,\, p\neq p_0} p^{v_p(D)})}{p_0^\alpha \prod_{p\mid D,\, p\neq p_0} p^{v_p(D)}} = O(1),$$

whence the first part of (a) follows by multiplicativity of ρ. Define $\beta_2 \in \mathbb{Z}$ to be such that $\beta_2 \equiv \beta_0 \pmod{p^{v_p(D)}}$ for any prime divisor $p \neq p_0$ of D and $\beta_2 \equiv \beta + kp_0^\alpha \pmod{p_0^{\alpha+1}}$. Then, by Lemma 6.2,

$$\begin{aligned}\frac{\rho_{f,\beta}(p_0^\alpha)}{p_0^\alpha} &= \frac{\rho_{f,\beta_2}(p_0^\alpha)}{p_0^\alpha} = \frac{\rho_{f,\beta_2}(p_0^\alpha \prod_{p\mid D,\, p\neq p_0} p^{v_p(D)})}{p_0^\alpha \prod_{p\mid D,\, p\neq p_0} p^{v_p(D)}} \prod_{p\mid D,\, p\neq p_0} \biggl(\frac{\rho_{f,\beta_0}(p^{v_p(D)})}{p^{v_p(D)}}\biggr)^{-1} \\ &= r_{g*g^{-1}_{\beta'_2}}((\beta_2)_D)(1+\chi_D(\beta'_2))h(D) \prod_{p\mid D,\, p\neq p_0} \biggl(\frac{\rho_{f,\beta_0}(p^{v_p(D)})}{p^{v_p(D)}}\biggr)^{-1} \\ &= \frac{\rho_{f,\beta_2}(p_0^{\alpha+1})}{p_0^{\alpha+1}} = \frac{\rho_{f,\beta+kp_0^\alpha}(p_0^{\alpha+1})}{p_0^{\alpha+1}}.\end{aligned}$$

The proof of part (b) is almost identical. Let $\beta_0 \in (\mathbb{Z}/D\mathbb{Z})^*$ be a residue representable by f and let β_1 be such that $\beta_1 \equiv \beta \pmod{p_0^\alpha}$ and $\beta_1 \equiv \beta_0 \pmod{p^{v_p(D)}}$ for any prime $p \mid D$. Then $(\beta_1, D) = 1$ and $g(f)$ is the unique genus class representing $\beta_1 \pmod D$. Hence $r_{g(f)*g^{-1}_{\beta'_1}}(1) > 1$, as the principal genus represents 1. Since β_1 is representable by f, there is some m such that $\sum_{d\mid mD+\beta_1} \chi_D(d) > 0$, hence, in particular $\chi_D(mD+\beta_1) = \chi_D(\beta_1) = 1$. Two applications of Lemma 6.2 yield

$$\begin{aligned}\frac{\rho_{f,\beta}(p_0^\alpha)}{p_0^\alpha} = \frac{\rho_{f,\beta_1}(p_0^\alpha)}{p_0^\alpha} &= \frac{\rho_{f,\beta_1}(p_0^\alpha D)}{p_0^\alpha D}\biggl(\frac{\rho_{f,\beta_1}(D)}{D}\biggr)^{-1} \\ &= (1-\chi_D(p_0)p_0^{-1}) \sum_{j\geq 0} 1_{p_0^j\mid\beta}\chi_D(p_0^j).\end{aligned}$$

Part (c) follows from [22, Corollary 2], which implies, as shown in [2, Lemma 31], that any quadratic polynomial $P(x) = a_1x^2 + a_2x + a_3$ of discriminant $D_P = a_2^2 - 4a_1a_3$ satisfies

$$|\{x \in \mathbb{Z}/p^k\mathbb{Z} : P(x) \equiv 0 \pmod{p^k}\}| \leq 2p^{v_p(D_P)/2}.$$

Consider for fixed y the polynomial $P_y(x) = f(x,y) = ax^2 + bxy + cy^2$ of discriminant $y^2D(f)$. There are less than $p^{\alpha-k}$ values of $y \in \mathbb{Z}/p^\alpha\mathbb{Z}$ for which $p^k \parallel y$. Thus

$$\rho_{f,0}(p^\alpha) \le 2\sum_{k=0}^{\alpha-1} p^{\alpha-k} p^{k+v_p(D(f))/2} \ll \alpha p^\alpha. \ \blacksquare$$

An immediate corollary, which will be essential for the W-trick, states that the ρ-densities are constant for lifts of non-zero residues $\beta \pmod{p^\alpha}$ to higher powers of p:

Corollary 6.4. *Let p be a prime and suppose that $\alpha \ge v_p(D)$ and $\beta \not\equiv 0 \pmod{p^\alpha}$. Then*

$$\rho_{f,\beta}(p^\alpha)p^{-\alpha} = \rho_{f,\beta+kp^\alpha}(p^{\alpha+1})p^{-(\alpha+1)} \quad \text{for all } k \in \mathbb{Z}/p\mathbb{Z}.$$

Proof. This follows from parts (a) and (b) of Lemma 6.3. ■

Proof of Proposition 6.1. Multiplicativity and the assumption on β_0 yield

$$\mathbb{E}_{n\in P}\sum_{d|n}\chi_D(d) = \Big(\prod_{p|q_0}\sum_{\alpha\ge 0} 1_{p^\alpha|\beta_0}\chi_D(p^\alpha)\Big)\mathbb{E}_{m\le M}\sum_{d|qm+\beta}\chi_D(d),$$

where $(q,\beta)=1$, and q and q_0 have the same prime divisors. We will estimate the mean value of $\sum_{d|qm+\beta}\chi_D(d)$ by the hyperbola method. Recall that χ_D is a character to the modulus $\prod_{p|D}p$ (cf. [19, Ch. 9.3]) and let χ_D^* be the character to the modulus $\prod_{p|q}p$ that is induced by χ_D. (Note that q is divisible by $\prod_{p|D}p$.) Thus $\chi_D^*(n)$ is only non-zero when n is coprime to q. Then

$$\mathbb{E}_{0\le m\le M}\sum_{d|qm+\beta}\chi_D(d) = \mathbb{E}_{0\le m<M}\Big(\sum_{\substack{d|(qm+\beta)\\ d\le T}}\chi_D^*(d) + \sum_{\substack{d|(qm+\beta)\\ d>T}}\chi_D^*(d)\Big),$$

where the cut-off T will be chosen as $T=\sqrt{qM}$. We begin with the *large divisors*.

Writing $G := (\mathbb{Z}/q\mathbb{Z})^*$ and denoting its dual group by $\hat{G}$, we have

$$\mathbb{E}_{0\le m<M}\sum_{\substack{d|(qm+\beta)\\ d>T}}\chi_D^*(d) = \frac{1}{M}\sum_{n\le Mq}\frac{1}{|\hat{G}|}\sum_{\chi\in\hat{G}}\overline{\chi}(\beta)\chi(n)\sum_{\substack{d|n\\ d>T}}\chi_D^*(d).$$

Since $T^2 \ge qM$, this equals

$$\frac{1}{M}\frac{1}{|\hat{G}|}\sum_{\chi\in\hat{G}}\overline{\chi}(\beta)\sum_{m\le T}\chi(m)\sum_{T<d\le Mq/m}(\chi\chi_D^*)(d).$$

The character $\chi\chi_D^*$ is a non-principal character to the modulus q unless χ is the character χ_D^* induced by χ_D. We consider the cases $\chi=\chi_D^*$ and $\chi\ne\chi_D^*$

separately. For $\chi \neq \chi_D^*$, we have

$$\frac{1}{M}\frac{1}{|\hat{G}|}\sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_D^*}}\overline{\chi}(\beta)\sum_{m\leq T}\chi(m)\sum_{T<d\leq Mq/m}(\chi\chi_D)(d) = O(qT/M).$$

If $\chi = \chi_D^*$, we have

$$\begin{aligned}
&\frac{1}{M}\frac{1}{|\hat{G}|}\overline{\chi_D^*}(\beta)\sum_{m\leq T}\chi_D^*(m)\sum_{T<d\leq Mq/m}(\chi_D^*\chi_D)(d)\\
&\quad= \chi_D(\beta)\frac{1}{M}\frac{1}{|\hat{G}|}\sum_{\substack{n\leq Mq\\ (n,q)=1}}\sum_{m\colon m^2<n}1_{m|n}\chi_D(m)\\
&\quad= \chi_D(\beta)\frac{1}{\phi(q)M}\sum_{\substack{m\leq\sqrt{qM}\\ (m,q)=1}}\chi_D(m)\left(\frac{Mq-m^2}{m}\frac{\phi(q)}{q}+O(q)\right)\\
&\quad= \chi_D(\beta)\frac{1}{qM}\sum_{\substack{m\leq\sqrt{qM}\\ (m,q)=1}}\chi_D(m)\frac{Mq-m^2}{m}+O(\log(q)\sqrt{q/M})\\
&\quad= \chi_D(\beta)\sum_{\substack{m\leq\sqrt{qM}\\ (m,W)=1}}\frac{\chi_D(m)}{m}-\frac{\chi_D(\beta)}{qM}\sum_{\substack{m\leq\sqrt{qM}\\ (m,W)=1}}\chi_D(m)m+O(\log(q)\sqrt{q/M}).
\end{aligned}$$

The second term is seen to be small, that is, $O(\sqrt{q/M})$, by partial summation. The first sum, $\sum_{m\leq\sqrt{qM}}\chi_D^*(m)/m$, is a partial sum of the convergent series

$$\sum_{m\geq1}\frac{\chi_D^*(m)}{m}=\prod_{p|q}\left(1-\frac{\chi_D(p)}{p}\right)L(1,\chi_D)=\prod_{p|q}\left(1-\frac{\chi_D(p)}{p}\right)\frac{2\pi h(D)}{k(D)\sqrt{-D}}.$$

Bounding their difference sum by partial summation, we obtain

$$\sum_{m\leq\sqrt{qM}}\frac{\chi_D^*(m)}{m}=\prod_{p\leq w(N)}\left(1-\frac{\chi_D(p)}{p}\right)L(1,\chi_D)+O(\sqrt{q/M}).$$

Hence, the large divisors satisfy

$$\mathbb{E}_{m\leq M}\sum_{\substack{d|(qm+\beta)\\ d>T}}\chi_D^*(d)=\chi_D(\beta)\prod_{p|q}\left(1-\frac{\chi_D(p)}{p}\right)L(1,\chi_D)+O(\log(q)\sqrt{q/M}).$$

Concerning the *small divisors* sum, we obtain

$$\begin{aligned}\mathbb{E}_{m\le M}\sum_{\substack{d\mid(qm+\beta)\\ d\le T}}\chi_D^*(d) &= \frac{1}{M}\sum_{d\le T}\Big(\chi_D^*(d)\frac{M}{d}+O(1)\Big)\\ &= \sum_{d\le T}\frac{\chi_D^*(d)}{d}+O\Big(\frac{T}{M}\Big)\\ &= L(1,\chi_D)\prod_{p\mid q}\Big(1-\frac{\chi_D(p)}{p}\Big)+O\Big(\frac{q}{T}+\frac{T}{M}\Big)\\ &= L(1,\chi_D)\prod_{p\mid q}\Big(1-\frac{\chi_D(p)}{p}\Big)+O(\sqrt{q/M}).\end{aligned}$$

Putting everything together, we obtain the estimate

$$\begin{aligned}&\mathbb{E}_{0\le m\le M}\sum_{d\mid qm+\beta}\chi_D(d)\\ &\quad= (1+\chi_D(\beta))L(1,\chi_D)\prod_{p\mid q}\Big(1-\frac{\chi_D(p)}{p}\Big)+O(\log(q)\sqrt{q/M}),\end{aligned}$$

which proves the result. ∎

7. W-trick. The aim of this section is to find a decomposition of the function r_f into a sum of functions that are equidistributed in residue classes to small moduli.

In the case of primes (see [6]), this was achieved by defining $W=\prod_{p\le w(N)}p$ to be the product of primes up to $w(N)$, where $w:\mathbb{N}\to\mathbb{R}$ is a slowly growing function. For n with $\gcd(n,W)=1$ the von Mangoldt function then splits as

$$\Lambda(n)=\sum_{a\in(\mathbb{Z}/W\mathbb{Z})^*}\Lambda(n)1_{n\equiv a\,(\mathrm{mod}\,W)},$$

and it suffices to consider the functions $n\mapsto\Lambda(Wn+a)$, $a\in(\mathbb{Z}/W\mathbb{Z})^*$, which are equidistributed in residue classes to small moduli.

In the case of the divisor function, the most natural decomposition makes use of the restricted divisor function that only counts divisors coprime to W (and is thus likely to be a quasirandom function): define

$$\tau'(n):=\sum_{d\colon(d,W)=1}1_{d\mid n}.$$

Then

$$\tau(n)=\tau'(n)\sum_{w}1_{w\mid n},$$

where w runs over all integers entirely composed of primes $\leq w(N)$. The second factor, $\sum_w 1_{w|n}$, is almost periodic. Indeed, let $\alpha(p)$ be such that

$$p^{\alpha(p)-1} < (\log N)^{C_1+1} \leq p^{\alpha(p)}.$$

Then any number n that is divisible by some w as above with $p^{\alpha(p)} \mid w$ for some $p \leq w(N)$ belongs to the exceptional set X_0 from Lemma 3.2. Choosing

$$\overline{W} := \prod_{p \leq w(n)} p^{\alpha(p)},$$

one can achieve that the second factor is a periodic function of period $\overline{W}$, when adjusting the values of τ at exceptional integers. This way, it suffices to consider the functions of the form $n \mapsto \tau'(\overline{W}n + a)$ for non-zero residues $a \in [\overline{W}]$. In fact, observing that $\tau(\overline{W}n + a) = \tau'(\overline{W}n + a) \sum_{w|\overline{W}} 1_{w|a}$ for unexceptional values of a, we essentially consider functions of the form $n \mapsto \tau(\overline{W}n + a)$.

In the case of representation functions a very similar W-trick works. We use the same choice of $\overline{W}$ as in the divisor function case above.

Definition 7.1. Let $\mathcal{A}$ be the set of residues $a \pmod{\overline{W}}$ such that

$$\rho_{f,a}(\overline{W}) > 0$$

and such that $a \not\equiv 0 \pmod{p^{\alpha(p)}}$.

Thus $\mathcal{A}$ contains only residue classes that are representable by f, and every $n \in [N]$ which fails to satisfy the second condition, that is, for which $n \equiv 0 \pmod{p^{\alpha(p)}}$ holds, belongs to the exceptional set X_0 from Lemma 3.2.

Definition 7.2 (Normalised and W-tricked representation function). Let $\beta \in \mathcal{A}$ and define $r'_{f,\beta} : [N/\overline{W}] \to \mathbb{R}$ by

$$\begin{aligned} r'_{f,\beta}(m) &= \frac{k(D)\sqrt{-D}}{2\pi} r_f(\overline{W}m + \beta) \bigg(\frac{\rho_{f,\beta}(\overline{W})}{\overline{W}} \bigg)^{-1} \\ &= \frac{k(D)\sqrt{-D}}{2\pi} r_f(\overline{W}m + \beta) \prod_{p \leq w(N)} \bigg(\frac{\rho_{f,\beta}(p^{\alpha(p)})}{p^{\alpha(p)}} \bigg)^{-1}. \end{aligned}$$

Thus, by Lemma 4.1,

$$\mathbb{E}_{n \leq M} r'_{f,\beta}(m) = 1 + O(\overline{W}^3 M^{-1/2}).$$

7.1. The major arc estimate. Our next aim is to give a major arc estimate for the W-tricked function $r'_{f,b}$: we show that this function has, up to a small error, a constant average on arithmetic progressions whose common difference is small in the sense that it is $w(N)$-smooth.

Definition 7.3. An integer is called *k-smooth* when each of its prime divisors is at most k.

Proposition 7.4 (Major arc analysis for $r'_{f,\beta}$). *Let $P \subseteq [N/\overline{W}]$ be a progression of $w(N)$-smooth common difference q_1 and let $\beta \in \mathcal{A}$. If $P = \{q_1 m + q_0 : 0 \leq m < M\}$ has length M, then*

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

Proof. Corollary 6.4 implies

$$\frac{\rho_{f,\beta}(\overline{W})}{\overline{W}} = \frac{\rho_{f,\overline{W}q_0+\beta}(\overline{W}q_1)}{\overline{W}q_1}.$$

Hence the result follows from Lemma 4.1. ∎

7.2. W-tricked majorant. Finally, we need to slightly adapt our majorant function for r_f to its W-tricked version. Let $\beta \in \mathcal{A}$. Then Lemmas 4.2 and 5.3 yield the pointwise majorisation

$$\begin{aligned} r'_{f,\beta}(n) \leq \sum_{f'\sim_g f} r'_{f',\beta}(n) &= O(1)(\rho_{f,\beta}(\overline{W})\overline{W}^{-1})^{-1} \sum_{d\mid \overline{W}n+\beta} \chi_D(d) \\ &= O(1) \prod_{p<w(N)} \biggl(1 - \frac{\chi_D(p)}{p}\biggr)^{-1} \sum_{\substack{d\mid\overline{W}n+\beta \\ p\mid d \Rightarrow p>w(N)}} \chi_D(d), \end{aligned}$$

where the last step uses Lemma 6.2. Since each function $r'_{f',\beta}(n)$ has average order $1 + o(1)$, the last expression is of bounded average order. Thus, the function

$$r'_{D(f)}(n) := \sum_{\substack{d\mid n \\ p\mid d\Rightarrow p>w(n)}} \chi_D(d)$$

may be used in place of $r_{D(f)}$ to run through the construction of the majorant as in Section 2. In view of the results from that section and the remarks at the end of Section 3 we find

$$r'_{D(f)}(n) \leq \beta'_{D,\gamma}(n)\nu'_{D,\gamma}(n),$$

where

$$\nu'_{D,\gamma}(n) = \sum_{s\geq 2/\gamma}^{(\log\log N)^3} \sum_{i\geq \log_2 s-2}^{6\log\log\log N} \sum_{u\in U(i,s)} 2^s 1_{u\mid n} \tau'_{D,\gamma}(n),$$

with

$$\tau'_{D,\gamma} := \sum_{\substack{d\in\langle \mathcal{P}_D\rangle \\ p\mid d\Rightarrow p>w(N)}} 1_{d\mid n} \chi\biggl(\frac{\log d}{\log N^{2\gamma}}\biggr),$$

and

$$\beta'_{D,\gamma}(n) := \sum_{\substack{m\in\langle\mathcal{Q}_D\rangle\\ p\mid m\Rightarrow p>w(N)\\ m<N^\gamma}} \biggl(\sum_{\substack{d\in\langle\mathcal{Q}_D\rangle\\ p\mid d\Rightarrow p>w(N)}} 1_{m^2d\mid n}\mu(d)\chi\biggl(\frac{\log d}{\log N^\gamma}\biggr)\biggr)^2.$$

For the two factors $\beta'_{D,\gamma}$ and $\nu'_{D,\gamma}$ one shows in the same way as for the original majorants that

$$C(\beta'_{D,\gamma}) := \sqrt{\log N} \prod_{\substack{q\in\mathcal{Q}_D\\ q\le w(N)}} (1+q^{-1})^{-1}\mathbb{E}_{n\le N}\beta'_{D,\gamma}(n)$$

and

$$C(\nu'_{D,\gamma}) := \frac{1}{\sqrt{\log N}} \prod_{\substack{p\in\mathcal{P}_D\\ p<w(N)}} (1-p^{-1})^{-1}\mathbb{E}_{n\le N}\nu'_{D,\gamma}(n)$$

are bounded independently of N. Since $\beta'_{D,\gamma}$ and $\nu'_{D,\gamma}$ are given by short divisor sums running over coprime sets of divisors, the average order of their product satisfies

$$\mathbb{E}_{n\le N}\beta'_{D,\gamma}(n)\nu'_{D,\gamma}(n) = \mathbb{E}_{n\le N}\beta'_{D,\gamma}(n)\mathbb{E}_{m\le N}\nu'_{D,\gamma}(m) + N^{O(\gamma)-1}.$$

Indeed, for coprime integers $y_1, y_2 < N^\gamma$, we have

$$\mathbb{E}_{n\le N}1_{y_1y_2\mid n} = \frac{1}{y_1y_2} + O(N^{2\gamma-1}) = \mathbb{E}_{n\le N}1_{y_1\mid n}\mathbb{E}_{n\le N}1_{y_2\mid n} + O(N^{2\gamma-1}),$$

and since the total number of divisors in the sum $\mathbb{E}_{n\le N}\beta'_{D,\gamma}(n)\nu'_{D,\gamma}(n)$ is $N^{O(\gamma)}$, the statement follows.

Since $\prod_{p\le w(N)}(1-\chi_D(p)p^{-1})^{-1} = C+o(1)$ for some constant C, we have proved the following lemma.

