EFFICIENT CONGRUENCING IN $\mathbb{Z}[t]$ MODULO t^2

TREVOR D. WOOLEY

Abstract. We develop an analogue of nested efficient congruencing applicable in the ring $\mathbb{Z}[t]/t^2\mathbb{Z}[t]$ so as to estimate mean values related to that of Vinogradov. Let k be a natural number, and suppose that $\varphi_j(u) \in \mathbb{Z}[t,u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials having Wronskian $W(u;\boldsymbol{\varphi}) = \det(\mathrm{d}^i\varphi_j(u)/\mathrm{d}u^i)_{1\leqslant i,j\leqslant k}$ with respect to u. Consider the number $\Upsilon_{s,k}(X;\boldsymbol{\varphi})$ of integral solutions of the system of equations

$$\sum_{i=1}^{s}\big(\varphi_j(u_i+v_it)-\varphi_j(u_{s+i}+v_{s+i}t)\big) \equiv 0 \ (\mathrm{mod}\ t^2) \quad (1 \leqslant j \leqslant k),$$

with $|u_i| \leqslant X$ and $|v_i| \leqslant X$ $(1 \leqslant i \leqslant s)$. We show that when $W(u;\boldsymbol{\varphi}) \not\equiv 0 \ (\mathrm{mod}\ t)$ and $1 \leqslant s \leqslant k(k+1)/2$, then $\Upsilon_{s,k}(X;\boldsymbol{\varphi}) \ll X^{2s+\varepsilon}$. Our conclusions extend to number fields and function fields, as we outline. We describe several consequences of our results, including forthcoming work establishing the main conjecture for certain systems of equations not possessing translation-dilation invariant properties.

1. Introduction

Our purpose in this memoir is to initiate the quantitative theory of congruences over $\mathbb{Z}[t]$ as they relate to relatives of Vinogradov's mean value theorem. In order to illustrate what we have in mind, consider a natural number k and polynomials $\varphi_j(u) \in \mathbb{Z}[t,u]$ $(1 \leqslant j \leqslant k)$. For the sake of expositional concision here, we have suppressed the dependence on t in our notation for the polynomials $\varphi_j(u)$. Our focus lies on the system of congruences

$$\sum_{i=1}^{s}\big(\varphi_j(x_i)-\varphi_j(x_{s+i})\big) \equiv 0 \ (\mathrm{mod}\ t^2) \quad (1 \leqslant j \leqslant k), \tag{1.1}$$

in which $s \in \mathbb{N}$, and for $1 \leqslant i \leqslant 2s$ the variables x_i lie in $\mathbb{Z}[t]$. There is no loss of generality here, of course, in supposing that $x_i = u_i + v_it$ for some $u_i, v_i \in \mathbb{Z}$ $(1 \leqslant i \leqslant 2s)$. Our goal will be to obtain estimates for the number $\Upsilon_{s,k}(X;\boldsymbol{\varphi})$ of solutions of the system (1.1) with $|u_i| \leqslant X$ and $|v_i| \leqslant X$ $(1 \leqslant i \leqslant 2s)$. There is nothing particularly significant about the modulus t^2 chosen in (1.1), aside from the simplicity of exposition. However, as we explain elsewhere [12, 13], it transpires that the estimates that we are able to obtain herein may be employed to obtain essentially optimal upper bounds for mean values associated with certain systems of equations failing to exhibit translation-dilation invariance. Since the latter systems are not accessible to techniques based on either decoupling or efficient congruencing methods, the circle of ideas presented here and in [12, 13] have the merit of permitting precise investigation of problems hitherto inaccessible.

In order to announce the main conclusions of this memoir, we must record some additional notation. We consider polynomials φ_j as introduced above, and we define the

2020 *Mathematics Subject Classification.* 11L15, 11L07, 11P55.

Key words and phrases. Exponential sums, Hardy-Littlewood method, congruences.