Lemma 7.5 (W-tricked majorant). *Let $\beta\in\mathcal{A}$. Then*

$$r'_{f,\beta}(m) \le \beta'_{D,\gamma}(\overline{W}m+\beta)\nu'_{D,\gamma}(\overline{W}m+\beta)$$

for all $m\le N/\overline{W}$. Furthermore, there is a positive real number $C_{D,\gamma}=O(1)$ such that

$$\mathbb{E}_{n\le N}\frac{\beta'_{D,\gamma}(n)\nu'_{D,\gamma}(n)}{C_{D,\gamma}} = 1+o(1).$$

8. Local factors and the reduction of the main theorem to a W-tricked version. Define the smoothed representation function $\bar{r}_f : [N]\to\mathbb{R}$ by

$$\bar{r}_f(n) := r_f(n)1_{n \,(\mathrm{mod}\,\overline{W})\in\mathcal{A}}.$$

According to the definition of $\mathcal{A}$, this function satisfies the conditions of Lemma 3.3. Thus it suffices to study correlations of functions $\bar{r}_f$ in order to prove the main theorem. As the main theorem will show, the asymptotic behaviour of these correlations,

$$\sum_{n\in K\cap\mathbb{Z}^d} \bar r_{f_1}(\psi_1(n))\dots\bar r_{f_t}(\psi_t(n)), \tag{8.1}$$

is determined by the local behaviour of the affine-linear system Ψ modulo small primes.

By splitting the summation range into progressions of common difference $\overline{W}$, we reduce the task of estimating (8.1) to an assertion (Proposition 8.1 below) about the uniformity of the W-tricked representation functions. Local factors measuring irregularities of the system Ψ modulo small primes will appear in this process.

Define for fixed quadratic forms $f_1,\dots,f_t$ and for an affine-linear system $\Psi:\mathbb{Z}^d\to\mathbb{Z}^t$ the set of residues

$$\begin{aligned}\mathcal{A}_\Psi &:= \{a\in[\overline{W}]^d : \psi_i(a)\in\mathcal{A}_{f_i} \text{ for all } i\in[t]\}\\ &= \Big\{a\in[\overline{W}]^d : \prod_{i=1}^t \rho_{f_i,\psi_i(a)}(\overline{W})>0 \text{ and } \prod_{i=1}^t \psi_i(a)\not\equiv 0 \ (\mathrm{mod}\ p^{v_p(\overline{W})})\Big\}.\end{aligned}$$

Notice that any n with non-zero contribution to (8.1) is congruent modulo $\overline{W}$ to an element of this set. For a fixed element $a\in\mathcal{A}_\Psi$ let $\tilde\Psi=(\tilde\psi_1,\dots,\tilde\psi_t):\mathbb{Z}^d\to\mathbb{Z}^t$ be the affine-linear system satisfying

$$\psi_i(\overline{W}m+a)=\overline{W}\tilde\psi_i(m)+c_i(a)$$

with $c_i(a)\in[\overline{W}]$. Thus, $\psi_i(a)\equiv c_i(a)\ (\mathrm{mod}\ \overline{W})$, and ψ_i and $\tilde\psi_i$ only differ in the constant term.

The main result will be deduced from the following proposition.

Proposition 8.1. *Let $\Psi:\mathbb{Z}^d\to\mathbb{Z}^t$ be a finite complexity system of forms, let $a\in\mathcal{A}_\Psi$, and let $\tilde\Psi:\mathbb{Z}^d\to\mathbb{Z}^t$ be defined as above. Then*

$$\sum_{m\in\mathbb{Z}^d\cap K'}\prod_{i=1}^t r'_{f_i,c_i(a)}(\tilde\psi_i(m)) = \mathrm{vol}(K')+o((N/\overline{W})^d),$$

where $K'\subseteq[-N/\overline{W},N/\overline{W}]^d$ is a convex body with $\overline{W}\tilde\Psi(K')+c(a)\subseteq[1,N]^t$.

For every $a\in\mathcal{A}_\Psi$, define the convex body

$$K_a:=\{x\in\mathbb{R}^d:\overline{W}x+a\in K\}$$

and note that $\mathrm{vol}(K_a)=\mathrm{vol}(K)/\overline{W}^d$. Then we can rewrite (8.1) by means of Proposition 8.1 as follows:

$$
\begin{aligned}
(8.2)\qquad &\sum_{n\in K\cap\mathbb{Z}^d} \bar{r}_{f_1}(\psi_1(n))\ldots\bar{r}_{f_t}(\psi_t(n))\\
&= \sum_{a\in\mathcal{A}_\Psi}\sum_{m\in K_a\cap\mathbb{Z}^d}\prod_{i=1}^t r_{f_i}(\psi_i(\overline{W}m+a))\\
&= \sum_{a\in\mathcal{A}_\Psi}\sum_{m\in K_a\cap\mathbb{Z}^d}\prod_{i=1}^t r'_{f_i,c_i(a)}(\tilde{\psi}_i(m))\frac{\rho_{f_i,\psi_i(a)}(\overline{W})}{\overline{W}}\,\frac{2\pi}{k(D_i)\sqrt{-D_i}}\\
&= \frac{\mathrm{vol}(K)+o(N^d)}{\overline{W}^d}\sum_{a\in\mathcal{A}_\Psi}\prod_{i=1}^t\frac{\rho_{f_i,\psi_i(a)}(\overline{W})}{\overline{W}}\,\frac{2\pi}{k(D_i)\sqrt{-D_i}}\\
&= \Bigg(\mathrm{vol}(K)\prod_{j=1}^t\frac{2\pi}{k(D_j)\sqrt{-D_j}}+o(N^d)\Bigg)\mathbb{E}_{a\in[\overline{W}]^d}1_{a\in\mathcal{A}_\Psi}\prod_{i=1}^t\frac{\rho_{f_i,\psi_i(a)}(\overline{W})}{\overline{W}}.
\end{aligned}
$$

By the Chinese remainder theorem, the above expectation is in fact a product over local densities, that is

$$
\begin{aligned}
(8.3)\qquad &\mathbb{E}_{a\in[\overline{W}]^d}1_{a\in\mathcal{A}_\Psi}\prod_{i=1}^t\frac{\rho_{f_i,\psi_i(a)}(\overline{W})}{\overline{W}}\\
&\qquad= \prod_{p<w(N)}\mathbb{E}_{a\in(\mathbb{Z}/p^{\alpha(p)}\mathbb{Z})^d}\prod_{i=1}^t\frac{\rho_{f_i,\psi_i(a)}(p^{\alpha(p)})}{p^{\alpha(p)}}1_{\psi_i(a)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha(p)})},
\end{aligned}
$$

where $\alpha(p)=v_p(\overline{W})$. To complete the proof that (8.2) and (8.3) indeed imply the main theorem, two further lemmas are required. The first shows that the above factors at primes are essentially local factors:

LEMMA 8.2 (Local factors). *Let p be a prime. Then*

$$
\mathbb{E}_{a\in(\mathbb{Z}/p^{\alpha(p)}\mathbb{Z})^d}\prod_{i=1}^t\frac{\rho_{f_i,\psi_i(a)}(p^{\alpha(p)})}{p^{\alpha(p)}}1_{\psi_i(a)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha(p)})}=\beta_p+O((\log N)^{-C_1/5}),
$$

where

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

is the local factor at p.

The second lemma is an estimate of the local factors.

LEMMA 8.3. *Let $\Psi=(\psi_1,\ldots,\psi_t):\mathbb{Z}^d\to\mathbb{Z}^d$ be a system of affine-linear forms for which no two forms ψ_i and ψ_j are affinely dependent, and all of whose linear coefficients are bounded by L. Then*

$$
\beta_p=1+O_{t,d,L}(p^{-2}).
$$

Thus,

$$\prod_{p \le w(N)} \beta_p = \left(1 + O_{t,d,L}\left(\frac{1}{w(N)}\right)\right) \prod_p \beta_p.$$

A second consequence of this lemma is that

$$\beta_p + O((\log N)^{-C_1/5}) = \beta_p(1 + O((\log N)^{-C_1/5})) \quad \text{for all } p \gg 1.$$

For the remaining $p \ll 1$, we require an upper bound on β_p. Since Lemma 6.3 implies $\rho_{f_i,A}(p^{\alpha(p)})p^{-\alpha(p)} \ll \alpha(p) \ll \log\log N$ for any $A \in \mathbb{Z}/p^{\alpha(p)}\mathbb{Z}$, we may deduce from Lemma 8.2 the very crude bound $\beta_p \ll (\log\log N)^t$. Thus, by (8.2), (8.3) and the two lemmas stated above, we obtain

$$\begin{aligned}
\sum_{n \in K \cap \mathbb{Z}^d} & \bar{r}_{f_1}(\psi_1(n)) \ldots \bar{r}_{f_t}(\psi_t(n)) \\
&= (\beta_\infty + o(N^d)) \prod_{p < w(N)} \left(\beta_p + O((\log N)^{-C_1/5})\right) \\
&= (\beta_\infty + o(N^d))\left(1 + O((\log N)^{-C_1/5})\right)^{\pi(w(N))} \\
&\quad \times \left(\prod_{p < w(N)} \beta_p + O\left(\frac{(\log\log N)^{O(t)}}{(\log N)^{C_1/5}}\right)\right) \\
&= \beta_\infty \prod_{p < w(N)} \beta_p + o(N^d) = \beta_\infty \prod_p \beta_p + o(N^d),
\end{aligned}$$

where we used that $w(N) = \log\log N$. Apart from the proof of the two lemmas, we have reduced the task of establishing the main theorem to that of proving Proposition 8.1.

We conclude this section with the proofs of the lemmas, for the purpose of which the following notion is introduced.

Definition 8.4 (Local divisor densities). For a given system $\Psi = (\psi_1, \ldots, \psi_t)$ of affine-linear forms, positive integers $d_1, \ldots, d_t$ and their least common multiple $m := \operatorname{lcm}(d_1, \ldots, d_t)$ define *local divisor densities* by

$$\alpha_\Psi(d_1, \ldots, d_t) := \mathbb{E}_{n \in (\mathbb{Z}/m\mathbb{Z})^d} \prod_{i \in [t]} 1_{\psi_i(n) \equiv 0 \,(\mathrm{mod}\, d_i)}.$$

Proof of Lemma 8.2. We shall show more precisely that β_p satisfies

$$\begin{aligned}
(8.4) \quad \beta_p = {} & \mathbb{E}_{a \in (\mathbb{Z}/p^{\alpha(p)}\mathbb{Z})^d} \prod_{i=1}^{t} \frac{\rho_{f_i,\psi_i(a)}(p^{\alpha(p)})}{p^{\alpha(p)}} 1_{\psi_i(a) \not\equiv 0 \,(\mathrm{mod}\, p^{\alpha(p)})} \\
& + O((\alpha(p))^t) \sum_{\substack{a_1,\ldots,a_t: \\ M := \max_i a_i \ge \alpha(p)}} \mathbb{E}_{a \in (\mathbb{Z}/p^M\mathbb{Z})^d} \prod_{i=1}^{t} 1_{\psi_i(a) \equiv 0 \,(\mathrm{mod}\, p^{a_i})}.
\end{aligned}$$

Suppose $m > \alpha(p)$. We split the sum $\mathbb{E}_{a\in(\mathbb{Z}/p^m\mathbb{Z})^d}\prod_{i=1}^t \rho_{f_i,\psi_i(a)}(p^m)p^{-m}$ over residues a into two parts according to whether

$$\prod_{i=1}^t 1_{\psi_i(a)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha(p)})} = 1 \text{ or } 0.$$

First note that for any a with $\psi_i(a)\not\equiv 0 \pmod{p^j}$ for all $i\in[t]$, any lift $\Psi(a+kp^j)$, $k\in[p]^d$, is componentwise divisible to the same powers of p as $\Psi(a)$. Hence, Corollary 6.4 implies

$$\begin{aligned}\mathbb{E}_{a\in(\mathbb{Z}/p^m\mathbb{Z})^d}&\prod_{i=1}^t \frac{\rho_{f_i,\psi_i(a)}(p^m)}{p^m} 1_{\psi_i(a)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha(p)})}\\ &= \mathbb{E}_{a\in(\mathbb{Z}/p^{\alpha(p)}\mathbb{Z})^d}\prod_{i=1}^t \frac{\rho_{f_i,\psi_i(a)}(p^{\alpha(p)})}{p^{\alpha(p)}} 1_{\psi_i(a)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha(p)})}.\end{aligned}$$

Thus, the terms of the first type give rise to the main term of (8.4). Combining parts (a)–(c) of Lemma 6.3 yields the general bound

$$\frac{\rho_{f_i,\psi_i(a)}(p^m)}{p^m} \ll \sum_{k=0}^m 1_{\psi_i(a)\equiv 0\,(\mathrm{mod}\,k)},$$

which shows that terms of the second type are bounded by

$$O((\alpha(p))^t) \sum_{\substack{0\leq a_1,\dots,a_t\leq m:\\ M:=\max_i a_i\geq \alpha(p)}} \mathbb{E}_{a\in(\mathbb{Z}/p^M\mathbb{Z})^d}\prod_{i=1}^t 1_{\psi_i(a)\equiv 0\,(\mathrm{mod}\,p^{a_i})}.$$

This proves the above expression for β_p. In order to establish the lemma, it thus remains to bound the sum over divisor densities

$$\delta_p := \sum_{\substack{a_1,\dots,a_t\\ M:=\max_i a_i\geq \alpha(p)}} \alpha_\Psi(p^{a_1},\dots,p^{a_t}).$$

Since the coefficients of $\dot{\Psi}$ are bounded, we have

$$\alpha_\Psi(p^{a_1},\dots,p^{a_t}) = \mathbb{E}_{n\in(\mathbb{Z}/p^{\max_i a_i}\mathbb{Z})^d}\prod_{i=1}^t 1_{\psi_i(n)\equiv 0\,(\mathrm{mod}\,p^{a_i})} \ll p^{-\max_i a_i},$$

which yields

$$\delta_p \ll \sum_{\substack{a_1,\dots,a_t\\ \max_i a_i\geq \alpha(p)}} p^{-\max_i a_i}.$$

Recall that

$$\alpha(p) = v_p(\overline{W}) = (C_1+1)\frac{\log\log N}{\log p} + O(1)$$

for some sufficiently large integer C_1. Estimating the number of tuples $(a_1,\dots,a_t)$ with $\max_i a_i = j$ crudely by $(j+1)^t$, we conclude that for $p \le w(n) = \log\log N$,

$$\begin{aligned}\delta_p &\ll \sum_{j \ge C_1(\log\log N)/2\log p} p^{-j} j^t \ll \sum_{j \ge C_1(\log\log N)/2\log p} p^{-j/2} \\ &\ll (\log N)^{-C_1/4}.\end{aligned}$$

Hence, $(\alpha(p))^t \delta_p \ll (\log N)^{-C_1/5}$, which proves the result. ■

Proof of Lemma 8.3. We may assume that p is large enough so that $p \nmid D_1 \dots D_t$. For such primes Lemma 6.3(c) yields

$$\begin{aligned}\beta_p &= \lim_{m\to\infty} \mathbb{E}_{a \in (\mathbb{Z}/p^m\mathbb{Z})^d} \prod_{j\in[t]} \frac{\rho_{f_i,\psi_i(a)}(p^m)}{p^m} \\ &= \lim_{m\to\infty} \mathbb{E}_{a \in (\mathbb{Z}/p^m\mathbb{Z})^d} \prod_{i=1}^{t} (1-\chi_{D_i}(p)p^{-1}) \sum_{j\ge 0} 1_{p^j \mid \psi_i(a)} \chi_{D_i}(p^j) \\ &= \sum_{a_1,\dots,a_t} \alpha(p^{a_1},\dots,p^{a_t}) \prod_{j\in[t]} (1-\chi_{D_j}(p)p^{-1})\chi_{D_j}(p^{a_j}).\end{aligned}$$

By splitting the sum $\sum_{a_1,\dots,a_t}$ into terms according to whether no a_i is non-zero, exactly one a_i is non-zero, or at least two a_i are non-zero, we obtain

$$\begin{aligned}\beta_p &= \sum_{a_1,\dots,a_t} \alpha(p^{a_1},\dots,p^{a_t}) \prod_{j\in[t]} (1-\chi_{D_j}(p)p^{-1})\chi_{D_j}(p^{a_j}) \\ &= \prod_{j\in[t]} (1-\chi_{D_j}(p)p^{-1}) \Big\{ 1 + \sum_{i=1}^{t} \sum_{a_i>0} \chi_{D_i}(p^{a_i}) p^{-a_i} \Big\} \\ &\quad + O\Big(\sum_{\substack{a_1,\dots a_t \\ \text{at least two } a_i>0}} \alpha(p^{a_1},\dots p^{a_t}) \Big).\end{aligned}$$

Here we used the fact that, for sufficiently large p with respect to t, d and L, we have $\alpha(p^{a_1},\dots,p^{a_t}) = p^{-a_i}$ whenever a_i is the only non-zero exponent.

It is easy to see that the main term equals $1 + O_t(p^{-2})$. Concerning the error term, we employ the fact that we are dealing with a finite complexity system of forms, i.e., no two forms are affinely related. For every p which is sufficiently large with respect to t, d, L we have

$$\alpha(p^{a_1},\dots,p^{a_t}) \le p^{-\max_{i\ne j}(a_i+a_j)} \le p^{-1-\max_i a_i}$$

whenever at least two a_i are non-zero. There are at most tj^{t-1} choices of coefficients $a_1,\dots,a_t$ that satisfy $\max_i a_i = j$, and thus the contribution of the error term to the value of β_p may be bounded by

$$O\Big(\sum_{j\geq 1} tj^{t-1}p^{-j-1}\Big) = O_t(p^{-2}).$$

This proves the lemma. ∎

Simultaneous majorant. To summarise, we reduced the task of proving the main theorem to that of proving Proposition 8.1. This will be carried out by the nilpotent Hardy–Littlewood method in the remainder of this paper. In order to apply the method, specifically Proposition 10.1 below, we require, for every occurring collection of $\{r'_{f_i,c_i(a)} : i = 1,\dots,t\}$, $a \in \mathcal{A}_\Psi$, a pseudorandom majorant that simultaneously majorises all $r'_{f_i,c_i(a)}$. The function $\sigma_{(f_i),a} : [N/\overline{W}] \to \mathbb{R}^+$,

$$\sigma_{(f_i),a}(m) := \mathbb{E}_{i\in[t]} \frac{\beta'_{D_i,\gamma}(\overline{W}m + b_i(a))\nu'_{D_i,\gamma}(\overline{W}m + b_i(a))}{C_{D_i,\gamma}}, \tag{8.5}$$

has the required majorant property.

9. Linear forms and correlation conditions. In this section we check that the majorant $\sigma_{(f_i),a}$ defined in (8.5) for a collection of W-tricked representation functions $r'_{f_1,c_1(a)},\dots,r'_{f_t,c_t(a)}$ is (after a minor technical modification) indeed a pseudorandom measure, that is, satisfies the linear forms and correlation conditions.

Write $M = N/\overline{W}$, let M' be a prime satisfying $M < M' \leq O_{t,d,L}(M)$, and define $\sigma^*_{(f_i),a} : [M'] \to \mathbb{R}^+$ by

$$\sigma^*_{(f_i),a}(n) = \begin{cases} \frac{1}{2}(1 + \sigma_{(f_i),a}(n)) & \text{if } n \leq M, \\ 1 & \text{if } M < n \leq M'. \end{cases}$$

As is seen in [8, App. D], $\sigma^*_{(f_i),a}$ is D-pseudorandom if the following two propositions, which are technical reductions of the linear forms and correlation conditions from [8], hold true.

Proposition 9.1 (D-Linear forms estimate). *Let $1 \leq d,t \leq D$ and let $(i_1,\dots,i_t) \in [t]^t$ be an arbitrary collection of indices. For any finite complexity system $\Psi : \mathbb{Z}^d \to \mathbb{Z}^t$ with bounded coefficients $\|\Psi\|_N \leq D$ and every convex body $K \subseteq [0,N]^d$ such that $\Psi(K) \subseteq [1,N/\overline{W}]^t$, we have*

$$\begin{aligned} \mathbb{E}_{n\in\mathbb{Z}^d\cap K} \prod_{j\in[t]} \nu'_{D_{i_j},\gamma}(\overline{W}\psi_j(n) + b_{i_j})\beta'_{D_{i_j},\gamma}(\overline{W}\psi_j(n) + b_{i_j}) \\ = \bigg(1 + O_D\Big(\frac{N^{d-1+O_D(\gamma)}}{\mathrm{vol}(K)}\Big) + o_D(1)\bigg) \prod_{j=1}^{t} C_{D_{i_j},\gamma} \end{aligned} \tag{9.1}$$

provided γ is small enough.

Proposition 9.2 (Correlation estimate). *For every $1 < m_0 \leq D$ there exists a function $\sigma_{m_0} : \mathbb{Z}_{M'} \to \mathbb{R}^+$ with bounded moments $\mathbb{E}_{n \in \mathbb{Z}_{M'}} \sigma_{m_0}^q(n) \ll_{m,q} 1$ such that for every interval $I \subset \mathbb{Z}_{M'}$, every $1 \leq m \leq m_0$ and every m-tuple $(i_1, \ldots, i_m) \in [t]^m$ and every choice of* (*not necessarily distinct*) *$h_1, \ldots, h_m \in \mathbb{Z}_{M'}$ we have*

$$\mathbb{E}_{n\in I} \prod_{j\in[m]} \nu'_{D_{i_j},\gamma}(\overline{W}(n+h_j)+b_{i_j})\beta'_{D_{i_j},\gamma}(\overline{W}(n+h_j)+b_{i_j}) \leq \sum_{1\leq i<j\leq m} \sigma_{m_0}(h_i-h_j)$$

provided γ is small enough.

Recall that the W-tricked majorant $\nu'_{D_j,\gamma}(\overline{W}m+b_j(a))\beta'_{D_j,\gamma}(\overline{W}m+b_j(a))$ for $r'_{f_j,a}$ has divisor sum structure:

$$\begin{aligned}(9.2)\qquad & \nu'_{D_j,\gamma}(n)\beta'_{D_j,\gamma}(n) \\ &= \Bigg(\sum_{s=2/\gamma}^{(\log\log N)^3} \sum_{i=\log_2 s-2}^{6\log\log\log N} \sum_{u\in U(i,s)} \sum_{\substack{d\in\langle \mathcal{P}_{D_j}\rangle \\ (d,uW)=1}} \sum_{v|u} 2^s 1_{d|n} 1_{u|n} \chi\bigg(\frac{\log d}{\log N^{2\gamma}}\bigg)\Bigg) \\ &\quad \times \Bigg(\sum_{\substack{m_j\in\langle \mathcal{Q}_{D_j}\rangle \\ (m_j,W)=1}} \chi\bigg(\frac{\log m_j}{\log N^{2\gamma}}\bigg) 1_{m_j^2|n} \bigg(\sum_{\substack{\varepsilon\in\langle Q_{D_i}\rangle \\ (\varepsilon,W)=1}} 1_{\varepsilon m_j^2|n}\mu(\varepsilon)\chi\bigg(\frac{\log\varepsilon}{\log N^{\gamma}}\bigg)\bigg)^2\Bigg).\end{aligned}$$

The function χ above is a cut-off. As no characters appear in this section, there is no danger of confusion.

Our strategy to prove the linear forms estimate is as follows. The first step is to show that in order to asymptotically evaluate (9.1) we may ignore all terms that arise from divisor densities of *dependent* divisibility events, that is, events $\{n : \prod_{i\in[t]} 1_{a_i|\psi_i(n)}\}$ where $(a_1, \ldots, a_t)$ are not pairwise coprime. The second step is the observation that the densities of independent divisibility events are, up to a small error, independent of the system Ψ of forms, which will finally allow us to reduce the verification of the linear forms condition to the task of verifying it separately for each of the two factors of each of the majorants in the case where $\Psi : \mathbb{Z} \to \mathbb{Z}$ is the identity function. The same strategy was used in [18, §6].

The main tool to exploit the divisor sum structure of our majorants is the following simple lemma (see [8, App. A] for a proof).

Lemma 9.3 (Volume packing argument). *Let $K \subseteq [-B, B]^d$ be a convex body and Ψ a system of affine-linear forms. Then*

$$\sum_{n\in\mathbb{Z}^d\cap K} \prod_{i\in[t]} 1_{d_i|\psi_i(n)} = \mathrm{vol}(K)\alpha(d_1, \ldots, d_t) + O(B^{d-1}\,\mathrm{lcm}(d_1, \ldots, d_t)).$$

In order to remove the above mentioned dependent divisibility events, we need to replace χ by a multiplicative function. A way to achieve this has been found by Goldston and Yıldırım and was employed and modified by Green and Tao [8] to check the linear forms condition for their majorant function for W-tricked primes. In this respect, the proof of Proposition 9.1 below builds on [8, App. D]. In particular, we shall employ many of the small technical arguments from there.

Recall that the cut-off χ was chosen to be a smooth, compactly supported function. Let ϑ be the modified Fourier transform of χ, defined via

$$e^x\chi(x) = \int_{\mathbb{R}} \vartheta(\xi) e^{-ix\xi}\, d\xi.$$

Fourier inversion, compact support and smoothness of χ, and partial integration yield the bound

$$\vartheta(\xi) \ll_A (1+|\xi|)^{-A}$$

for all $A > 0$. Green and Tao make use of this rapid decay to truncate the integral representation of χ as follows. Let $I = \{\xi \in \mathbb{R} : |\xi| \leq \log^{1/2} N^\gamma\}$, then for any $A > 0$,

$$\begin{aligned}\chi\biggl(\frac{\log m}{\log N^\gamma}\biggr) &= \int_{\mathbb{R}} m^{-\frac{1+i\xi}{\log N^\gamma}} \vartheta(\xi)\, d\xi \\ &= \int_{I} m^{-\frac{1+i\xi}{\log N^\gamma}} \vartheta(\xi)\, d\xi + O_A(m^{-1/\log N^\gamma} \log^{-A} N^\gamma).\end{aligned} \tag{9.3}$$

Later on, this truncation will simplify the process of swapping integrals and summations. We proceed to check the linear forms estimate.

Proof of Proposition 9.1. Define the system $\varPhi = (\varphi_j)_{j\in[t]} : \mathbb{Z}^d \to \mathbb{Z}^t$ by $\varphi_j(n) := \overline{W}\psi_j(n) + b_{i_j}$. A prime p is called *exceptional* for $\varPhi$ if the reduction of $\varPhi$ modulo p has affinely dependent forms. For the system defined here, all exceptional primes are bounded by $w(N) + O(D)$. All information we will use about $\varPhi$ is the bound on exceptional primes and the fact that it has finite complexity. Consider an arbitrary cross term that appears on the left hand side of (9.1) when inserting the definition (9.2) and fixing the parameters s_j, i_j, u_j for each factor. That is, we consider

$$\begin{aligned}\mathbb{E}_{n\in\mathbb{Z}^d\cap K} \prod_{j\in[t]} \Biggl(\sum_{\substack{d_j \in \langle \mathcal{P}_{D_j}\rangle \\ (d_j, u_j W)=1}} \sum_{v_j | u_j} 2^{s_j} 1_{d_j u_j | \varphi_j(n)} \chi\biggl(\frac{\log d_j}{\log N^\gamma}\biggr)\Biggr) \\ \times \sum_{\substack{m_j \in \langle \mathcal{Q}_{D_i}\rangle \\ (m_j, W)=1}} \chi\biggl(\frac{\log m_j}{\log N^\gamma}\biggr) \Biggl(\sum_{e_j \in \langle \mathcal{Q}_{D_i}\rangle} 1_{e_j m_j^2 | \varphi_j(n)} \mu(e_j) \chi\biggl(\frac{\log e_j}{\log N^\gamma}\biggr)\Biggr)^2\end{aligned}$$

$$= \sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \Bigg(\prod_{j\in[t]} 2^{s_j}\mu(e_j)\mu(e'_j)\tau(u_j) \prod_{\substack{x\in\\ \{d_j,m_j,e_j,e'_j\}}} \chi\Big(\frac{\log x}{\log N^\gamma}\Big)\Bigg) \times \mathbb{E}_{n\in\mathbb{Z}^d\cap K} \prod_{i\in[t]} 1_{u_i d_i m_i^2 \varepsilon_i | \varphi_i(n)},$$

where $\varepsilon_i = \mathrm{lcm}(e_i, e'_i)$ and where we denote by bold letters such as $\mathbf{d}$ any t-tuple of positive $w(N)$-smooth integers which we shall implicitly assume to satisfy the correct multiplicative restrictions, e.g. $d_i \in \langle \mathcal{P}_i \rangle$ and $(d_i, v_i W) = 1$ in this case.

Note that $u_j d_j m_j^2 \varepsilon_j = N^{O(\gamma)}$ for all summands with non-zero contribution. Indeed, $d_j, e_j, e'_j, m_j \leq N^\gamma$ by definition of the cut-off. We have $u_j < N^\gamma$ by construction of the divisor majorant, as the u_j arise as divisors of certain numbers bounded by N^γ (cf. also the remarks following Proposition 4.2 of [18]). Therefore, the volume packing lemma implies

$$\begin{aligned}&\mathbb{E}_{n\in\mathbb{Z}^d\cap K} \prod_{i\in[t]} 2^{s_i}\tau(u_i) 1_{u_i d_i m_i^2 \varepsilon_i | \varphi_i(n)} \\ &= \alpha_\Phi(u_1 d_1 m_1^2 \varepsilon_1, \dots, u_t d_t m_t^2 \varepsilon_t) \prod_{i\in[t]} 2^{s_i}\tau(u_i) + O(M^{d-1+O(\gamma)}/\mathrm{vol}(K)),\end{aligned}$$

where the bound $2^{s_j} \leq 2^{(\log\log N)^3} \ll M^\gamma$ allowed to hide the factors 2^{s_j} in the error term.

Since $u_j d_j m_j^2 \varepsilon_j = N^{O(\gamma)}$, there are only $N^{O(\gamma)}$ terms altogether in all sums of the majorant, including those over s_j, i_j and u_j. This and the boundedness of χ imply that the volume packing error term has a total contribution of $O(M^{d-1+O(\gamma)}/\mathrm{vol}(K))$ towards (9.1), and we are left with the main term, that is,

$$\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \alpha_\Phi((u_i d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} 2^{s_j}\mu(e_j)\mu(e'_j)\tau(u_j) \prod_{x\in\{d_j,m_j,e_j,e'_j\}} \chi\Big(\frac{\log x}{\log N^\gamma}\Big).$$

Next we show that we may assume that each u_i is coprime to $u_j d_j m_j^2 \varepsilon_j$ for all $j \neq i$ and that $(u_i, d_i m_i^2 \varepsilon_i) = 1$. These properties yield

$$\alpha_\Phi(u_1 d_1 m_1^2 \varepsilon_1, \dots, u_t d_t m_t^2 \varepsilon_t) = \alpha_\Phi(d_1 m_1^2 \varepsilon_1, \dots, d_t m_t^2 \varepsilon_t) \frac{1}{u_1 \dots u_t}.$$

We shall also abbreviate $\mathbf{u} = (u_1, \dots, u_t)$, implicitly assuming that the conditions $u_j \in U(i_j, s_j)$ on these tuples still apply.

Claim 2. *For all choices of $(s_j)_{j\in[t]}$ and $(i_j)_{j\in[t]}$ we have*

$$\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}\sum_{\mathbf{u}}\alpha_{\Phi}((u_i d_i m_i^2\varepsilon_i)_{i\in[t]})\prod_{j\in[t]}2^{s_j}\mu(e_j)\mu(e_j')\tau(u_j) \times\prod_{x\in\{d_j,m_j,e_j,e_j'\}}\chi\Big(\frac{\log x}{\log N^{\gamma}}\Big)$$
$$=\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}\alpha_{\Phi}((d_i m_i^2\varepsilon_i)_{i\in[t]})\sideset{}{'}\sum_{u_1,\dots,u_t}\prod_{j\in[t]}\frac{2^{s_j}\tau(u_j)}{u_j}\mu(e_j)\mu(e_j') \times\prod_{x\in\{d_j,m_j,e_j,e_j'\}}\chi\Big(\frac{\log x}{\log N^{\gamma}}\Big)+O_D(N^{-(\log\log N)^{-4}}),$$

where $\sum'$ indicates that the sum is extended only over choices $(u_1,\dots,u_t)$ satisfying the coprimality conditions $(u_i,u_jd_jm_j^2\varepsilon_j)=1$ whenever $i\neq j$ and $(u_i,d_im_i^2\varepsilon_i)=1$ for $i\in[t]$.

Proof. We have to bound the contribution from the excluded choices of $(u_1,\dots,u_t)$. Any prime divisor of any u_i is at least as large as $N^{1/(\log\log N)^3}$ by construction. Thus, whenever the coprimality conditions fail, the divisibility events we are considering are included in $\{n : p^2\mid\prod_{i\in[t]}\phi_i(n)\}$ for some $p>N^{1/(\log\log N)^3}$. By finite complexity and the bounds on exceptional primes of Φ, we have

$$\sum_{\substack{N^{(\log\log N)^{-3}}\\<p<N^{\gamma}}}\mathbb{E}_{n\in\mathbb{Z}^d\cap K}1_{p^2\mid\prod_i\phi_i(n)}\ll_t\sum_{\substack{N^{(\log\log N)^{-3}}\\<p<N^{\gamma}}}p^{-2}=O_t(N^{-(\log\log N)^{-3}}).$$

We will make use of this with the help of Cauchy–Schwarz. Since $2^{s_j}\le 2^{(\log\log N)^3}$ and since χ^2 is at most 1, we can crudely bound the following second moment:

$$\mathbb{E}_{n\in\mathbb{Z}^d\cap K}\prod_{i\in[t]}\Big(\sum_{\mathbf{d},\mathbf{m},\mathbf{u},\mathbf{e},\mathbf{e}'}1_{u_id_im_i^2\varepsilon_i\mid\psi_i(n)}2^{s_i}\tau(u_i)\prod_{x\in\{d_j,m_j,e_j,e_j'\}}\chi^2\Big(\frac{\log x}{\log N^{\gamma}}\Big)\Big)^2$$
$$\ll 2^{2t(\log\log N)^3}\prod_{i\in[t]}\Big(\mathbb{E}_{n\in\mathbb{Z}^d\cap K}\Big(\sum_{\mathbf{d},\mathbf{m},\mathbf{u},\mathbf{e},\mathbf{e}'\in[N^{\gamma}]^t}1_{u_id_im_i^2\varepsilon_i\mid\psi_i(n)}\tau(u_i)\Big)^{2t}\Big)^{1/t}$$
$$\ll(\log N)^{O(t)}2^{2t(\log\log N)^3}.$$

The combination of these two bounds proves the claim. ■

Note that the same argument furthermore shows that the main term from Claim 2 equals

(9.4)
$$\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \alpha_{\Phi}((d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} \sum_{u_j} \frac{2^{s_j}\tau(u_j)}{u_j} \mu(e_j)\mu(e_j') \prod_{\substack{x\in\\ \{d_j,m_j,e_j,e_j'\}}} \chi\Big(\frac{\log x}{\log N^{\gamma}}\Big) + O_D(N^{-(\log\log N)^{-4}}).$$

Thus, we are left with the main term in (9.4). We proceed by inserting the integral representation (9.3) of each of the $4t$ factors involving χ. Multiplying out this product we obtain a main term and a number of error terms. Since $\chi(\log m/\log N^{\gamma}) \ll m^{-1/\log N^{\gamma}}$, all these error terms may be seen to be of the same form, which allows us to combine them into one error term. Writing $z_{j,k} = (1+i\xi_{j,k})/\log N^{\gamma}$ for $j \in [t]$, $k \in [4]$ and noting that $|z_{j,k}| \ll (\log N^{\gamma})^{-1/2}$, we see that the main term from (9.4) is equal to

$$(9.5)\quad \sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \Big(\prod_{i\in[t]} \sum_{u_i} \frac{2^{s_i}\tau(u_i)}{u_i}\Big) \alpha_{\Phi}(d_1 m_1^2 \varepsilon_1, \ldots, d_t m_t^2 \varepsilon_t) \times \Big\{ \int_I \cdots \int_I \prod_{j\in[t]} \mu(e_j)\mu(e_j') e_j^{-z_{j,1}} e_j'^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}} \prod_{k\in[4]} \vartheta(\xi_{j,k})\, d\xi_{j,k} + O_A\Big(\log^{-A} N^{\gamma} \prod_{j\in[t]} (e_j e_j' d_j m_j)^{-1/\log N^{\gamma}}\Big)\Big\}.$$

The error term here indeed has small contribution: On the one hand, we have
$$\sum_{s_1,\ldots,s_t} \sum_{i_1,\ldots,i_t} \prod_{j\in[t]} \sum_{u_j\in U(i_j,s_j)} \frac{2^{s_j}\tau(u_j)}{u_j} = O(1).$$

See the proof of [18, Proposition 4.2] for details. On the other hand, the divisor sum is bounded:

$$\begin{aligned} &\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \alpha_{\Phi}(d_1 m_1^2 \varepsilon_1, \ldots, d_t m_t^2 \varepsilon_t) \prod_{j\in[t]} (e_j e_j' d_j m_j)^{-1/\log N^{\gamma}} \\ &\quad = \sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \prod_{\substack{p>w(N)\\ p^{a_i}\| d_i m_i^2 \varepsilon_i}} \alpha_{\Phi}(p^{a_1}, \ldots, p^{a_t}) \prod_{\substack{j\in[t]\\ p^{a_j'}\| e_j e_j' d_j m_j}} (p^{a_j + a_j'})^{-1/\log N^{\gamma}} \\ &\quad \ll \prod_{p>w(N)} (1 + p^{-(1+1/\log N^{\gamma})})^{-O(t)} \ll (\log N)^{O(t)}. \end{aligned}$$

Here, we crudely bounded the number of occurring t-tuples $(a_1, \ldots, a_t)$ that satisfy $\max_i a_i = k$ by $k^{O(t)}$ and apply to each of these tuples the bound $\alpha_{\Phi}(p^{a_t}, \ldots, p^{a_t}) \ll p^{-k}$.

Thus, when we choose A in (9.5) sufficiently large, the error term above makes a total contribution of $\ll_A \log^{-A/2} N^{\gamma}$.

It remains to estimate the main term from above. Changing the order of summation and integration leads to an absolutely convergent sum in the integrand. Since the range of integration is compact, this change is permitted, and hence the main term is equal to

$$\tag{9.6} \int_I \cdots \int_I \Big(\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \Big(\prod_{i\in[t]} \sum_{u_i} \frac{2^{s_i}\tau(u_i)}{u_i} \Big) \alpha_\Phi((d_k m_k^2 \varepsilon_k)_{k\in[t]}) \\ \times \prod_{j\in[t]} \mu(e_j)\mu(e_j') e_j^{-z_{j,1}} e_j'^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}} \Big) \prod_{k\in[4]} \vartheta(\xi_{j,k})\, d\xi_{j,k}.$$

Our next aim is to show that all relevant terms in the integrand are in fact the independent terms, that is, they are those terms for which the t products $u_i d_i m_i^2 \varepsilon_i$, $i \in [t]$, are pairwise coprime. This will eventually allow us to swap the sums with the product while only introducing a small error. For the u_i we have just done this.

Since each entry of $\mathbf{d}$, $\mathbf{m}$, $\mathbf{e}$, and $\mathbf{e}'$ is completely composed of primes greater than $w(N)$, the following claim holds.

Claim 3. *We have*

$$\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'} \alpha_\Phi((d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} \mu(e_j)\mu(e_j') e_j^{-z_{j,1}} e_j'^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}} \\ = (1 + O_D(w(N)^{-1})) \\ \times {\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}}' \alpha_\Phi((d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} \mu(e_j)\mu(e_j') e_j^{-z_{j,1}} e_j'^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}},$$

where $\sum'$ indicates that the summation is extended only over choices of t-tuples that satisfy the coprimality condition $(d_i m_i \varepsilon_i, d_{i'} m_{i'} \varepsilon_{i'}) = 1$ for any $i \neq i'$.