Wronskian of derivatives

$$W(u;\boldsymbol{\varphi}) = \det\big(\varphi_j^{(i)}(u)\big)_{1\leqslant i,j\leqslant k}, \tag{1.2}$$

in which we write $\varphi_j^{(r)}(u)$ for the r-th derivative $\mathrm{d}^r\varphi_j(u)/\mathrm{d}u^r$. The system of polynomials $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_k)$ may be considered independent modulo t when $W(u;\boldsymbol{\varphi}) \not\equiv 0 \pmod t$. We recall that the counting function $\Upsilon_{s,k}(X;\boldsymbol{\varphi})$ associated with the system of equations (1.1) counts the number of integral solutions of the system of congruences

$$\sum_{i=1}^{s}\big(\varphi_j(u_i + v_it) - \varphi_j(u_{s+i} + v_{s+i}t)\big) \equiv 0 \pmod{t^2} \quad (1 \leqslant j \leqslant k), \tag{1.3}$$

with $|u_i| \leqslant X$ and $|v_i| \leqslant X$ $(1 \leqslant i \leqslant 2s)$.

Theorem 1.1. *Suppose that $\varphi_j(u) \in \mathbb{Z}[t,u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u;\boldsymbol{\varphi}) \not\equiv 0 \pmod t$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, one has*

$$\Upsilon_{s,k}(X;\boldsymbol{\varphi}) \ll X^{2s+\varepsilon}. \tag{1.4}$$

Here and elsewhere, unless indicated otherwise, the implicit constants in Vinogradov's notation $\ll$ and $\gg$ depend at most on ε, s, k and the coefficients of $\boldsymbol{\varphi}$. We note that the number of available choices for the variables $\mathbf{u}$ and $\mathbf{v}$ is essentially $(2X+1)^{4s}$, so the conclusion of Theorem 1.1 achieves an upper bound of size roughly equal to the square-root of this trivial estimate when $s \leqslant k(k+1)/2$.

We illuminate the conclusion of Theorem 1.1 by highlighting a number of special cases as corollaries. We first distinguish the special case in which the polynomials $\varphi_j(u)$ are independent of t. In this scenario, it is convenient to define $\Upsilon^*_{s,k}(X;\boldsymbol{\varphi})$ to be the number of integral solutions of the Diophantine system

$$\left.\begin{aligned} \sum_{i=1}^{s}\big(\varphi_j(u_i) - \varphi_j(u_{s+i})\big) &= 0 \\ \sum_{i=1}^{s}\big(v_i\varphi_j'(u_i) - v_{s+i}\varphi_j'(u_{s+i}) &= 0 \end{aligned}\right\} (1 \leqslant j \leqslant k), \tag{1.5}$$

with $|u_i| \leqslant X$ and $|v_i| \leqslant X$ $(1 \leqslant i \leqslant 2s)$.

Corollary 1.2. *Suppose that $\varphi_j \in \mathbb{Z}[u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u;\boldsymbol{\varphi}) \neq 0$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, one has $\Upsilon^*_{s,k}(X;\boldsymbol{\varphi}) \ll X^{2s+\varepsilon}$.*

In order to confirm that Corollary 1.2 follows from Theorem 1.1, one has only to observe that since φ_j is independent of t for $1 \leqslant j \leqslant k$, one has

$$\varphi_j(u+vt) \equiv \varphi_j(u) + v\varphi_j'(u)t \pmod{t^2}.$$

By equating coefficients of 1 and t, we consequently see that the systems (1.3) and (1.5) are equivalent, whence $\Upsilon_{s,k}(X;\boldsymbol{\varphi}) = \Upsilon^*_{s,k}(X;\boldsymbol{\varphi})$.

By orthogonality, the conclusion of Corollary 1.2 delivers upper bounds for mean values of exponential sums. As usual, we write $e(z)$ for $\mathrm{e}^{2\pi\mathrm{i}z}$. Then, given k-tuples $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, we

put

$$\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta})=\sum_{j=1}^{k}\big(\alpha_j\varphi_j(u)+\beta_jv\varphi_j'(u)\big),$$

and define

$$F_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)=\sum_{|u|\leqslant X}\sum_{|v|\leqslant X}e(\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta})).$$

Thus, we see that under the hypotheses of Corollary 1.2, one has

$$\int_{[0,1)^k}\int_{[0,1)^k}|F_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta}\ll X^{2s+\varepsilon}. \tag{1.6}$$