Proof. Note that the summand is multiplicative and may be written as a product over primes $p > w(N)$. Any summand

$$\alpha_\Phi((d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} \mu(e_j)\mu(e_j') e_j^{-z_{j,1}} e_j'^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}}$$

with entries failing coprimality may be factorised into a product of one factor of the same form that satisfies coprimality and one factor for which every prime p that appears as a divisor of some $d_i m_i \varepsilon_i$ divides at least another $d_{i'} m_{i'} \varepsilon_{i'}$, $i' \neq i$. For a fixed tuple $(k_1, \ldots, k_t)$ of the latter type (that is, $p \mid k_i$ implies $p \mid \prod_{i'\neq i} k_{i'}$), the contribution may be bounded as follows employing the triangle inequality:

$$\begin{aligned}
&\alpha(k_1,\dots,k_t)\\
&\quad\times\Bigg|\sum_{\substack{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'\\(d_im_i\varepsilon_i,\ k_1\dots k_t)=1}}{}' \alpha_{\Phi}((d_im_i^2\varepsilon_i)_{i\in[t]})\prod_{j\in[t]}\mu(e_j)\mu(e_j')e_j^{-z_{j,1}}e_j'^{-z_{j,2}}d_j^{-z_{j,3}}m_j^{-z_{j,4}}\Bigg|\\
&=\alpha(k_1,\dots,k_t)\\
&\quad\times\Bigg|\prod_{p\mid k_1\dots k_t}(1+O(p^{-1}))\\
&\qquad\times\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}{}' \alpha_{\Phi}((d_im_i^2\varepsilon_i)_{i\in[t]})\prod_{j\in[t]}\mu(e_j)\mu(e_j')e_j^{-z_{j,1}}e_j'^{-z_{j,2}}d_j^{-z_{j,3}}m_j^{-z_{j,4}}\Bigg|\\
&\le\alpha(k_1,\dots,k_t)\prod_{p\mid k_1\dots k_t}(1+O(p^{-1}))\\
&\quad\times\Bigg|\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}{}' \alpha_{\Phi}((d_im_i^2\varepsilon_i)_{i\in[t]})\prod_{j\in[t]}\mu(e_j)\mu(e_j')e_j^{-z_{j,1}}e_j'^{-z_{j,2}}d_j^{-z_{j,3}}m_j^{-z_{j,4}}\Bigg|.
\end{aligned}$$

Next, we bound the sum over all terms $\alpha(k_1,\dots,k_t)\prod_{p\mid k_1\dots k_t}(1+O(p^{-1}))$ that occur. Written as a product over primes, a crude bound for this quantity is given by

$$\prod_{p>w(N)}\Big\{1+\sum_{\substack{a_1,\dots,a_t\\ \text{at least two}\\ a_i>0}}O(a_1^4+\dots+a_t^4)\alpha_{\Phi}(p^{a_1},\dots,p^{a_t})\big(1+O(p^{-1})\big)\Big\}-1,$$

where we used the very crude bound $\tau_5(p^{a_i})\ll a_i^4$ on the generalised divisor function τ_5. The five factors correspond to d_i, m_i^2, ε_i/e_i, ε_i/e_i' and e_ie_i'/ε_i. To further bound the above expression, we observe that the number of tuples $(a_1,\dots,a_t)$ with $\max_i a_i=k$ is at most tk^{t-1}. For such choices of $(a_1,\dots,a_t)$, we have $\sum_i a_i^4\le tk^4$ and $\alpha_{\Phi}(p^{a_1},\dots,p^{a_t})\le p^{-k-1}$, since Φ has finite complexity and at least two of the a_i are non-zero. Further, for large enough p, we have $p^{-k}t^2k^{t-3}(1+O(p^{-1}))<p^{-3k/4}$ for all $k\ge1$. We certainly may assume that N is large enough for $p>w(N)$ to satisfy this condition. Thus

$$\sum_{\substack{a_1,\dots,a_t\\ \text{at least two}\\ a_i>0}}O(a_1^4+\dots+a_t^4)\alpha_{\Phi}(p^{a_1},\dots,p^{a_t})(1+O(p^{-1}))\le\sum_{k\ge1}p^{-3k/4-1}\le p^{-3/2}.$$

Since

$$\prod_{p>w(N)}(1+p^{-3/2})-1\le\sum_{n>w(N)}n^{-3/2}\ll w(N)^{-1/2},$$

the result follows. ∎

Note that in the above claim

$$(9.7)\qquad \sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}{}' \alpha_\Phi((d_i m_i^2 \varepsilon_i)_{i\in[t]}) \prod_{j\in[t]} \mu(e_j)\mu(e'_j) e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}}$$
$$= \sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}{}' \prod_{j\in[t]} \frac{\mu(e_j)\mu(e'_j)}{d_j m_j^2 \varepsilon_j} e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}}.$$

The last step of the rearrangement is to show that we may swap the inner product and sum in the integrand.

Claim 4. *The sum and product in* (9.7) *may be interchanged:*

$$\sum_{\mathbf{d},\mathbf{m},\mathbf{e},\mathbf{e}'}{}' \prod_{j\in[t]} \frac{\mu(e_j)\mu(e'_j)}{d_j m_j^2 \varepsilon_j} e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}}$$
$$= (1 + O(w(N)^{-1/2})) \prod_{j\in[t]} \sum_{d_j,m_j,e_j,e'_j} \frac{\mu(e_j)\mu(e'_j)}{d_j m_j^2 \varepsilon_j} e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}}.$$

Proof. The proof is essentially the same as the one of the previous claim. ■

The next claim will imply that the integral (9.6) equals, up to a small error, the integral of the main term from Claim 4.

Claim 5.

$$\int_I \cdots \int_I \Bigg| \prod_{j\in[t]} \sum_{d_j,m_j,e_j,e'_j} \frac{\mu(e_j)\mu(e'_j)}{d_j m_j^2 \varepsilon_j} e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}} \prod_{k\in[4]} \vartheta(\xi_{j,k}) \Bigg|$$
$$\times \prod_{(j',k')\in[t]\times[4]} d\xi_{j',k'} = O(1).$$

Proof. (Cf. [8, equation (D.23) and the proof thereof].) We begin by writing the integrand as a product over primes

$$\Bigg| \prod_{j\in[t]} \sum_{d_j,m_j,e_j,e'_j} \frac{\mu(e_j)\mu(e'_j)}{d_j m_j^2 \varepsilon_j} e_j^{-z_{j,1}} {e'_j}^{-z_{j,2}} d_j^{-z_{j,3}} m_j^{-z_{j,4}} \prod_{k\in[4]} \vartheta(\xi_{j,k}) \Bigg|$$
$$\ll_A \prod_{j\in[t]} \prod_{k\in[4]} (1 + |\xi_{j,k}|)^{-A}$$
$$\times \prod_{q\in\mathcal{Q}_j} (1 - q^{-1-z_{j,1}} - q^{-1-z_{j,2}} + q^{-1-z_{j,1}-z_{j,2}}) \prod_{p\in\mathcal{P}_j} (1 - p^{-1-z_{j,3}})^{-1}.$$

For $\Re s > 0$, the prime number theorem in arithmetic progressions yields

$$\sum_{p\in\mathcal{Q}_i} p^{-1-s} = \frac{1}{2}\log\frac{1}{s} + O_{D_i}(1).$$

This also holds for $\mathcal{P}_i$ in place of $\mathcal{Q}_i$. Thus, if we choose A sufficiently large, the above is seen to be bounded by

$$\begin{aligned}&\prod_{j\in[t]}\prod_{k\in[4]}(1+|\xi_{j,k}|)^{-A}\\ &\qquad\times\prod_{q\in\mathcal{Q}_j}(1-q^{-1-z_{j,1}}-q^{-1-z_{j,2}}+q^{-1-z_{j,1}-z_{j,2}})\prod_{p\in\mathcal{P}_j}(1-p^{-1-z_{j,3}})^{-1}\\ &\qquad\ll\prod_{j\in[t]}\prod_{k\in[4]}(1+|\xi_{j,k}|)^{-A}|z_{j,1}|^{1/2}|z'_{j,2}|^{1/2}|z_{j,1}+z'_{j,2}|^{-1/2}|z_{j,3}|^{-1/2}\\ &\qquad\ll\log^t N^\gamma\log^{-t}N^\gamma\prod_{j\in[t]}(1+|\xi_{j,1}|)^{1/2}(1+|\xi_{j,2}|)^{1/2}\prod_{k\in[4]}(1+|\xi_{j,k}|)^{-A}\\ &\qquad\ll\prod_{j\in[t]}\prod_{k\in[4]}(1+|\xi_{j,k}|)^{-A/2}.\end{aligned}$$

For any $A>2$ the integral of the final expression is $O(1)$. ■

Together with Claim 3, equation (9.7) and Claim 4, the above claim implies that the integral (9.6) is given by

$$\begin{aligned}&\Big(\prod_{i\in[t]}\sum_{u_i}\frac{2^{s_i}\tau(u_i)}{u_i}\Big)\int_I\cdots\int_I\prod_{j\in[t]}\sum_{d_j,m_j,e_j,e'_j}\frac{\mu(e_j)\mu(e'_j)}{d_jm_j^2\varepsilon_j}e_j^{-z_{j,1}}{e'_j}^{-z_{j,2}}d_j^{-z_{j,3}}m_j^{-z_{j,4}}\\ &\qquad\qquad\times\prod_{k\in[4]}\vartheta(\xi_{j,k})\prod_{(j',k')\in[t]\times[4]}d\xi_{j',k'}+o(1).\end{aligned}$$

After removing the truncation of the integral again, the latter expression is seen to equal

$$\Big(\prod_{i\in[t]}\sum_{u_i}\frac{2^{s_i}\tau(u_i)}{u_i}\Big)\prod_{j\in[t]}\sum_{d_j,m_j,e_j,e'_j}\frac{\mu(e_j)\mu(e'_j)}{d_jm_j^2\varepsilon_j}\prod_{x\in\{e_j,e'_j,m_j,d_j\}}\chi\Big(\frac{\log x}{\log N^\gamma}\Big)+o(1).$$

Putting everything together, we have shown that

$$\begin{aligned}&\mathbb{E}_{n\in\mathbb{Z}^d\cap K}\prod_{j\in[t]}\nu'_{D_{i_j},\gamma}(\varphi_j(n))\beta'_{D_{i_j},\gamma}(\varphi_j(n))\\ &\qquad=(1+O_d(w(N)^{-1/2}))\\ &\qquad\quad\times\prod_{j\in[t]}\Big(\sum_{s_j,i_j,u_j}\sum_{d_j}\sum_{m_j,e_j,e'_j}\frac{2^{s_j}\tau(u_i)}{u_j}\frac{\mu(e_j)\mu(e'_j)}{d_jm_j^2\varepsilon_j}\\ &\qquad\qquad\qquad\times\prod_{x\in\{e_j,e'_j,m_j,d_j\}}\chi\Big(\frac{\log x}{\log N^\gamma}\Big)+o(1)\Big).\end{aligned}$$

The last expression now is independent of Φ. Applying the asymptotic in each of the known one-dimensional cases

$$\mathbb{E}_{n\leq N}\nu'_{D_{i_j},\gamma}(n)\beta'_{D_{i_j},\gamma}(n)=C_{D_{i_j},\gamma}+o(1),$$

where $\Phi:\mathbb{Z}\to\mathbb{Z}$ is given by the identity, implies that each of the factors above is of the correct form. This completes the proof of the proposition.

Proof of Proposition 9.2. The proof of the correlation estimate follows in a very similar manner to those of the corresponding estimates for the divisor function majorant in [18, §7] and the von Mangoldt function majorant from [8, App. D]. We restrict attention to the case of pairwise distinct h_i; the remaining case follows, as before, by choosing $\sigma_{m_0}(0)$ sufficiently large. Employing the volume packing lemma, we may show as in [18, §7] that

$$\mathbb{E}_{n\in I}\prod_{j\in[m]}\nu'_{D_{i_j},\gamma}(\overline{W}(n+h_j)+b_{i_j})\beta'_{D_{i_j},\gamma}(\overline{W}(n+h_j)+b_{i_j})$$
$$\ll\prod_{\substack{p\mid\Delta\\ p>w(N)}}\sum_{a_1,\dots,a_m}\alpha(p^{a_1},\dots,p^{a_m}),$$

where $\Delta:=\prod_{j\neq j'}(\overline{W}(h_j-h_{j'})+b_{i_j}-b_{i_{j'}})$. This estimate allows us to proceed as in [18, §7].

10. Application of the transference principle. This section provides a quick overview of the results around the von Neumann theorem and the inverse theorem for the Gowers norms. We apply these results at the end of the section to reduce Proposition 8.1 to a non-correlation estimate.

In the dense setting, that is, if $g:\mathbb{Z}\to\mathbb{R}$ is a bounded function with asymptotic density, the *Gowers uniformity norms*, defined as

$$\|g\|_{U^s[N]}:=\Big(\mathbb{E}_{x\in[N]}\mathbb{E}_{h\in[N]^s}\prod_{\omega\in\{0,1\}^s}g(x+\omega\cdot h)\Big)^{1/2^s},$$

capture all information on the correlations of g with respect to finite complexity systems. This generalises as follows.

Proposition 10.1 (Green–Tao [8], generalised von Neumann theorem). *Let t,d,L be positive integer parameters. Then there are constants C_1 and D, depending on t,d and L, such that the following is true. Let C with $C_1\leq C\leq O_{t,d,L}(1)$ be arbitrary and suppose that $N'\in[CN,2CN]$ is a prime. Let $\nu:\mathbb{Z}_{N'}\to\mathbb{R}^+$ be a D-pseudorandom measure, and suppose that $f_1,\dots,f_t:[N]\to\mathbb{R}$ are functions with $|f_i(x)|\leq\nu(x)$ for all $i\in[t]$ and $x\in[N]$. Suppose that $\Psi=(\psi_1,\dots,\psi_t)$ is a finite complexity system of affine-linear forms whose linear coefficients are bounded by L. Let $K\subset[-N,N]^d$ be a* *convex body such that $\Psi(K) \subset [1,N]^t$. Suppose also that*

$$\min_{1\le j\le t} \|f_j\|_{U^{t-1}[N]} = o(1). \tag{10.1}$$

Then

$$\sum_{n\in K} \prod_{i\in[t]} f_i(\psi_i(n)) = o(N^d).$$

Establishing the Gowers uniformity condition (10.1) itself is a task that is conceptually equivalent to that of finding an asymptotic for the expression $\sum_{n\in K}\prod_{i\in[t]} f(\psi_i(n))$ directly, and should therefore not be any easier. The specific system of affine-linear forms that appears in the definition of the uniformity norms, however, allows an alternative characterisation of Gowers uniform functions.

A characterisation of Gowers uniform functions. Whether or not a function f is Gowers uniform, is characterised by the non-existence or existence of a polynomial nilsequence ([2]) that correlates with f. On the one hand, correlation with a nilsequence obstructs uniformity:

Proposition 10.2 (Green–Tao [8, Cor. 11.6]). *Let $s \ge 1$ be an integer and let $\delta \in (0,1)$ be real. Let $G/\Gamma = (G/\Gamma, d_{G/\Gamma})$ be an s-step nilmanifold with some fixed smooth metric $d_{G/\Gamma}$, and let $(F(g(n)\Gamma))_{n\in\mathbb{N}}$ be a bounded s-step nilsequence with Lipschitz constant at most L. Let $f : [N] \to \mathbb{R}$ be a function that is bounded in the L_1-norm, that is, assume $\|f\|_{L_1} = \mathbb{E}_{n\in[N]}|f(n)| \le 1$. If furthermore*

$$\mathbb{E}_{n\in[N]} f(n)F(g(n)\Gamma) \ge \delta$$

then

$$\|f\|_{U^{s+1}[N]} \gg_{s,\delta,L,G/\Gamma} 1.$$

An inverse result to this statement has been known as the Inverse Conjecture for the Gowers norms for some time and has recently been resolved (see [11]). The inverse conjectures are stated for bounded functions. With our application to the normalised divisor function in mind, we only recall the transferred statement (cf. [8, Prop. 10.1]) here.

Proposition 10.3 (Green–Tao–Ziegler, relative inverse theorem for the Gowers norms). *For any $0 < \delta \le 1$ and any $C \ge 20$, there exists a finite collection $\mathcal{M}_{s,\delta,C}$ of s-step nilmanifolds G/Γ, each equipped with a metric $d_{G/\Gamma}$, such that the following holds. Given any $N \ge 1$, suppose that $N' \in [CN, 2CN]$ is prime, that $\nu : [N'] \to \mathbb{R}^+$ is an $(s+2)2^{s+1}$-pseudorandom measure, and that $f : [N] \to \mathbb{R}$ is any arithmetic function with $|f(n)| \le \nu(n)$*

[2] For definitions of nilmanifolds and nilsequences, see, for instance, [10].

for all $n \in [N]$ and such that

$$\|f\|_{U^{s+1}[N]} \geq \delta.$$

Then there is a nilmanifold $G/\Gamma \in \mathcal{M}_{s,\delta,C}$ in the collection and a 1-bounded s-step nilsequence $(F(g(n)\Gamma))_{n\in\mathbb{N}}$ on it that has Lipschitz constant $O_{s,\delta,C}(1)$, such that we have the correlation estimate

$$|\mathbb{E}_{n\in[N]} f(n)F(g(n)\Gamma)| \gg_{s,\delta,C} 1.$$

This inverse theorem now reduces the required uniformity-norm estimate (10.1) to the potentially easier task of proving that the centralised version of f does not correlate with polynomial nilsequences.

10.1. Reduction of the main theorem to a non-correlation estimate. We already reduced the main theorem to the W-tricked version given in Proposition 8.1, which we now restate:

Proposition 8.1. *Let $\Psi : \mathbb{Z}^d \to \mathbb{Z}^t$ be a finite complexity system of forms, let $a \in \mathcal{A}_\Psi$, and let $\tilde{\Psi} : \mathbb{Z}^d \to \mathbb{Z}^t$ be the translate of Ψ defined as in Section 8. Then*

$$\mathbb{E}_{m\in\mathbb{Z}^d\cap K'} \prod_{i=1}^{t} r'_{f_i,c_i(a)}(\tilde{\psi}(m)) = 1 + o_{t,d,L}(1),$$

where $K' \subseteq [-N/\overline{W}, N/\overline{W}]^d$ is a convex body such that $\overline{W}\tilde{\Psi}(K') + c(a) \subseteq [1,N]^t$.

Writing

$$\mathbb{E}_{m\in\mathbb{Z}^d\cap K'} \prod_{i=1}^{t} r'_{f_i,c_i(a)}(\tilde{\psi}(m)) = \mathbb{E}_{m\in\mathbb{Z}^d\cap K'} \prod_{i=1}^{t} \big(\big(r'_{f_i,c_i(a)}(\tilde{\psi}(m)) - 1\big) + 1\big)$$

and multiplying out, we obtain a constant term 1 and all other terms are of a form the generalised von Neumann theorem applies to, provided we can show that

$$\|r'_{f_i,c_i(a)} - 1\|_{U^{t-1}} = o(1)$$

for all $i \in [t]$. By the inverse theorem, it suffices to show that

$$|\mathbb{E}_{n\in[N/\overline{W}]}(r'_{f_i,c_i(a)}(n) - 1)F(g(n)\Gamma)| = o_{G/\Gamma,t}(1)$$

for all $(t-2)$-step nilsequences $(g(n)\Gamma)_{n\leq N/\overline{W}}$ and 1-bounded Lipschitz functions F. This task will be carried out in Sections 14–18.

11. Non-correlation with nilsequences. The so far standard line of attack to obtain a result of the form ‘the function h does not correlate with k-step nilsequences’ is to employ the Green–Tao factorisation theorem [10, 1.19], which allows us to reduce this task to the case where the nilsequence is close to being equidistributed. A separate estimate which shows that h does not correlate with periodic (nil)sequences allows us to further assume that the Lipschitz function involved has zero mean, that is, $\int_{G/\Gamma} F = 0$. Periodic sequences are regarded as major arcs. We have already deduced a major arc estimate in Section 7.1. The remaining case with the strong assumption that the nilsequence behaves in a very equidistributed way corresponds to the minor arc analysis of the classical Hardy–Littlewood method (cf. the discussion in [9, §4]). The procedure of passing to the equidistributed (minor arc) case is fairly independent of the individual problem and is completely described in §2 of [9]. Thus, we restrict our attention here to providing the necessary major and minor arc estimates specific to our problem and only summarise the procedures from [9] we employ.

Our approach to the minor arc estimate is modelled on a strategy one might choose in the classical setting: If θ is a rational that belongs to a suitably chosen notion of 'minor arc', then one obtains an upper bound for the expression

$$\mathbb{E}_{n\le N} r_f(n)e(\theta n) = \frac{1}{N}\sum_{\substack{x,y\\ f(x,y)\le N}} e(\theta f(x,y)) = \frac{1}{N}\sum_{\substack{x,y\\ f(x,y)\le N}} e(\theta(ax^2+bxy+cy^2))$$

by splitting into suitable summation ranges, fixing either x or y, and applying Weyl's inequality ([3]). Thus, in our case, we aim to employ the quadratic structure of the form f by means of Weyl's inequality in order to deduce the estimate

$$\mathbb{E}_{n\le N} r_f(n)F(g(n)\Gamma) = o(1)$$

for sufficiently equidistributed sequences $(g(n)\Gamma)_{n\le N}$. When working with a sequence $(F(g(n)\Gamma))_{n\in[N]}$ directly, Weyl's differencing trick may only be employed locally on so called generalised Bohr neighbourhoods, where one can make the locally polynomial structure of a nilsequence explicit (cf. the approach in [7]).

The crucial fact that makes Weyl's differencing trick work for exponential sums is that the exponential function is a group homomorphism. Since F is a Lipschitz function, one expects it to have a good, i.e. short, Fourier approximation. In general, elements of a Fourier basis in the non-abelian case arise from characters, i.e. homomorphisms. Thus there is a good chance that it is possible to employ Weyl's inequality globally for elements of the Fourier basis and hence for a short Fourier approximation of a Lipschitz function.

In our case, the situation is considerably simplified by the availability of a complete quantitative equidistribution theory for polynomial orbits on nilmanifolds, which has been worked out by Green and Tao in [10]. In partic-

[3] See the next section for more details.

ular, their generalisation of Leon Green's theorem ('Quantitative Leibman theorem' [10, Thm. 1.16]) asserts that any polynomial sequences on a nilmanifold G/Γ is δ-equidistributed [4] *if and only if* its projection on the horizontal torus is δ'-equidistributed, where the dependence is polynomial. The horizontal torus bears the advantage of being isomorphic to an ordinary torus $\mathbb{R}^{d_{\mathrm{ab}}}/\mathbb{Z}^{d_{\mathrm{ab}}}$. Consequently, we need not consider the representation theory on nilpotent Lie groups and their homogeneous spaces; analysing the projected sequence on the horizontal torus by standard Fourier analysis, or even the quantitative version of Weyl's equidistribution theory, is sufficient. (The latter theory will actually reduce matters to looking at sequences $\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ arising from horizontal characters.)