A further specialisation yields a concrete example more readily appreciated. We put $\varphi_j(u)=u^{d_j}$ $(1\leqslant j\leqslant k)$, and observe that $W(u;\boldsymbol{\varphi})\neq 0$ whenever $1\leqslant d_1<d_2<\ldots<d_k$. We now take $\Upsilon_{s,k}^{+}(X;\mathbf{d})$ to be the number of integral solutions of the system of equations

$$\left.\begin{aligned}\sum_{i=1}^{s}(u_i^{d_j}-u_{s+i}^{d_j})&=0\\ \sum_{i=1}^{s}(v_iu_i^{d_j-1}-v_{s+i}u_{s+i}^{d_j-1})&=0\end{aligned}\right\}(1\leqslant j\leqslant k), \tag{1.7}$$

with $|u_i|\leqslant X$ and $|v_i|\leqslant X$ $(1\leqslant i\leqslant 2s)$.

Corollary 1.3. *Let $d_1,\ldots,d_k$ be distinct positive integers, and let s be a positive integer with $s\leqslant k(k+1)/2$. Then for each $\varepsilon>0$, one has $\Upsilon_{s,k}^{+}(X;\mathbf{d})\ll X^{2s+\varepsilon}$.*

Finally, we specialise further to the case that $d_j=j$ $(1\leqslant j\leqslant k)$. This special case is an extension of Vinogradov's mean value theorem that deserves special attention. We denote by $J_{s,k}^{*}(X)$ the number of integral solutions of the system

$$\left.\begin{aligned}\sum_{i=1}^{s}(u_i^{j}-u_{s+i}^{j})&=0\\ \sum_{i=1}^{s}(v_iu_i^{j-1}-v_{s+i}u_{s+i}^{j-1})&=0\end{aligned}\right\}(1\leqslant j\leqslant k), \tag{1.8}$$

with $|u_i|\leqslant X$ and $|v_i|\leqslant X$ $(1\leqslant i\leqslant 2s)$. The quantity $J_{s,k}^{*}(X)$ counts the number of solutions of the Vinogradov system

$$\sum_{i=1}^{s}\big((u_i+v_it)^j-(u_{s+i}+v_{s+i}t)^j\big)\equiv 0\ (\mathrm{mod}\ t^2)\quad(1\leqslant j\leqslant k),$$

with $|u_i|\leqslant X$ and $|v_i|\leqslant X$ $(1\leqslant i\leqslant 2s)$. A consequence of Corollary 1.3 is the upper bound supplied in our final corollary.

Corollary 1.4. *Let s be a positive integer. Then for each $\varepsilon>0$, one has*

$$J_{s,k}^{*}(X)\ll X^{\varepsilon}(X^{2s}+X^{4s-k(k+1)}).$$

This corollary is sharp up to the factor of X^{ε}. On one hand, a consideration of those diagonal solutions of (1.8) with

$$\{u_1+v_1t,\dots,u_s+v_st\}=\{u_{s+1}+v_{s+1}t,\dots,u_{2s}+v_{2s}t\} \tag{1.9}$$

reveals that $J^*_{s,k}(X)\gg X^{2s}$ for $s\in\mathbb{N}$. Meanwhile, a crude major arc estimation of standard type reveals that

$$J^*_{s,k}(X)\gg X^{4s-k(k+1)}.$$

The significance of the exponent $k(k+1)$ is, of course, that it is equal to the sum of the degrees of the polynomials defining the system of equations (1.8). We note that the conclusion of Corollary 1.4 is made available, in all essentials, by [5, Theorem 1.1]. The statement of the latter result is sufficiently heavy in notation that the reader will likely require some measure of determination to find the desired conclusion, although the reader will find [5, Example 1.4] very helpful. This work of Guo and Zorin-Kranich improves on earlier work of Parsell, Prendiville and Wooley [6] that applies to quite general translation-dilation invariant systems of higher dimension (see also [1, 4]).