Our strategy, after reducing to the equidistributed case, is the following: Let P denote a polynomial of degree d. Then equidistribution of $(g(n)\Gamma)_{n\leq N}$ on G/Γ implies that $(\pi \circ g(n))_{n\leq N}$ is equidistributed on the horizontal torus, which implies, as a consequence of Weyl's equidistribution theory, that $(\pi \circ g(P(n)))_{n\leq N^{1/d}}$ is equidistributed on the horizontal torus, which implies that $(g(P(n))\Gamma)_{n\leq N^{1/d}}$ is equidistributed on G/Γ. The distribution of polynomial subsequences was not considered in [10], but will follow from results of that paper. These results will be proved in Sections 14 and 15.

For the above strategy to work, a strong major arc analysis is required, because the W-trick introduces very large coefficients into the quadratic forms under consideration. For the major arc analysis, we rely on the observation that all of these large coefficients turn out to be entirely composed of small prime factors. We briefly describe in the next section how this information is used to choose major and minor arcs in the classical setting. The general case will be carried out in Section 15 (especially Corollary 15.2 and Proposition 15.4 which deal with polynomial subsequences that have large but smooth coefficients) and Section 16, which provides a factorisation of polynomial sequences into major and minor arcs.

12. A special choice of major and minor arcs is necessary.

In this section we describe briefly and solely for motivational purposes how the major and minor arcs are chosen in the model case of correlation with linear phase functions $e(\theta n)$ instead of general nilsequences. Here the task is to show that

$$\mathbb{E}_{n\leq N}(r'_{f,\beta}(n) - 1)e(\theta n) = o(1).$$

In Section 7.1, we saw that $r'_{f,\beta} - 1$ does not correlate with any q-periodic function of $w(N)$-smooth period q, provided N/q is still quite large. It is therefore possible to choose the major arcs to consist of all rationals $\theta \in [0, 1)$ that are close to a rational with $w(N)$-smooth denominator: in that case

[4] The quantitative notion of equidistribution is recalled in Section 14.

$e(n\theta)$ is close to a periodic function with $w(N)$-smooth period. The minor arcs then comprise all θ that are not close to rationals with $w(N)$-smooth denominators. For such a 'minor arc' θ, we automatically have $\mathbb{E}_{n\le N}e(\theta n) = o(1)$.

Thus, we define the major arcs to be

$$\mathfrak{M} := \bigcup_{q\in\mathfrak{Q}} \mathfrak{M}_q,$$

where $\mathfrak{Q}$ is the following set of all not too large $w(N)$-smooth denominators:

$$\mathfrak{Q} := \{1 \le q \le N^{\varepsilon} : p \mid q \Rightarrow p \le w(N)\}$$

and where $\mathfrak{M}_q$ is the set of real numbers that are well approximated by some rational with $w(N)$-smooth denominator:

$$\mathfrak{M}_q := \left\{\theta : \left|\theta - \frac{\alpha}{q}\right| \le \frac{1}{qN^{1-\varepsilon}} \text{ for some } (\alpha, q) = 1\right\}.$$

The reason behind this choice of major arc is the following. When we pass to W-tricked versions of the representation function, which are up to normalisation of the form $n \mapsto r_f(\overline{W}n + \beta)$, then this restriction to a *linear* substructure cannot directly be expressed by the quadratic form f. For the minor arcs treatment, we, however, hope to work with the quadratic form directly. We will therefore consider all choices $(x', y') \in [\overline{W}]^2$ such that $f(x', y') \equiv \beta \pmod{\overline{W}}$ and consider for each choice the quadratic form $f(\overline{W}x + x', \overline{W}y + y')$ in x, y. Fixing either x or y, we hope to apply Weyl's inequality when $\theta \notin \mathfrak{M}$ to estimate

$$\sum_{n\le(N-\beta)/\overline{W}} r(\overline{W}n + \beta)e(\theta n)$$

$$= \sum_{\substack{x',y'\in[\overline{W}] \\ f(x',y')\equiv\beta \,(\mathrm{mod}\, \overline{W})}} \sum_{\substack{x,y \\ f(\overline{W}x+x',\overline{W}y+y')\le N}} e\left(\frac{\theta(f(\overline{W}x + x', \overline{W}y + y') - \beta)}{\overline{W}}\right).$$

Here we obtain for fixed x', y' and either fixed x or fixed y a quadratic inside the exponential with leading coefficient $\theta\overline{W}a$ or $\theta\overline{W}c$ where a and c are coefficients of f. For the application of Weyl's inequality, we require that this leading coefficient is close to a rational with large denominator.

Since $ac\overline{W} \ll N^{o(1)}$, the choice of major and minor arcs guarantees that, when $\theta \notin \mathfrak{M}$, i.e.

$$\left|\theta - \frac{\alpha}{q}\right| \le \frac{1}{qN^{1-\varepsilon}}$$

for some q that has a prime factor $> w(N)$, or satisfies $q > N^{\varepsilon}$, then

$$\left|a\overline{W}\theta - \frac{\alpha'}{q'}\right| \le \frac{1}{qN^{1-\varepsilon-o(1)}},$$

where q' has a prime factor $> w(N)$, or satisfies $q' > N^{\varepsilon - o(1)}$. Thus, $a\overline{W}\theta$ can still be thought of as minor arc, when replacing N by $N^{1-o(1)}$.

13. A brief overview of the concepts around nilsequences. Let G be a connected, simply connected, k-step nilpotent Lie group, and let Γ be a discrete co-compact subgroup. Then G/Γ is called a *k-step nilmanifold.* A *filtration* $G_\bullet$ of G is a sequence of subgroups

$$G = G_0 = G_1 \geq G_2 \geq \cdots \geq G_d \geq G_{d+1} = \{\mathrm{id}_G\}$$

such that for any $d \geq i, j \geq 0$ the commutator group $[G_i, G_j]$ is a subgroup of G_{i+j}. The filtration is said to have degree d if G_{d+1} is the first element in the sequence that is trivial. By definition, a nilpotent group always has a filtration.

The quantitative analysis carried out in [10] relies on the existence of a certain type of basis, a Mal'cev basis, for the Lie algebra $\mathfrak{g}$ of G. Adapted to any filtration, there exists a Mal'cev basis for $\mathfrak{g}$ that parametrises via the exponential map both the groups in the filtration and the uniform subgroup Γ in a very natural way. For each such basis $\mathcal{X}$, Green and Tao introduce a metric $d_{\mathcal{X}}$ for G and its quotient G/Γ in [10, Def. 2.2], which then allows them to define Lipschitz functions on G/Γ, and also to introduce a notion of slowly varying (or smooth) sequences $(\varepsilon(n))_{n\in\mathbb{Z}}$ that take values in G. Despite the fact that any of the statements on nilsequences require a fixed choice of Mal'cev basis $\mathcal{X}$ and corresponding metric $d_{\mathcal{X}}$, we will not need to directly work with any of the specific properties of either of these objects: they will only implicitly be present through the results from [10] we build on. For this reason, we content ourselves with referring to [10, §2 and App. A] for background and exact definitions.

Definition 13.1 (Polynomial sequence; [10, Def. 1.8]). Let $g : \mathbb{Z} \to G$ be a G-valued sequence, and define the discrete derivative

$$\partial_h g(n) := g(n+h)g(n)^{-1} \quad \text{for each } h \in \mathbb{Z}.$$

Then g is a *polynomial sequence* with coefficients in $G_\bullet$ when for every $i \in \{0, \ldots, d+1\}$, and every choice of $h_1, \ldots, h_i \in \mathbb{Z}$ all ith derivatives satisfy $\partial_{h_i} \ldots \partial_{h_1} g(n) \in G_i$. We write $\mathrm{poly}(\mathbb{Z}, G_\bullet)$ for all polynomial sequences adapted to $G_\bullet$ and say they are of *degree d*, where d is the degree of the filtration.

Two facts about polynomial sequences are of particular importance. The first is a theorem of Lazard: $\mathrm{poly}(\mathbb{Z}, G_\bullet)$ *forms a group*; see [10, §6] for a proof and the reference to the original work. The second important property is a more explicit description of polynomial sequences. It is shown in [10, §6 and the remarks following Def. 1.8] that every polynomial sequence can be written in the form $g(n) = a_1^{p_1(n)} \ldots a_k^{p_k(n)}$, where k is some integer,

$a_1, \dots, a_k \in G$, and $p_1, \dots, p_k : \mathbb{Z} \to \mathbb{Z}$ are polynomials. Observe that, if the sequence g_i defined by $g_i(n) = a_i^{p_i(n)}$ belongs to $\mathrm{poly}(\mathbb{Z}, G_\bullet)$, then the assertion that the discrete derivatives of order $d+1$ all equal id_G directly translates to $\deg(p_i) \leq d$. In general the degree of the polynomial sequence g is much larger than the degrees of the polynomial exponents $p_1, \dots, p_k$ that appear in the above mentioned representation.

Definition 13.2 (Horizontal torus). Write $\pi : G \to (G/\Gamma)_{\mathrm{ab}} := G/([G,G]\Gamma)$ for the canonical projection of G on the abelianisation of G/Γ. $(G/\Gamma)_{\mathrm{ab}}$ is called the *horizontal torus* of G.

We will extensively work with horizontal characters $\eta : G \to \mathbb{R}/\mathbb{Z}$. These are additive homomorphisms that annihilate Γ. Note that when g has degree d, that is, when g has coefficients in a filtration of degree d, then the projection $\eta \circ g$ can be written as an ordinary polynomial of degree at most d taking values in $\mathbb{R}/\mathbb{Z}$.

[10, Def. 2.6] defines the notion of the modulus $|\eta|$ of a horizontal character. All that is important to us is that $\|\eta\|_{\mathrm{Lip}} \ll |\eta|$.

14. Reduction from nilmanifolds to the abelian setting. In this section we provide the tool for passing from a general nilmanifold to the abelian setting of the horizontal torus. We caution, however, that by far the largest amount of the real work behind these results is hidden in the application of [10, Thm. 1.16], while the converse statements we prove are fairly straightforward.

Integral to all what follows are the two quantitative notions of equidistribution that were introduced in [10, Def. 1.2]:

Definition 14.1 (Quantitative equidistribution, [10]). Let G/Γ be a nilmanifold endowed with Haar measure and let $\delta_1, \delta_2 \in (0,1)$ be parameters. A finite sequence $(g(n)\Gamma)_{n \leq N}$ is said to be δ_1-*equidistributed* if

$$\Big|\mathbb{E}_{n \in [N]} F(g(n)\Gamma) - \int_{G/\Gamma} F\Big| \leq \delta_1 \|F\|_{\mathrm{Lip}}$$

for all Lipschitz functions $F : G/\Gamma \to \mathbb{C}$ with

$$\|F\|_{\mathrm{Lip}} := \|F\|_\infty + \sup_{x,y \in G/\Gamma,\, x \neq y} \frac{|F(x) - F(y)|}{d_{G/\Gamma}(x,y)}.$$

$(g(n)\Gamma)_{n \leq N}$ is said to be *totally δ_2-equidistributed* if

$$\Big|\mathbb{E}_{n \in P} F(g(n)\Gamma) - \int_{G/\Gamma} F\Big| \leq \delta_2 \|F\|_{\mathrm{Lip}}$$

for all Lipschitz functions F as above and all arithmetic progressions $P \subseteq [N]$ of length $|P| \geq \delta_2 N$.

For polynomial sequences these two notions of equidistribution are equivalent in the sense that every totally δ_2-equidistributed sequence is δ_2-equidistributed, and every δ_1-equidistributed sequence is totally $\delta_2(\delta_1)$-equidistributed, where $\delta_1^A \leq \delta_2(\delta_1) \leq \delta_1$ for some A only depending on the degree of the sequence, and the dimension and step of the nilmanifold. (As this observation will not be used later on, a proof is omitted.)

We set out by recalling the quantitative version of Weyl's inequality from [10], and the notion of smoothness norms in terms of which this inequality is phrased.

Any polynomial $g : \mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ of degree $\leq d$ has an expansion of the form

$$g(n) = \alpha_0 + \alpha_1 \binom{n}{1} + \cdots + \alpha_d \binom{n}{d}.$$

The *smoothness norm* of g is defined by

$$\|g\|_{C^\infty[N]} := \sup_{1\leq j\leq d} N^j \|\alpha_j\|_{\mathbb{R}/\mathbb{Z}}.$$

This norm was introduced in [10, Def. 2.7] as a measure of slow variation of polynomial sequences on tori. Indeed,

$$\|g(n) - g(n-1)\|_{\mathbb{R}/\mathbb{Z}} \ll_d \|g\|_{C^\infty[N]}/N. \tag{14.1}$$

For us it will be more convenient to work with the coefficients of the ordinary representation of g. When $g(n) = \beta_d n^d + \beta_{d-1}n^{d-1} + \cdots + \beta_0$, then (cf. [9, Lemma 3.2]) there is $q \geq 1$ with $q = O_d(1)$ such that

$$\|q\beta_j\|_{\mathbb{R}/\mathbb{Z}} \ll N^{-j}\|g\|_{C^\infty[N]} \tag{14.2}$$

for $j = 1, \ldots, d$. This follows by expressing each β_j as a linear combination of α_i. The coefficients appearing are bounded by $O_d(1)$.

In the other direction we can show

$$\|g\|_{C^\infty[N]} \ll \sup_{1\leq j\leq d} N^j \|j!\beta_j\|_{\mathbb{R}/\mathbb{Z}}. \tag{14.3}$$

Indeed, $j!\beta_j$ is a linear combination of α_i, $i \geq j$, where the coefficient of α_j is 1 and all other coefficients are $O_d(1)$. Let j_0 be the maximal index for which $\|g\|_{C^\infty[N]} = N^{j_0}\|\alpha_{j_0}\|$. Then $N^i\|\alpha_i\| < N^{j_0}\|\alpha_{j_0}\|$ for all $i > j_0$. Thus $\|\alpha_i\| < N^{j_0-i}\|\alpha_{j_0}\|$. Then $\|j_0!\beta_{j_0}\| = \|\alpha_{j_0}\|(1 + O_d(N^{-1}))$, which proves the result.

Part (a) of the following is Green and Tao's Proposition 4.3 from [10]. While the latter is quite a deep result, its converse, which we prove as part (b), is rather straightforward.

Proposition 14.2 (Weyl).

(a) *Suppose that $g : \mathbb{Z} \to \mathbb{R}$ is a polynomial of degree d, and let $0 < \delta < 1/2$. If $(g(n) \pmod{\mathbb{Z}})_{n\in[N]}$ is not δ-equidistributed in $\mathbb{R}/\mathbb{Z}$, then* *there is an integer k with $1 \le k \ll \delta^{-O_d(1)}$ such that $\|kg\|_{C^\infty[N]} \ll \delta^{-O_d(1)}$.*

(b) *Suppose that the parameter $\delta = \delta(N) \in (0,1)$ satisfies $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Further, suppose there are positive integers $k_1, \dots, k_d$ satisfying $k_j \ll \delta^{-2^{d-j}}$ such that*

$$\|k_j \alpha_j\|_{\mathbb{R}/\mathbb{Z}} \le \delta^{-2^{d-j}}/N^j.$$

Then, provided N is large enough, there is some positive integer $A = O_d(1)$ such that $(g(n) \pmod{\mathbb{Z}})_{n\in[N]}$ is not totally δ^A-equidistributed in $\mathbb{R}/\mathbb{Z}$.

Remarks. (1) The precise choice of exponents in the bounds $\delta^{-2^{d-j}}$ is not important to this result, but we will later make use of the fact that this way $k_d k_{d-1} \dots k_{d-j} \ll \delta^{-2^{j+1}+1}$.

(2) In part (b), the conditions $\|k_j\alpha_j\|_{\mathbb{R}/\mathbb{Z}} \le \delta^{-2^{d-j}}/N^j$ can be replaced by $\|k_j\beta_j\|_{\mathbb{R}/\mathbb{Z}} \le \delta^{-2^{d-j}}/N^j$ as they imply $\|k_j j!\beta_j\|_{\mathbb{R}/\mathbb{Z}} \ll \delta^{-2^{d-j}}/N^j$.

Proof. To prove (b), put $k = \operatorname{lcm}(k_1, \dots, k_d)$. Then, by the assumption on δ,

$$\|k\alpha_j\|_{\mathbb{R}/\mathbb{Z}} \le \delta^{-A'}/N^j = o(1)$$

for some $A' = O_d(1)$ for each $j \in [d]$. Consider the sequence

$$(g(kn))_{n\in[(N/k)\delta^{2A'}]}.$$

By (14.1), each $g(kn)$ in the range satisfies $\|g(k) - g(kn)\| \ll \delta^{A'}$. Thus $e \circ g = \exp(2\pi i g(\cdot))$ is almost constant on this range and we obtain, for N sufficiently large,

$$\Big|\mathbb{E}_{n\in[(N/k)\delta^{2A'}]} e(g(kn)) - \int\limits_{\mathbb{R}/\mathbb{Z}} e(x)\,dx\Big| \ge 1 - \left(\frac{2\pi\delta^{-A'}\delta^{2A'}N}{N}\right)^2 \gg \delta^{A'}\|e\|_{\mathrm{Lip}},$$

that is, $(g(n) \pmod{\mathbb{Z}})_{n\le N}$ is not totally $\delta^{2A'}/k = \delta^{O_d(1)}$-equidistributed. ■

The equidistribution of nilsequences is related to the equidistribution of certain polynomial sequences via the following projection theorem.

Proposition 14.3 (Green–Tao 'Quantitative Leibman theorem'). *Let m, d, N be positive integers, and let $\delta \in (0, 1/2)$ be a parameter. Let G/Γ be an m-dimensional nilmanifold together with a filtration $G_\bullet$ of degree d and a δ^{-1}-rational Mal'cev basis adapted to this filtration. Suppose that $g \in \operatorname{poly}(\mathbb{Z}, G_\bullet)$. Then there are positive constants B and B', only depending on m and d, such that the following holds. If $(g(n)\Gamma)_{n\le N}$ is not totally δ-equidistributed in G/Γ, then there is a non-trivial horizontal character η of modulus $|\eta| \ll \delta^{-O_{m,d}(1)}$ such that $(\eta \circ g(n))_{n\le N}$ is not totally δ^B-equidistributed in $\mathbb{R}/\mathbb{Z}$.*

Conversely, if there is a non-trivial horizontal character η of modulus $|\eta| \ll \delta^{-1}$ such that $(\eta \circ g(n))_{n\leq N}$ fails to be totally δ-equidistributed in $\mathbb{R}/\mathbb{Z}$, then $(g(n)\Gamma)_{n\leq N}$ is not totally $\delta^{B'}$-equidistributed in G/Γ.

Proof. If $(g(n)\Gamma)_{n\leq N}$ is not totally δ-equidistributed, then there is a progression $P = \{p_0, p_0 + q, \dots, p_0 + \ell q\}$ of length at least δN such that the sequence $(g(n)\Gamma)_{n\in P}$ fails to be δ-equidistributed. Define $g' \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ by $g'(n) := g(qn + p_0)$. Then [10, Thm. 2.9] implies that there is a non-trivial horizontal character $\eta : G \to \mathbb{R}/\mathbb{Z}$ of modulus $|\eta| \ll \delta^{-O_{m,d}(1)}$ such that $\|\eta \circ g'\|_{C^\infty[\delta N]} \ll \delta^{-O_{m,d}(1)}$. By Proposition 14.2(b), this implies that $\eta \circ g$ fails to be totally δ^B-equidistributed for some $B = O_{m,d}(1)$.

In the other direction, if there is a non-trivial horizontal η of modulus bounded by δ^{-1} such that $(\eta\circ g(n))_{n\leq N}$ fails to be totally δ-equidistributed, then we again find a progression $P = \{p_0, p_0 + q, \dots, p_0 + \ell q\}$ of length at least δN such that the sequence $(\eta\circ g(n)\Gamma)_{n\in P}$ fails to be δ-equidistributed. By Proposition 14.2(a) we have

$$\|\eta \circ g(p_0 + jq) - \eta \circ g(p_0 + (j - 1)q)\|_{\mathbb{R}/\mathbb{Z}} \ll \delta^{-O_{m,d}(1)}/N \tag{14.4}$$

for all $j \in \{1, \dots, \ell\}$. Since η is an additive character on a compact group, we have $\int_{(G/\Gamma)_{\mathrm{ab}}} e(\eta(x))\, dx = 0$. Consider the subprogression

$$P' = \{p_0, p_0 + q, \dots, p_0 + \ell' q\} \subset P,$$

where $\ell' = \delta^{B'} N$, with $B' = O_{m,d}(1)$ large enough so that (14.4) guarantees

$$\|\eta \circ g(p_0) - \eta \circ g(p_0 + jq)\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{|P'|}{N\delta^{O_{m,d}(1)}} \leq \frac{1}{4\pi}$$

for all $j, 0 \leq j \leq \ell'$. This implies

$$\Big|\mathbb{E}_{n\in P'}\, e(\eta \circ g(n)) - \int\limits_{G/\Gamma} e(\eta(x))\, dx\Big| = |\mathbb{E}_{n\in P'}\, e(\eta \circ g(n))| > \frac{1}{2},$$

using the fact that $\Re(e(x)) = \cos(2\pi x) \geq 1 - (2\pi x)^2 > 1/2$ for $x \leq 1/4$.

Since $\|e \circ \eta\|_{\mathrm{Lip}(G/\Gamma)} \ll \|e\|_{\mathrm{Lip}(\mathbb{R}/\mathbb{Z})}\|\eta\|_{\mathrm{Lip}(G/\Gamma)} \ll \delta^{-O_{m,d}(1)}$, where the bound on the Lipschitz constant of η comes from the bound on the modulus (cf. [10, Def. 2.6]) of the character, we may in fact choose $B' = O_{m,d}(1)$ large enough to ensure that also

$$1/2 > \delta^{B'}\|e \circ \eta\|_{\mathrm{Lip}}.$$

Thus, $(g(n))_{n\leq N}$ is not totally $\delta^{B'}$-equidistributed in G/Γ. ∎

15. Equidistribution of polynomial subsequences via Weyl's inequality. With the help of the quantitative Leibman theorem (Proposition 14.3), which reduces questions about the equidistribution of polynomial nilsequences to questions about the equidistribution of polynomials taking values in $\mathbb{R}/\mathbb{Z}$, we analyse in this section the distribution of polynomial subsequences of polynomial orbits.

The first result states that on the torus, polynomial subsequences of δ-equidistributed sequences are equidistributed too. Before stating this proposition properly we give an informal description of its contents here. A polynomial $g : \mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ is equidistributed if and only if one of its coefficients is irrational. Quantitative equidistribution is an assertion on whether or not there is a Lipschitz function $F : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ for which $|\mathbb{E}_{n\le N} F(g(n)) - \int_{\mathbb{R}/\mathbb{Z}} F|$ fails to be small. Approximating the Lipschitz function F by a Fourier series, one sees that studying this quantity is equivalent to studying the exponential sums $\mathbb{E}_{n\le N} e(\omega g(n))$ for certain rational ω. The latter is naturally approached by Weyl's inequality which then shows that the quantitative equidistribution of g is an assertion about whether or not there is a coefficient of g that is not close to a rational with small denominator. This rational approximation property is preserved when we consider compositions $g \circ P$ of g with an integral polynomial P whose leading coefficient is not too large. To see this we only need to consider the case where g has a 'highly irrational' coefficient. Take the largest-index coefficient of g which is 'highly irrational' and call it β_{i_0}. Then we may check that the largest-index coefficient of $g \circ P$ which arises from the highly irrational coefficient β_{i_0} of g is still considerably irrational. (Some bounds on the lower coefficients of P are needed in order to avoid cancellation.)

Proposition 15.1 (Equidistribution of polynomial subsequences: abelian case). *Suppose that $g : \mathbb{Z} \to \mathbb{R}$ is a polynomial of degree d and that $P(n) = \sum_{i=0}^{d'} \gamma_i n^i$ is a polynomial with integer coefficients of degree d' such that the leading coefficient $\gamma_{d'}$ is bounded by L_0, while all other coefficients satisfy the inequality $\gamma_i \le N^{(d'-i)/d'}$. Let $0 < \delta < 1/2$ and suppose $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Then there is some integer $A = O_d(1)$ such that when $(g(n) \pmod{\mathbb{Z}})_{n\in[N]}$ is totally δ-equidistributed and when $L_0 \le \delta^{-1/A}$, then $(g \circ P(n) \pmod{\mathbb{Z}})_{n\in[N^{1/d'}]}$ is totally $\delta^{1/O_{d,d'}(1)}$-equidistributed.*

Proof. Since g is totally δ-equidistributed, Proposition 14.2(b) implies that there is an integer $A' = O_d(1)$ such that no d-tuple of positive integers $k_1, \dots, k_d$ satisfies simultaneously $k_j \ll \delta^{-2^{d-j}/A'}$ and $\|k_j\beta_j\| \ll \delta^{-2^{d-j}/A'}/N^j$ for all $j = 1, \dots, d$. We deduce that there is some index i_0 among them such that $\|k_{i_0}\beta_{i_0}\| \ll \delta^{-2^{d-i_0}/A'} N^{-i_0}$ does not hold for any $k_{i_0} \ll \delta^{-2^{d-i_0}/A'}$. Suppose i_0 is maximal with this property. Then for all ℓ with $i_0 < \ell \le d$ we find $\kappa_\ell \ll \delta^{-2^{d-\ell}/A'}$ such that

$$\|\kappa_\ell \beta_\ell\| \le \delta^{-2^{d-\ell}/A'} N^{-\ell}. \tag{15.1}$$

For any $j \in \{1, \dots, d\}$, considering the jth term of

$$\sum_{j=0}^{d} \beta_j (P(n))^j = g \circ P(n)$$

we have

$$\beta_j (P(n))^j = \beta_j (\gamma_{d'})^j n^{jd'} + \beta_j Q_j(n),$$

where $Q_j(n)$ is a polynomial of degree $\leq jd' - 1$ such that the coefficient of n^i for any i is bounded by $O_{d,d'}(N^j N^{-i/d'} \delta^{-j/A})$ since

$$(P(n))^j = \Big(\sum_{t=1}^{d'} \gamma_t n^t\Big)^j = \sum_{(t_1,\dots,t_j)\in[d']^j} \gamma_{t_1} \dots \gamma_{t_j} n^{t_1+\dots+t_j}$$

and

$$\gamma_{t_1} \dots \gamma_{t_j} \leq L_0^j N^{j-(t_1+\dots+t_j)/d'}.$$

Define σ_i, $i = 0, \dots, dd'$, to be the following coefficients

$$\sum_{i=0}^{dd'} \sigma_i n^i = g \circ P(n) = \sum_{j=0}^{d} \beta_j (P(n))^j.$$

Comparing coefficients, each σ_i may be written as a linear combination of β_j with $j \geq i/d'$; $\sigma_{jd'}$ is the σ-coefficient of largest index whose representation in terms of β's contains β_j, which appears with coefficient $(\gamma_{d'})^j$ in the representation.

Next, we aim to show that there is $A'' = O_{d,d'}(1)$ such that every choice of $k_1, \dots, k_{dd'}$ with $k_j \leq \delta^{-2^{dd'-j}/A''}$ for each $j \in \{1, \dots, dd'\}$ contains some k_{j_0} such that

$$\|k_{j_0} \sigma_{j_0}\| > \delta^{-2^{dd'-j_0}/A''} N^{-j_0/d'}.$$

This, when applied with $k_j = qk$ for any $k \leq \delta^{-1/A''}$, would in view of (14.2) imply $\|k_j g \circ P\|_{C^\infty[N^{1/d'}]} \gg \delta^{-1/A''}$, from which the result follows by Proposition 14.2(a).

We will show that we can pick $j_0 = i_0 d'$. Thus, suppose for contradiction that

$$\|k_{i_0 d'} \sigma_{i_0 d'}\| \leq \delta^{-2^{dd'-i_0 d'}/A''} N^{-i_0} \tag{15.2}$$

holds for some $k_{i_0 d'} \leq \delta^{-2^{dd'-i_0 d'}/A''}$. Note that

$$k_{i_0 d'} \sigma_{i_0 d'} = k_{i_0 d'} (\gamma_{d'})^{i_0} \beta_{i_0} + \sum_{\ell > i_0} k_{i_0 d'} C_\ell \beta_\ell,$$

where the C_ℓ are integers of order $O_{d,d'}(N^{\ell - i_0} \delta^{-d/A})$ as can be deduced from the equation

$$C_\ell = \sum_{\substack{t_1,\dots,t_\ell \in [d'] \\ t_1+\dots+t_\ell = i_0 d'}} \gamma_{t_1} \cdots \gamma_{t_\ell}.$$

We wish to discard all the terms with $\ell > i_0$ in the above expression for $k_{i_0 d'}\sigma_{i_0 d'}$ in order to deduce that β_{i_0} is well approximable by rationals, which will hopefully lead us to the sought-for contradiction. Thus, in view of (15.1), we multiply the above expression for $k_{i_0 d'}\sigma_{i_0 d'}$ by $\kappa := \prod_{\ell > i_0} \kappa_\ell$. Inequality (15.2) yields

$$\begin{aligned}\|\kappa k_{i_0 d'}\sigma_{i_0 d'}\| &\ll \delta^{-2^{dd'-i_0 d'}/A''} \delta^{-(2^0+\dots+2^{d-i_0-1})/A'} N^{-i_0} \\ &= \delta^{-2^{dd'-i_0 d'}/A''} \delta^{-(2^{d-i_0}-1)/A'} N^{-i_0}.\end{aligned}$$

Writing $\bar{k} = k_{i_0 d'}(\gamma_{d'})^{i_0} \prod_{\ell > i_0} \kappa_\ell$, we have

$$k_{i_0 d'}\sigma_{i_0 d'} \prod_{\ell > i_0} \kappa_\ell = \bar{k}\beta_{i_0} + k_{i_0 d'} \sum_{\ell > i_0} \kappa C_\ell \beta_\ell,$$

where in view of (15.1) and the bound on the C_ℓ,

$$\begin{aligned}\|k_{i_0 d'}\kappa C_\ell \beta_\ell\| &\ll \delta^{-2^{dd'-i_0 d'}/A''} \delta^{-(2^0+\dots+2^{d-i_0-1})/A'} N^{-\ell} N^{\ell - i_0} \delta^{-d/A} \\ &= \delta^{-2^{dd'-i_0 d'}/A''} \delta^{-(2^{d-i_0}-1)/A'} \delta^{-d/A} N^{-i_0}.\end{aligned}$$

Recalling that $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$, this upper bound is seen to be $o(1)$. Together with the bound on $\|\kappa k_{i_0 d'}\sigma_{i_0 d'}\|$ this allows us to employ the triangle inequality provided N is large enough that no wrap-around issues can occur. In particular, this allows us to deduce that

$$\|\bar{k}\beta_{i_0}\| \ll \delta^{-2^{dd'-i_0 d'}/A''} \delta^{-(2^{d-i_0}-1)/A'} \delta^{-d/A} N^{-i_0}.$$

When we choose $A'' = 2^{dd'+1}A'$ and $A = 2dA'$ (to ensure that $L_0^j \leq \delta^{-d/A} \leq \delta^{-1/(2A')}$), this translates to

$$\|\bar{k}\beta_{i_0}\| \ll \delta^{-2^{d-i_0}/A'} N^{-i_0},$$

while we obtain the following bound on $\bar{k}$:

$$\bar{k} \leq \delta^{-2^{dd'-i_0 d'}/A''} L_0^{i_0} \delta^{-2^{d-i_0-1}/A'} \leq \delta^{-2^{d-i_0}/A'}.$$

Hence, we obtained a contradiction to the rational non-approximability properties of β_{i_0}. ■

Next, we slightly extend this result. Consider the binary quadratic form $f(x,y)$ for fixed y and its restriction to subprogressions modulo q in the x variable:

$$f(qx+r,y) = aq^2x^2 + x(2aqr + bqy) + (ar^2 + bry + cy^2).$$

This defines a quadratic polynomial $P(x) := \gamma_2 x^2 + \gamma_1 x + \gamma_0 := f(qx+r, y)$ in x. Being interested in (x, y) such that $f(x, y) \leq N$, we may suppose that $y \ll N^{1/2}$. Further assume that q is k-smooth (we will be interested in the case $q = \overline{W}$) and satisfies $q \ll N^{o(1)}$. Then the coefficients of this quadratic polynomial in x have the following properties: γ_2 is k-smooth, and $\gamma_2 \ll q^2 N^{(2-2)/2}$, $\gamma_1 \ll q^1 N^{(2-1)/2}$, $\gamma_0 \ll q^0 N^{(2-0)/2}$.

The proposition below is tailored to address polynomials with these specific properties.

Proposition 15.2. *Let $0 < \delta < 1/2$ and suppose $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Let k be a positive integer and suppose that the polynomial sequence $g : \mathbb{Z} \to \mathbb{R}$, $g(n) = \sum_{j=0}^{d} \beta_j n^j$, has the property that for every k-smooth integer q with $q \leq N^{o(1)}$, for every choice of $k_1, \ldots, k_d$ with $0 < k_j \leq \delta^{-2^{d-j}}$ for $j = 1, \ldots, d$, and for every sufficiently large N, we have*

$$\sup_{1 \leq j \leq d} \|q^j k_j \beta_j\| \delta^{2^{d-j}} (N/q)^j \geq 1.$$

If $P(n) = \sum_{i=0}^{d'} \gamma_i n^i$ is an integer-coefficient polynomial of degree d' whose leading coefficient is a k-smooth *integer satisfying $\gamma_{d'} < N^{o(1)}$, while all other coefficients satisfy $\gamma_i \leq N^{(d'-i)/d'} {\gamma_{d'}}^{i/d'}$, we obtain a conclusion similar to the one in the previous proposition:*

There is a k-smooth number $\tilde{q}$ with $\tilde{q} \ll N^{o(1)}$ such that each of the sequences $(g \circ P(\tilde{q}n + r) (\mathrm{mod}\, \mathbb{Z}))_{n \in [(N/\gamma_{d'} \tilde{q}^{d'})^{1/d'}]}$ for $r \in [\tilde{q}]$ is totally $\delta^{1/O_{d,d'}(1)}$-equidistributed, provided N is large enough.

Remark. The unconventional form of the inapproximability conditions imposed on the β_i comes from our choice of major and minor arcs (cf. Proposition 15.4 below and the next section).

Proof. Consider $q := \gamma_{d'}$, and let, as in the previous proof, i_0 be the maximal index for which

$$\|q^{i_0} k_{i_0} \beta_{i_0}\| \delta^{2^{d-i_0}} (N/q)^{i_0} \gg 1$$

for all $k_{i_0} \leq \delta^{-2^{d-i_0}}$. Thus, for $\ell > i_0$ there are $\kappa_\ell \leq \delta^{-2^{d-\ell}}$ such that

$$\|q^\ell \kappa_\ell \beta_\ell\| \ll \delta^{-2^{d-\ell}} (N/q)^{-\ell}. \tag{15.3}$$

We wish to employ this information to proceed as in the previous proof, that is, we wish to assume for contradiction that all coefficients of $g \circ P$ are close to rationals. In particular this would apply to the $(i_0 d')$th coefficient. Writing that coefficient as a linear combination of β's we would then like to deduce that β_{i_0} has to be close to a rational, which produces a contradiction. Unfortunately, the above information is not quite sufficient for our purposes yet: we require similar bounds on $\|\kappa_\ell \beta_\ell\|$ instead of on $\|q^\ell \kappa_\ell \beta_\ell\|$. To work around this, we pass to higher powers q^t of q, aiming to find a small t and an index i_t such that $\|q^{tdi_t}k_{i_t}\beta_{i_t}\| \gg \delta^{-2^{d-i_t}}(N/q^{dt})^{-i_t}$, while $\|q^{t\ell}k_\ell\beta_\ell\| \ll \delta^{-2^{d-\ell}}(N/q^t)^{-\ell}$ for $\ell > i_t$. The gap between q^{tdi_t} and $q^{t\ell}$ (for $\ell > i_t$) introduced by the extra factor d will be sufficient to analyse $g \circ P$ on subprogressions modulo $q^{td/d'}$.

Returning to the proof, note that (15.3) implies

$$\|q^{t\ell}\kappa_\ell\beta_\ell\| \leq q^{(t-1)\ell}\|q^\ell\kappa_\ell\beta_\ell\| \ll \delta^{-2^{d-\ell}}(N/q^t)^{-\ell}$$

for $\ell > i_0$ and for all positive integers t. By assumption on the rationality properties of the β_j, $j = 1, \dots, d$, there is an index i_1, which by the previous observation necessarily satisfies $i_1 \leq i_0$, such that

$$\|q^{2i_1}k_{i_1}\beta_{i_1}\|\delta^{2^{d-i_1}}(N/q^2)^{i_1} \gg 1$$

for all $k_{i_1} \leq \delta^{-2^{d-i_1}}$.

Proceeding like this, we obtain a decreasing sequence $i_0 \geq i_1 \geq i_2 \geq \cdots$ of positive integers such that for every j the following two families of inequalities hold:

$$\|q^{(j+1)i_j}k_{i_j}\beta_{i_j}\| \gg \delta^{-2^{d-i_j}}(N/q^{j+1})^{-i_j}$$

for all $k_{i_j} \leq \delta^{-2^{d-i_j}}$, and for every ℓ with $d \geq \ell > i_j$ there is $\kappa_\ell \leq \delta^{-2^{d-\ell}}$ such that

$$\|q^{(j+1)\ell}\kappa_\ell\beta_\ell\| \ll \delta^{-2^{d-\ell}}(N/q^{j+1})^{-\ell}.$$

By positivity of the indices i_j, there is $t = O_{d,d'}(1)$ such that $i_{t-1} = i_t = i_{t'}$ for all $t < t' \leq tdd'$. Setting $\tau = tdd'$, we therefore have

$$\|q^{(1+\tau)i_t}k_{i_t}\beta_{i_t}\|\delta^{2^{d-i_t}}(N/q^{1+\tau})^{i_t} \gg 1 \tag{15.4}$$

for all $k_{i_t} \leq \delta^{-2^{d-i_t}}$, while we find for every $\ell > i_t$ a positive integer $\kappa_\ell \leq \delta^{-2^{d-\ell}}$ such that

$$\|q^{t\ell}\kappa_\ell\beta_\ell\| \ll \delta^{-2^{d-\ell}}(N/q^t)^{-\ell}. \tag{15.5}$$

Now recall that $d' = \deg(P)$ and consider the sequence

$$g(P(q^{\tau/d'}n + r))_{n \in [(N/q^{\tau+1})^{1/d'}]}$$

for an arbitrary $r \in [q^{\tau/d'}]$. Defining coefficients σ_i by

$$\sum_{i=0}^{dd'} \sigma_i n^i = g(P(q^{\tau/d'}n + r)) = \sum_{j=0}^{d} \beta_j(P(q^{\tau/d'}n + r))^j,$$

we have

$$\sigma_{i_t d'} = \beta_{i_t}(\gamma_{d'}q^\tau)^{i_t} + \sum_{\ell > i_t} \beta_\ell q^{\tau i_t} C_\ell, \tag{15.6}$$

with integer coefficients C_ℓ. We need a bound on C_ℓ and proceed to show that $C_\ell = O(N^{\ell-i_t}q^{i_t})$. Expanding out products yields

$$(P(nq^{\tau/d'}+r))^\ell = \Big(\sum_{j=1}^{d'} \gamma_j (q^{\tau/d'}n+r)^j\Big)^\ell$$

$$= \sum_{\substack{(j_1,\dots,j_\ell)\\ \in[d']^\ell}} \gamma_{j_1}\dots\gamma_{j_\ell} \sum_{\substack{(u_1,\dots,u_\ell)\le\\ (j_1,\dots,j_\ell)}} \binom{j_1}{u_1}\dots\binom{j_\ell}{u_\ell}(q^{\tau/d'}n)^{u_1+\dots+u_\ell} r^{(j_1-u_1)+\dots+(j_\ell-u_\ell)}.$$

Consider any term involving $(q^{\tau/d'}n)^{i_t d'} = q^{\tau i_t}n^{i_t d'}$.

If $j_1+\dots+j_\ell = u_1+\dots+u_\ell = i_t d'$, then the coefficient of $q^{\tau i_t}n^{i_t d'}$ is $\gamma_{j_1}\dots\gamma_{j_\ell} \le N^{\ell-i_t}q^{i_t}$. If $j_1+\dots+j_\ell > u_1+\dots+u_\ell = i_t d'$, then the coefficient of $(q^t n)^{i_t d'}$ is bounded by $O_{d,d'}(\gamma_{j_1}\dots\gamma_{j_\ell}r^{\ell d'}) = O_{d,d'}(N^{\ell-i_t-1/d'}q^\ell r^{\ell d'}) = O(N^{\ell-i_t})$, since $r < q^{\tau/d'} \ll N^{o(1)}$. Thus in total, $C_\ell = O(N^{\ell-i_t}q^{i_t})$.

We return to analysing the rational approximations of the individual terms of (15.6). Notice that $\tau \ge t\ell$ for all $\ell \in [d]$. Thus (15.5) guarantees for $\ell > i_t$ the existence of $\kappa_\ell \le \delta^{-2^{d-\ell}}$ such that

$$\|\beta_\ell\kappa_\ell q^{\tau i_t}C_\ell\| \ll \delta^{-2^{d-\ell}}N^{-\ell}q^{\tau i_t}C_\ell \ll \delta^{-2^{d-\ell}}N^{-i_t}(q^{\tau+1})^{i_t}. \tag{15.7}$$

We are finally in a position to show that there is $A = O_{d,d'}(1)$ such that

$$g(P(q^{\tau/d'}n+r))_{n\in[(N/q^{\tau+1})^{1/d'}]}$$

is totally $\delta^{1/A}$-equidistributed. More precisely, we show that there is $A' = O_{d,d'}(1)$ such that for every $k_{i_t d'} \le \delta^{-2^{dd'-i_t d'}/A'}$,

$$\|k_{i_t d'}\sigma_{i_t d'}\| > (N/q^{\tau+1})^{-i_t}\delta^{-2^{d'(d-i_t)}/A'}.$$

Hence the result follows from Proposition 14.2(a). Suppose for contradiction that

$$\|k_{i_t d'}\sigma_{i_t d'}\| \le (N/q^{\tau+1})^{-i_t}\delta^{-2^{d'(d-i_t)}/A'}$$

for some $k_{i_t d'} \le \delta^{-2^{dd'-i_t d'}/A'}$. Let $\kappa := \kappa_d\dots\kappa_{i_t+1}$ (or $\kappa = 1$ when the product is empty), then, since $\kappa_\ell \le \delta^{-2^{d-\ell}}$,

$$\|\kappa k_{i_t d'}\sigma_{i_t d'}\| \ll (N/q^{\tau+1})^{-i_t}\delta^{-2^{d'(d-i_t)}/A'}\delta^{-(2^{d-i_t}-1)}.$$

Considering the summands in (15.6), the bounds (15.7) imply

$$\|\beta_\ell\kappa q^{\tau i_t}C_\ell\| \ll \delta^{-(2^{d-i_t}-1)}\delta^{-2^{d'(d-i_t)}/A'}N^{-i_t}(q^{\tau+1})^{i_t}.$$

Appealing to the assumptions that both q and δ^{-1} are bounded by $N^{o(1)}$, the above is seen to equal $O(N^{-1+o(1)}) = o(1)$ since $i_t \ge 1$. Thus, provided N is large enough, no wrap-around issues appear when examining the circle norm $\|k_{i_t d'}\kappa\sigma_{i_t d'}\|$ and we obtain the following statement on rational approximation of β_{i_t}:

$$\begin{aligned}\|k_{i_t d'}\kappa\beta_{i_t}(\gamma_{d'}q^\tau)^{i_t}\| = \|k_{i_t d'}\kappa\beta_{i_t}(q^{\tau+1})^{i_t}\| &= \Big\|k_{i_t d'}\kappa\sigma_{i_t d'} - \sum_{\ell>i_t}\beta_\ell\kappa q^{\tau i_t}C_\ell\Big\| \\ &\le |k_{i_t d'}\kappa\sigma_{i_t d'}| + \sum_{\ell>i_t}|\beta_\ell\kappa q^{\tau i_t}C_\ell| \\ &\ll \delta^{-(2^{d-i_t}-1)}\delta^{-2^{d'(d-i_t)}/A'}N^{-i_t}(q^{\tau+1})^{i_t}.\end{aligned}$$

Choosing $A' = 2^{d'(d-i_t)}$, this shows that there is $\bar{k}$, namely $\bar{k} = k_{i_t d'}\kappa a^{i_t}$, bounded by $\delta^{-2^{d-i_t}}$ such that

$$\|\bar{k}\beta_{i_t}q^{\tau+1}\| \ll \delta^{-2^{d-i_t}}(N/q^{\tau+1})^{-i_t},$$

contradicting (15.4). ■

Combining either of the previous two results with the quantitative Leibman theorem yields the general case of the equidistribution theorem for subsequences.

Proposition 15.3 (Equidistribution of polynomial subsequences). *Let N, d, d' be positive integers, let L_0 and $\delta \in (0,1/2)$ be parameters, and suppose that $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Let $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ be a polynomial sequence of degree d and suppose that the finite orbit $(g(n)\Gamma)_{n\in[N]}$ is totally δ-equidistributed in G/Γ. Let $P : \mathbb{Z} \to \mathbb{Z}$ be an integer-coefficient polynomial of degree d' whose coefficients are bounded by L_0.*

Then there is some $A = O_{d,d'}(1)$ such that whenever $L_0^A < \delta$, then the polynomial subsequence $((g \circ P)(n))_{n\in[(N/\gamma_{d'})^{1/d'}]}$ is totally $\delta^{1/O_{d,d'}(1)}$-equidistributed on G/Γ.

Proof. We first pass to the abelian setting: by Proposition 14.3, there are constants $A, A' = O_{m,d}(1)$ such that every sequence $(\eta\circ g(n))_{n\in[N]}$ for a horizontal character η of modulus at most δ^{-A} is totally $\delta^{1/A'}$-equidistributed. Applying Proposition 15.1, we deduce that for each such character η the sequence $(\eta\circ g\circ P(n))_{n\in[(N/\gamma_{d'})^{1/d'}]}$ is totally $\delta^{1/O_{d,d',m}(1)}$-equidistributed in $\mathbb{R}/\mathbb{Z}$. An application of the other direction of Proposition 14.3 then allows us to return to G/Γ and deduce the stated equidistribution property of $(g\circ P(n))_{n\in[(N/\gamma_{d'})^{1/d'}]}$ in G/Γ. ■

Similarly, Proposition 15.2 results in an assertion for polynomial orbits on general nilsequences:

Proposition 15.4. *Let N, d, d', k be positive integers, and let $\delta \in (0,1/2)$ be such that $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Let $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ be a polynomial sequence of degree d and suppose that for every k-smooth number q with $q \ll N^{o(1)}$, the sequence $(g(qn)\Gamma)_{n\in[N/q]}$ is totally δ-equidistributed in G/Γ.*

Suppose further that $P : \mathbb{Z} \to \mathbb{Z}$ is an integer-coefficient polynomial of degree d' as in Proposition 15.2. *That is, if $P(n) = \sum_{i=0}^{d'} \gamma_i n^i$, then $\gamma_{d'}$ is a k-smooth integer with $\gamma_{d'} < N^{o(1)}$, while all other coefficients satisfy the inequality $\gamma_i \leq N^{(d'-i)/d'} \gamma_{d'}^{i/d'}$.*

Then there is a k-smooth number $\tilde{q}$ with $\tilde{q} \ll N^{o(1)}$ such that each of the sequences $(g \circ P(\tilde{q}n + r)\Gamma)_{n \in [(N/\gamma_{d'}\tilde{q}^{d'})^{1/d'}]}$ for $r \in [\tilde{q}]$ is totally $\delta^{1/O_{d,d'}(1)}$-equidistributed in G/Γ, provided N is large enough.

Proof. Let $\eta : G/\Gamma \to \mathbb{R}/\mathbb{Z}$ be an arbitrary non-trivial horizontal character of modulus bounded by $\delta^{-O_{m,d}(1)}$ and suppose that $\eta \circ g$ has the polynomial representation $\eta \circ g(n) = \sum_{j=0}^{d} \beta_j n^j$ in $\mathbb{R}/\mathbb{Z}$. Let $q \leq N^{o(1)}$ be k-smooth and consider the sequence

$$(\eta \circ g(qn)\Gamma)_{n \in [N/q]}.$$

By the equidistribution assumption on the subsequences of g, and by Propositions 14.3 and 14.2(b), there is an integer $B = O_d(1)$ such that for every choice of $k_1, \dots, k_d$ with $0 < k_j \leq \delta^{-2^{d-j}/B}$ for $j = 1, \dots, d$, and for every sufficiently large N, we have

$$\sup_{1 \leq j \leq d} \|q^j k_j \beta_j\| \delta^{2^{d-j}/B} (N/q)^j \geq 1.$$

Thus, with $\delta^{1/B}$ in place of δ, the conditions of Proposition 15.2 are satisfied and hence there is $\tilde{q} \ll N^{o(1)}$ such that for every $r \in [\tilde{q}]$ the sequence

$$(\eta \circ g \circ P(\tilde{q}n + r) \pmod{\mathbb{Z}})_{n \in [(N/\gamma_{d'}\tilde{q})^{1/d'}]}$$

is totally $\delta^{1/O_{d,d'}(1)}$-equidistributed in $\mathbb{R}/\mathbb{Z}$, provided N is large enough. An application of Proposition 14.3 to get back to G/Γ gives the result. ■

16. The factorisation into minor and major arcs. In view of the previous section, a 'minor arc sequence' $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ should satisfy the conditions of Proposition 15.4 in order to guarantee its applicability. That is, given $k \in \mathbb{N}$, $\delta = \delta(N) \in (0, 1/2)$, and $R \ll N^{o(1)}$, the sequence g should have the property that for every k-smooth number $q \leq R$ the finite sequence $(g(qn)\Gamma)_{n \in [N/q]}$ is δ-equidistributed in G/Γ.

In this section we will achieve a factorisation of an arbitrary polynomial sequence g into a product $\varepsilon g' \gamma$, where ε is slowly varying ('smooth'), γ is periodic with a k-smooth common difference, and g' has the 'minor arc property' described above. We will ensure that g' satisfies a slightly stronger version of this: when we restrict g' to subprogressions on which γ is constant and on which ε is almost constant, then the restricted sequence still enjoys the 'minor arc property'.

This factorisation will be obtained by iteration of the Green–Tao factorisation theorem [10, Thm. 1.19] employing its dimension reduction as a guarantee for termination of the iteration. Before we state the factorisation theorem, we recall the notion of smoothness of sequences.

DEFINITION 16.1 ((M,N)-smooth sequence, [10, Def. 1.18]). Let G/Γ be a nilmanifold together with a Q-rational Mal'cev basis $\mathcal{X}$ and metric $d = d_{\mathcal{X}}$. Let $(\varepsilon(n))_{n\in\mathbb{Z}}$ be a sequence in G, and let $M, N \geq 1$. Then ε is said to be (M,N)-*smooth* if both $d(\varepsilon(n), \mathrm{id}_G) \leq M$ and $d(\varepsilon(n), \varepsilon(n-1)) \leq M/N$ are satisfied for all $n \in [N]$.

In the later iteration of the Green–Tao factorisation theorem we will encounter a product of smooth sequences, which needs to be shown to be smooth itself. Notice therefore that, when $(\varepsilon(n))_{n\in\mathbb{Z}}$ is (M,N)-smooth and when $(\varepsilon'(n))_{n\in\mathbb{Z}}$ is $(M,N/q)$-smooth, then the triangle inequality and right-invariance of the metric d yield

$$d(\varepsilon(qn+j)\varepsilon'(n), \mathrm{id}_G) \leq d(\varepsilon(qn+j), \mathrm{id}_G) + d(\varepsilon'(n), \mathrm{id}_G) \leq 2M$$

for all $n \in [N/q]$. Employing also the approximate left-invariance of d (see [10, Lemma A.5]), we obtain

$$d(\varepsilon(qn+j)\varepsilon'(n), \varepsilon(q(n-1)+j)\varepsilon'(n-1)) \leq 2qQ^{O(1)}M/N.$$

Thus, $(\varepsilon(qn+j)\varepsilon'(n))_{n\in\mathbb{Z}}$ is $(2Q^{O(1)}M, N/q)$-smooth.

The tool to split into major and minor arcs is the following Green–Tao factorisation theorem.

THEOREM 16.2 (Green–Tao, [10, Thm. 1.198]). *Let $m, d \geq 0$, and let $Q_0, N \geq 1$ and $A > 0$ be real numbers. Suppose that G/Γ is an m-dimensional nilmanifold together with a filtration $G_\bullet$ of degree d. Suppose that $\mathcal{X}$ is a Q_0-rational Mal'cev basis $\mathcal{X}$ adapted to $G_\bullet$ and that $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$. Then there is an integer Q with $Q_0 \leq Q \ll Q_0^{O_{A,m,d}(1)}$, a rational subgroup $G' \subseteq G$, a Mal'cev basis $\mathcal{X}'$ for G'/Γ' in which each element is a Q-rational combination of the elements of $\mathcal{X}$, and a decomposition $g = \varepsilon g' \gamma$ into polynomial sequences $\varepsilon, g', \gamma \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ with the following properties:*

1. *$\varepsilon : \mathbb{Z} \to G$ is (Q,N)-smooth;*
2. *$g' : \mathbb{Z} \to G'$ takes values in G', and the finite sequence $(g'(n)\Gamma')_{n\in[N]}$ is $1/Q^A$-equidistributed in G'/Γ', using the metric $d_{\mathcal{X}'}$ on G'/Γ';*
3. *$\gamma : \mathbb{Z} \to G$ is Q-rational, and $(\gamma(n)\Gamma)_{n\in\mathbb{Z}}$ is periodic with period at most Q.*

The proof of our modified factorisation theorem will proceed via an iterative application of the theorem stated above. Our next aim is to prove an auxiliary lemma which will guarantee that the iteration process stops after finitely many steps. The way this goal is attained is to ensure that every time we refine our splitting of $[N]$ into subprogressions, the polynomial sequence

g we try to factorise fails to be totally equidistributed (with some parameter) on *each* of the new subprogressions. This way an application of the factorisation theorem on any new subprogression yields a *lower* dimensional rational subgroup.

LEMMA 16.3. *Let G/Γ be an m-dimensional nilmanifold and let $g \in \mathrm{poly}(G_\bullet, \mathbb{Z})$ be a polynomial sequence of degree d. Let $\delta \in (0, 1/2)$ be such that $\delta^{-t} \ll_t N$ for all $t \in \mathbb{N}$. Further let $a \leq \delta^{-1}$ be an integer, and $b \in [a]$. Suppose that $(g(q(an+b))\Gamma)_{n\in[N/q]}$ fails to be δ-equidistributed in G/Γ for some $q \ll N^{o(1)}$. Then there is some $B = O_{m,d}(1)$ such that each of the sequences $(g(n(aq)^d + r)\Gamma)_{n\in[N/q^d]}$ for $r \in [(aq)^d]$ fails to be δ^B-equidistributed in G/Γ.*

Proof. By Propositions 14.3 and 14.2(a), there is a non-trivial horizontal character η of modulus bounded by $\delta^{-O_{m,d}(1)}$ such that the function $h : \mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ defined by $h(n) := \eta \circ g(q(an + b))$ satisfies $\|h\|_{C^\infty[N/aq]} \ll \delta^{-O_{m,d}(1)}$. Let $\eta \circ g(n) = \sum_{j=0}^d \beta_j n^j$ and $\eta \circ g(q(an + b)) = \sum_{j=0}^d \sigma_j n^j$ be polynomial representations in $\mathbb{R}/\mathbb{Z}$. Then

$$\sup_{1\leq j\leq d} \|\sigma_j\|(N/aq)^j \ll \delta^{-O_{m,d}(1)}.$$

Since

$$\sigma_j = \beta_j(aq)^j + \sum_{\ell>j} \binom{\ell}{j} \beta_\ell (aq)^j (bq)^{\ell-j}, \tag{16.1}$$

we find, using a downward induction starting with $j = d$, that

$$\|\beta_j(aq)^d\| \ll \delta^{-O_{m,d}(1)} N^{-j}(aq)^d = o(1).$$

Indeed, for $j = d$ the assertion is immediate. Suppose now it holds for $j \in \{j_0 + 1, \ldots, d\}$ for some $j_0 \geq 1$. We proceed to check the case where $j = j_0$ by analysing (16.1) for $j = j_0$, multiplied through by $t = (aq)^{d-j_0}$. Observe that for all positive integers t and for all $i \in \{1, \ldots, d\}$,

$$\|\sigma_i t\| \ll t\|\sigma_i\| \ll tN^{-i}(aq)^i \delta^{-O_{m,d}(1)}.$$

By the assumptions on δ, a and q, this bound is $o(1)$ when $t = (aq)^{d-j_0}$ and $i = j_0$. Similarly, the induction hypothesis implies that for every $\ell \in \{j_0 + 1, \ldots, d\}$ and all t we have

$$\|\beta_\ell(aq)^d t\| \ll t\|\beta_\ell(aq)^d\| \ll tN^{-\ell}(aq)^d \delta^{-O_{d,m}(1)},$$

which certainly is $o(N^{-j_0}(aq)^d \delta^{-O_{d,m}(1)})$ if we set $t = (qb)^{\ell-j_0}$. This allows us to apply the triangle inequality to split up $\|\sigma_{j_0}(aq)^{d-j_0}\|$ in the manner of (16.1) to deduce the assertion for j_0.

Next, pick $r \in [(aq)^d]$ and define $\tilde{\sigma}_0, \ldots, \tilde{\sigma}_d$ such that $\eta \circ g((aq)^d n + r) = \sum_{j=0}^d \tilde{\sigma}_j n^j$; then

$$\tilde{\sigma}_j = \sum_{\ell=j}^{d} \binom{\ell}{j} r^{\ell-j}(aq)^{jd}\beta_\ell.$$

Since $jd \geq d$ for all $j \in \{1,\dots,d\}$, we have

$$\begin{aligned}\left\| \binom{\ell}{j} r^{\ell-j}(aq)^{jd}\beta_\ell \right\| &\ll \binom{\ell}{j} r^{\ell-j}(aq)^{(j-1)d}\|(aq)^d\beta_\ell\| \\ &\ll_d r^{\ell-j}(aq)^{jd}N^{-\ell}\delta^{-O_{d,m}(1)} \ll_d (aq)^{\ell d}N^{-\ell}\delta^{-O_{d,m}(1)}.\end{aligned}$$

By the assumptions on δ and q, this bound equals $o(1)$ and hence we can apply the triangle inequality to split up $\|\tilde{\sigma}_j\|$:

$$\|\tilde{\sigma}_j\| \ll_d \sum_{\ell=j}^{d}(aq)^{\ell d}N^{-\ell}\delta^{-O_{d,m}(1)} \ll_d (N/(aq)^d)^{-j}\delta^{-O_{d,m}(1)}.$$

By Propositions 14.2(b) and 14.3, this implies the result. ∎

Now we finally turn to the modified factorisation theorem which gives the correct type of minor arcs.

Theorem 16.4 (Modified factorisation theorem). *Let $m, d, N, A \geq 1$ be integers, and let $k, Q_0, R \geq 1$ be integer parameters. Suppose that G/Γ is a m-dimensional nilmanifold together with a filtration $G_\bullet$ of degree d. Suppose that $\mathcal{X}$ is a Q_0-rational Mal'cev basis $\mathcal{X}$ adapted to $G_\bullet$ and that $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$. Suppose further that $Q_0 \ll \log k$ and $k, R = O(N^{o(1)})$. Then there is an integer Q with $Q_0 \leq Q \ll Q_0^{O_{A,m,d}(1)}$, and a partition of $[N]$ into at most R^{dm} disjoint subprogressions P, each of length at least N/R^{dm} and each of k-smooth common difference bounded by R^{dm} such that the restriction of $(g(n))_{n\in P}$ to any of the progression P can be factorised as follows.*

There is a rational subgroup $G' \leq G$, depending on P, and a Mal'cev basis $\mathcal{X}'$ for G'/Γ' such that every element of $\mathcal{X}'$ is a Q-rational combination of elements from $\mathcal{X}$ (that is, each coefficient is rational of height bounded by Q). Suppose $P = \{n \equiv r \pmod q\}$. Then we have a factorisation

$$g(qn + r) = \varepsilon_P(n)g'_P(n)\gamma_P(n),$$

where $\varepsilon_P, g'_P, \gamma_P$ are polynomial sequences from $\mathrm{poly}(\mathbb{Z}, G_\bullet)$ with the properties

1. *$\varepsilon_P : \mathbb{Z} \to G$ is $(Q, N/q)$-smooth;*
2. *$g'_P : \mathbb{Z} \to G'$ takes values in G' and for each k-smooth number $\tilde{q} \leq R$ the finite sequence $(g'_P(\tilde{q}n)\Gamma')_{n\leq N/(q\tilde{q})}$ is totally Q^{-A}-equidistributed in G'/Γ';*
3. *$\gamma_P : \mathbb{Z} \to G$ is Q-rational and $(\gamma_i(n)\Gamma)_{n\in\mathbb{Z}}$ is periodic with a k-smooth period which is bounded by $R^{md}Q$.*

Proof. We may suppose that g does not satisfy (2), that is, there is some k-smooth integer $q_1 \leq R$ and $b_1 < a_1 \leq Q_0^A$ such that $(g(q_1(a_1 n + b_1))\Gamma)_{n \leq N/q_1}$ fails to be Q_0^{-A}-equidistributed. Writing $z_1 := (a_1 q_1)^d$, Lemma 16.3 implies that each of the sequences $(g(z_1 n + r_1)\Gamma)_{n \leq N/z_1}$ with $r_1 \in [z_1]$ fails to be $Q_0^{-AA'}$-equidistributed for some $A' = O_{m,d}(1)$. Now, we run through all $r_1 \in [z_1]$ in turn.

Applying the factorisation theorem in its original form to any of these sequences yields some $Q_1 \ll Q_0^{O(A,m,d)}$, a proper Q_1-rational subgroup $G_1 < G$ of dimension strictly smaller than m, and a factorisation

$$g(z_1 n + r_1) = \varepsilon_{r_1}(n) g'_{r_1}(n) \gamma_{r_1}(n)$$

where the finite sequence $(g'_{r_1}(n)\Gamma_1)_{n \leq N/z_1}$ is totally Q_1^{-A}-equidistributed in

$$G_1/\Gamma_1 := G_1/(\Gamma \cap G_1).$$

If g'_{r_1} is Q_1^{-A}-equidistributed on every subprogression $\{n \equiv b_2 \pmod{a_2 q_2}\}$ of k-smooth common difference $a_2 q_2$, where $b_2 < a_2 < Q_1^A$ and $q_2 < R$, then we stop (and turn to the next choice of r_1). Otherwise, invoking Lemma 16.3 again, there is a k-smooth integer $a_2 q_2$ as above such that with $z_2 := (a_2 q_2)^d$ the finite sequence $(g_{r_1,r_2}(n))_{n \leq N/(z_1 z_2)}$ defined by $g_{r_1,r_2}(n) := g'_{r_1}(z_2 n + r_2)$ is not Q_1^{-A}-equidistributed for any $r_2 \in [z_2]$. We proceed as before.

This process yields a tree of operations which has height at most $m = \dim G$, since each time the factorisation theorem is applied a new sequence $g'_{r_1,\dots,r_i}$ is found that takes values in some strictly lower dimensional submanifold $G_i = G_i(r_1, \dots, r_i)$ of $G_{i-1}(r_1, \dots, r_{i-1})$. Thus, we can apply the factorisation theorem at most m times in a row before the manifold involved has dimension 0.

The tree we run through starts with g, which has z_1 neighbours g_{r_1}, one for each $r_1 \in [z_1]$. Each g_{r_1} has $z_2 = z_2(r_1, r_2)$ neighbours g_{r_1,r_2}, one for each $r_2 \in [z_2]$, etc.

As a result, we obtain a decomposition of the range $[N]$ into at most R^{2dm} subprogressions of the form

$$\begin{aligned} P &= \{z_1(z_2(\dots(z_t m + r_t)\dots) + r_2) + r_1 : m \leq N/(z_1 \dots z_t)\} \\ &= \{z_1 \dots z_t m + r : m \leq N/(z_1 \dots z_t)\}, \end{aligned}$$

for some r, and where each z_i depends on $r_1, \dots, r_{i-1}$. The common difference of such a progression P is k-smooth and bounded by R^{2dm}. Thus, P has length at least $N/R^{2dm} = N^{1-o_m(1)}$. The iteration process furthermore yields a factorisation of $g_{r_1,\dots,r_t}$, which is the restriction of g to P:

$$g_{r_1,\dots,r_t}(m) = g(z_1 \dots z_t m + r) = \tilde{\varepsilon}_{r_1,\dots,r_t}(m) g'_t(m) \tilde{\gamma}_{r_1,\dots,r_t}(m),$$

where

$$\tilde{\varepsilon}_{r_1,\dots,r_t}(m) = \varepsilon_{r_1}(z_2 \dots z_t m + \tilde{r}_2) \dots \varepsilon_{r_1,\dots,r_{t-1}}(z_t m + \tilde{r}_t) \varepsilon_{r_1,\dots,r_t}(m)$$

for certain integers $\tilde{r}_2, \ldots, \tilde{r}_t$, and

$$\tilde{\gamma}_{r_1,\ldots,r_t}(m) = \gamma_{r_1,\ldots,r_t}(m)\gamma_{r_1,\ldots,r_{t-1}}(z_t m + \tilde{r}_t) \ldots \gamma_{r_1}(z_2 \ldots z_t m + \tilde{r}_2).$$

In view of the remarks following the definition of smoothness of sequences, the factor $\tilde{\varepsilon}_{r_1,\ldots,r_t}(m)$ is a $(Q_0^{O_{A,d,m}(1)}, N/(z_1 \ldots z_t))$-smooth sequence. Further, the periodic sequences $\tilde{\gamma}_{r_1,\ldots,r_t}(m)$ are easily seen to have a $Q_0^{O_{A,d,m}(1)}$-smooth, i.e. k-smooth, period. ∎

17. Reduction to the case of minor arc nilsequences. With the help of the modified factorisation theorem (Theorem 16.4), we will show that the general non-correlation estimate follows from the special case of non-correlation with 'minor arc nilsequences' that enjoy property (ii) of the modified factorisation theorem.

The general case is the following proposition.

Proposition 17.1. *Let G/Γ be a nilmanifold of dimension $m \geq 1$, let $G_\bullet$ be a filtration of G of degree $d \geq 1$, and let $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$ be a polynomial sequence. Suppose that G/Γ has a Q-rational Mal'cev basis $\mathcal{X}$ for some $Q \geq 2$, defining a metric $d_{\mathcal{X}}$ on G/Γ. Suppose that $F : G/\Gamma \to [-1,1]$ is a Lipschitz function, and let $M_0 = \log\log\log N$ and $N' = \lfloor N/\overline{W} \rfloor$. Then*

$$|\mathbb{E}_{n\in[N']}(r'_{f,\beta}(n) - 1)F(g(n))\Gamma| \ll_{m,d,\gamma,A} Q^{O_{m,d,\gamma,A}(1)}(1 + \|F\|)M_0^{-A}$$

for any $A > 0$ and $N \geq 2$.

As in §2 of [9], we will deduce this result from the following special case involving only 'minor arc nilsequences'.

Proposition 17.2 (Non-correlation, equidistributed case). *Let $N > 0$ be a large integer and let δ, k and R be parameters such that $\delta \in (0, 1/2)$, $\delta^{-t} \ll_t N'$ for all $t \in \mathbb{N}$, $R \ll N^{o(1)}$ and $k = w(N)$. Suppose that $(G/\Gamma, d_{\mathcal{X}})$ is an m-dimensional nilmanifold with some filtration $G_\bullet$ of degree d and suppose that $g \in \mathrm{poly}(\mathbb{Z}, G_\bullet)$. Suppose further that for every k-smooth number $\tilde{q} \leq R$ the finite sequence $(g(\tilde{q}n)\Gamma)_{n\in[N'/\tilde{q}]}$ is δ-equidistributed in G/Γ. Then for every Lipschitz function $F : G/\Gamma \to \mathbb{R}$ satisfying $\int_{G/\Gamma} F = 0$ and for every k-smooth number $q \ll N^{o(1)}$ and every $r \in [q]$, we have*

$$|\mathbb{E}_{n\in[N']}(r'_{f,\beta}(qn + r) - 1)F(g(n)\Gamma)| \ll \delta^c \|F\|$$

for some c such that $c^{-1} = O_{m,d}(1)$.

Proof of Proposition 17.1 assuming Proposition 17.2. Observe that $N' = N^{1-o(1)}$. We may assume that $Q \leq M_0$, thus $Q \leq M_0 = \log w(N)$. The modified factorisation theorem can now be applied to the sequence $(g(n)\Gamma)_{n\leq N}$ with the following parameters: $k = w(N)$, $Q_0 = \log w(N)$, $R = N^{o(1)}$. This yields a partition of $[N']$ into at most R^{2md} progressions of $w(N)$-smooth common differences. By the triangle inequality, it suffices to show that

$$|\mathbb{E}_{n\in P}(r'_{f,\beta}(n)-1)F(g(n)\Gamma)| \ll_{m,d,\gamma,A} Q^{O_{m,d,\gamma,A}(1)}(1+\|F\|)M_0^{-A}$$

for every progression P in the partition.

For each of these progressions $P =: \{q_P n + r_P\}$, the modified factorisation theorem provides us with a factorisation of the restriction of g to P:

$$g(q_P n + r_P) =: g_P(n) = \varepsilon_P(n) g'_P(n)\gamma_P(n),$$

where $\varepsilon_P, g'_P, \gamma_P$ satisfy (i)–(iii) from Theorem 16.4. Proceeding as in [9, §2] (see *loc. cit.* for full details), we split each P into subprogressions $P = P_1 \cup \cdots \cup P_t$ in such a way that

- $\gamma_P(n)$ is constant on each progression, say $\gamma_P(n) = \gamma_j$ for $n \in P_j$, and
- $\varepsilon_P(n)$ is almost constant: to be precise, $|n-n'| \le N'/(qQ^B)$ for some $B = O(1)$ and all $n, n' \in P_j$, which implies $d(\varepsilon_P(n), \varepsilon_P(n')) \le Q^{-B+1}$ by smoothness of ε_P.

From each P_j, we choose a fixed element, say n_j. Then the Lipschitz property of F, right-invariance of the metric, and smoothness of ε_P imply that for every $n \in P_j$,

$$|F(\varepsilon_P(n)g'_P(n)\gamma(n)\Gamma) - F(\varepsilon_P(n_j)g'_P(n)\gamma_j\Gamma)| \le Q^{-B/2},$$

provided B was chosen large enough. Hence it suffices to show that

$$|\mathbb{E}_{n\in P_j}(r'_{f,\beta}(n)-1)F(\varepsilon_P(n_j)\gamma_j(\gamma_j^{-1}g'_P(n)\gamma_j)\Gamma)| \\ \ll_{m,d,\gamma,A} Q^{O_{m,d,\gamma,A}(1)}(1+\|F\|)M_0^{-A}.$$

The aim is now to apply Proposition 17.2 to $g_j : \mathbb{Z} \to \gamma_j^{-1}G\gamma_j =: H_j$,

$$g_j(n) := \gamma_j^{-1}g'_P(q_{P_j}n + r_{P_j})\gamma_j.$$

Property (ii) of the modified factorisation theorem was set up so as to ensure that g_j still enjoys the 'minor arc property' (on $H_j/(\Gamma\cap H_j)$ rather than G/Γ of course). Note that the Lipschitz constant of $F_j : H_j/(\Gamma \cap H_j) \to \mathbb{C}$, $F_j(x(\Gamma\cap H_j)) := F(\varepsilon_P(n_j)\gamma_j\Gamma)$ is bounded by $M\|F\|$ by [10, Lemma A.16]. Since P_j has a $w(N)$-smooth common difference and length at least $N^{1-o(1)}$, Proposition 7.4 implies that $r_{f,\beta}-1$ does not correlate with any function $n \mapsto c1_{P_j}(n)$, where c is a constant. Hence we can subtract off the mean value of F_j and reduce to the assumption $\int_{H_j/\Lambda_j} F_j = 0$.

All remaining technical details work exactly as in [9, §2 and App. B], so we have chosen, given their technical complexity, to omit them here. ∎

18. Completion of the non-correlation estimate. We complete the proof of Proposition 17.2 and therefore the analysis of correlation of $r'_{f,\beta}$ with nilsequences. Recalling the conditions of Proposition 17.2, we are given a polynomial sequence $(g(n)\Gamma)_{n\in[N']}$ such that for every $w(N)$-smooth number

$\tilde{q} \le R$ the finite sequence $(g(\tilde{q}n)\Gamma)_{n\in[N'/\tilde{q}]}$ is δ-equidistributed in G/Γ. The parameter δ satisfies the condition $\delta^{-t} \ll_t N'$, which will allow us later to apply Proposition 15.4. We are required to show that for every Lipschitz function $F : G/\Gamma \to \mathbb{R}$ satisfying $\int_{G/\Gamma} F = 0$, for every $w(N)$-smooth number $q \ll N^{o(1)}$, and for every $r \in [q]$, we have

$$|\mathbb{E}_{n\in[N'/q]}(r'_{f,\beta}(qn+r)-1)F(g(n)\Gamma)| \ll \delta^{1/O_{m,d}(1)}\|F\|.$$

By δ-equidistribution of $(g(n)\Gamma)_{n\in[N]}$ and since $\int F = 0$, it suffices to show that

$$|\mathbb{E}_{n\in[N'/q]}r'_{f,\beta}(qn+r)F(g(n)\Gamma)| \ll \delta^{1/O_{m,d}(1)}\|F\|.$$

We may suppose that $f = \langle a,b,c\rangle$ has reduced form, that is, $|b| \le a \le c$. Write $X(f,N) := \{(x,y) : f(x,y) \le N\}$; our aim is to decompose the binary sequence

$$\{g((ax^2+bxy+cy^2)\Gamma)\}_{(x,y)\in X(f,N)}$$

into a sum of polynomial subsequences $(g'(P(n)\Gamma))_{n\le(N')^{1/\deg(P)}}$ of some equidistributed sequence $(g'(n)\Gamma)_{n\le N'}$. In order to do so, let $(x_0,y_0) \in \mathbb{R}^2$ be the point on the ellipse $f(x,y) = ax^2+bxy+cy^2 = N$ that satisfies $x_0 = y_0 \sim N^{1/2}$. Since f has reduced form, we have both $ax_0^2 \le N$ and $cy_0^2 \le N$. With respect to (x_0,y_0), the summation over $(x,y) \in X(f,N)$ now splits into three parts (cf. Figure 1) such that on each part one of the variables x and y may be fixed, while the free variable will range over an interval of length at least $x_0 \sim N^{1/2}$. This decomposition yields

$$\begin{aligned}(18.1)\qquad &\frac{2\pi}{\sqrt{-D}}\Big|\sum_{n\le(N'-r)/q} r'_{f,\beta}(qn+r)F(g(n)\Gamma)\Big|\\ &\le \bigg(\frac{\rho_{f,\beta}(\overline{W})}{\overline{W}}\bigg)^{-1}\\ &\quad\times\bigg\{\sum_{y\le y_0}\Big|\sum_{x:f(x,y)\le N} 1_{f(x,y)\equiv\overline{W}r+\beta \pmod{\overline{W}q}}F\bigg(g\bigg(\frac{f(x,y)-\beta-\overline{W}r}{\overline{W}q}\bigg)\Gamma\bigg)\Big|\\ &\quad+\sum_{x\le x_0}\Big|\sum_{y:\,f(x,y)\le N} 1_{f(x,y)\equiv\overline{W}r+\beta \pmod{\overline{W}q}}F\bigg(g\bigg(\frac{f(x,y)-\beta-\overline{W}r}{\overline{W}q}\bigg)\Gamma\bigg)\Big|\\ &\quad+\sum_{y\le y_0}\Big|\sum_{x\le x_0} 1_{f(x,y)\equiv\overline{W}r+\beta \pmod{\overline{W}q}}F\bigg(g\bigg(\frac{f(x,y)-\beta-\overline{W}r}{\overline{W}q}\bigg)\Gamma\bigg)\Big|\bigg\}.\end{aligned}$$

To remove the congruence condition $f(x,y) \equiv \overline{W}r+\beta \pmod{\overline{W}q}$ in this explicit form, we consider the set $S(q\overline{W}, \overline{W}r+\beta)$ of all solutions $(x',y') \in [q\overline{W}]^2$ to the congruence $f(x',y') \equiv \overline{W}r+\beta \pmod{q\overline{W}}$. By Corollary 6.4 the density of these solutions for a $w(N)$-smooth integer q, any $r \in [q]$ and

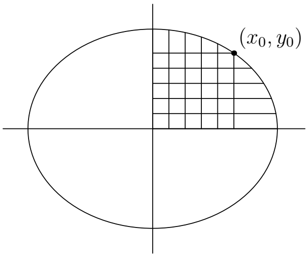

Fig. 1. Scheme of how the summation is split: we sum along horizontal lines (y fixed), along vertical lines (x fixed), and another time over the segments of the horizontal lines that are contained in the 'box', that is, over the double-counted segments.

$\beta \in \mathcal{A}$ satisfies

$$\frac{\rho_{f,\overline{W}r+\beta}(q\overline{W})}{q\overline{W}} = \frac{\rho_{f,\beta}(\overline{W})}{\overline{W}}.$$

To simplify the notation, define $\beta' := \overline{W}r + \beta$ and $q' := \overline{W}q$. Considering any of the three parts of our summation above, we may continue this as follows:

$$\begin{aligned}&\left(\frac{\rho_{f,\beta}(\overline{W})}{\overline{W}}\right)^{-1} \sum_{y \le y_0} \Bigg| \sum_{x\colon f(x,y) \le N} 1_{f(x,y) \equiv \beta' \,(\mathrm{mod}\, q')} F\bigg(g\Big(\frac{f(x,y)-\beta'}{q'}\Big)\Gamma\bigg)\Bigg| \\ &\quad = q\overline{W}\ \mathbb{E}_{(x',y') \in S(q',\beta')} \\ &\qquad \sum_{y\colon q'y+y' \le y_0} \Bigg| \sum_{\substack{x\colon f(q'x+x',q'y+y') \\ \le N}} F\bigg(g\Big(\frac{f(q'x+x',q'y+y')-\beta'}{q'}\Big)\Gamma\bigg)\Bigg|.\end{aligned}$$

Observe that

$$\frac{f(\overline{W}qx+x',\overline{W}qy+y') - \overline{W}r - \beta}{q\overline{W}} = \overline{W}qax^2 + b'x + c',$$

for some b', c' depending on y, y', x', b, c, q and $\overline{W}$, is a polynomial that satisfies the conditions of Proposition 15.4. Thus, setting $P(x) := \overline{W}qax^2 + b'x + c'$, we are considering the polynomial subsequence $(g \circ P(n)\Gamma)_{n \le (N'/qq')^{1/2}}$ of $(g(n)\Gamma)_{n \le N'/q}$. By Proposition 15.4 there is for each P a $w(N)$-smooth integer $\tilde{q} \ll N^{o(1)}$ such that for every $\tilde{r} \in [\tilde{q}]$ the sequence

$$g(P(\tilde{q}x + \tilde{r}))_{x \le N^{1/2}/(\overline{W}q\tilde{q})}$$

is totally $\delta^{1/O_d(1)}$-equidistributed. Splitting the summation into subprogressions modulo $\tilde{q}$, we have via the triangle inequality

$$\begin{aligned}
&q\overline{W}\,\mathbb{E}_{(x',y')\in S(q',\beta')} \sum_{y\colon q'y+y'\le y_0} \Big| \sum_{\substack{x\colon f(q'x+x',q'y+y')\\ \le N}} F(g\circ P(x)\Gamma)\Big| \\
&\le q\overline{W}\,\mathbb{E}_{(x',y')\in S(q',\beta')} \sum_{y\colon q'y+y'\le y_0} \sum_{\tilde{r}} \Big| \sum_{\substack{x\colon f(q'(\tilde{q}x+\tilde{r})+x',q'y+y')\\ \le N}} F(g\circ P(\tilde{q}x+\tilde{r})\Gamma)\Big| \\
&\ll q\overline{W}\,\mathbb{E}_{(x',y')\in S(q',\beta')} \sum_{y\colon q'y+y'\le y_0} \tilde{q}\,\frac{N^{1/2}}{\overline{W}q\tilde{q}}\delta^{1/O_d(1)}\|F\|_{\mathrm{Lip}} \\
&\ll \delta^{1/O_d(1)}\,\frac{N'}{q}\|F\|_{\mathrm{Lip}}.
\end{aligned}$$

As these arguments also apply to the remaining two parts of the sum (18.1), this completes the proof of Proposition 17.2 and also the proof of the main theorem.

Acknowledgements. I should like to thank my PhD supervisor Ben Green for suggesting the problems studied in this paper and for many valuable discussions and advice. I am also very grateful to Tim Browning for insightful comments and suggestions, and to Tom Sanders for helpful conversations.

While working on this paper the author was supported by an EPSRC studentship and a studentship from Trinity College, Cambridge.

References

[1] R. de la Bretèche and T. D. Browning, *Binary linear forms as sums of two squares*, Compos. Math. 144 (2008), 1375–1402.

[2] T. D. Browning and R. Munshi, *Rational points on singular intersections of quadrics*, arXiv:1108.1902.

[3] R. J. Cook, *Simultaneous quadratic equations*, J. London Math. Soc. 4 (1971), 319–326.

[4] D. A. Cox, *Primes of the Form x^2+ny^2*, Pure Appl. Math., Wiley, 1989.

[5] P. Erdős, *On the sum $\sum_{k=1}^{x} d(f(k))$*, J. London Math. Soc. 27 (1952), 7–15.

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

[7] B. J. Green and T. C. Tao, *Quadratic uniformity of the Möbius function*, Ann. Inst. Fourier (Grenoble) 58 (2008), 1863–1935.

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

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

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

[11] B. J. Green, T. C. Tao and T. Ziegler, *An inverse theorem for the Gowers $U^k[N]$ norm*, arXiv:1009.3998v2.

[12] 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.

[13] K. Henriot, *Nair–Tenenbaum bounds uniform with respect to the discriminant*, Math. Proc. Cambridge Philos. Soc. 152 (2012), 405–424.

[14] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.

[15] H. Iwaniec, *The half dimensional sieve*, Acta Arith. 29 (1976), 69–95.

[16] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[17] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. 13 (1908), 305–312.

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

[19] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I, Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge Univ. Press, 2006.

[20] K. Prachar, *Über Zahlen der Form $a^2 + b^2$ in einer arithmetischen Progression*, Math. Nachr. 10 (1953), 51–54.

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

[22] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. 4 (1991), 793–835.

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

Received on 23.6.2011
and in revised form on 1.1.2012 (6741)