A key feature of the system (1.8) is that it is fully translation-dilation invariant. Thus, whenever $(u_i,v_i)_{1\leqslant i\leqslant 2s}$ gives a solution of the system (1.8), then for any integers a and b, the tuple $(u_i+a,v_i+b)_{1\leqslant i\leqslant 2s}$ also provides a solution of the system (1.8). This feature is critical for the decoupling approach to bounding $J^*_{s,k}(X)$ in [5], as well as the efficient congruencing approach of [6]. The approach of this paper implicitly makes use of the observation that the system (1.5) is approximated by the system (1.8), so that translation-dilation invariance also plays a critical role in our present treatment. This translation-dilation invariance property, however, creates difficulties for us, in that additional special subvarieties are present in the solution set of the system (1.8) possessing a significant number of solutions. Thus, while the aforementioned diagonal solutions (1.9) contribute roughly $s!(2X+1)^{2s}$ solutions to the total counted by $J^*_{s,k}(X)$, there are additional solutions making a contribution of the same order of magnitude. Indeed, the solutions of (1.8) with

$$u_1=u_2=\ldots=u_{2s}\quad\text{and}\quad v_1+\ldots+v_s=v_{s+1}+\ldots+v_{2s}$$

contribute $\gg X\cdot X^{2s-1}=X^{2s}$ solutions to $J^*_{s,k}(X)$. We shall return to this observation when conditioning variables in §6.

Our approach to proving Theorem 1.1 is not merely some kind of efficient congruencing analogue of the decoupling method of [5]. The latter approach must accommodate the bivariate nature, involving u_i and v_i, of the underlying monomials of the system (1.8). Instead, we apply an efficient congruencing approach making intrinsic use of the arithmetic of $\mathbb{Z}[t]/t^2\mathbb{Z}[t]$, working in the univariate system (1.1). This approach is flexible, permitting various generalisations beyond the test case examined in this memoir. We are confident that variants of our methods should apply to systems analogous to (1.1) in which the single variable polynomials $\varphi_j(x)$ are replaced by many variable variants, with x_i a polynomial in t of higher degree, and with the modulus t^2 replaced by a higher degree polynomial. We regard the present memoir as a proof-of-concept excursion on the theme.

A second important feature of the efficient congruencing approach, as opposed to real decoupling approaches, is that it is applicable in number fields, function fields, and indeed other settings in which one studies discrete sets of points in valued fields. We briefly sketch

out both kinds of conclusions, and the ideas necessary for proofs, in §§11 and 12, handling number field analogues in §11 and function field analogues in §12.

Before preparations begin for our proof of Theorem 1.1, we pause to announce the main conclusion of a second memoir [12] that makes critical use of Corollary 1.4. This concerns the number $I_{s,k}(X)$ of integral solutions of the system of equations

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \quad (2 \leqslant j \leqslant k), \tag{1.10}$$

with $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant s)$.

Theorem 1.5. *When k and s are natural numbers with $k \geqslant 2$, and $\varepsilon > 0$, one has*

$$I_{s,k}(X) \ll X^{s+\varepsilon} + X^{2s-(k^2+k-2)/2}.$$

Thus, whenever s and ε are positive numbers, one has

$$\int_{[0,1)^{k-1}} \left| \sum_{1 \leqslant x \leqslant X} e(\alpha_2 x^2 + \ldots + \alpha_k x^k) \right|^{2s} \mathrm{d}\boldsymbol{\alpha} \ll X^{s+\varepsilon} + X^{2s-(k^2+k-2)/2}.$$

The conclusion of this theorem may be compared with a general consequence [11, Corollary 1.2 and Theorem 14.1] of efficient congruencing, which would achieve the same bound in the ranges $1 \leqslant s \leqslant k(k-1)/2$ and $s \geqslant k(k+1)/2$, and [3, Theorem 1.1], which enhances the former range to $1 \leqslant s \leqslant (k^2-1)/2$. Since elementary arguments yield the lower bound

$$I_{s,k}(X) \gg X^s + X^{2s-(k^2+k-2)/2},$$

it is evident that our upper bounds achieve the main conjecture associated with these mean value estimates. We stress that the system (1.10) is not translation-dilation invariant, and that, aside from the special case $k = 2$ of the theorem, this is the first instance in which the main conjecture has been established for an incomplete Vinogradov system.

This memoir is organised as follows. We discuss Fourier analysis relevant to our work in $\mathbb{Z}[t]/t^r\mathbb{Z}[t]$ in §2. This prepares the way for our detailed account of the proof of Theorem 3.3 in §§3-9, which provides the basic nested inductive step in the argument. The key infrastructure is described in §3, with implications for translation-dilation invariant families in §4. The nested structure is inductively built, with the case $k = 1$ as the base of the induction. We discuss this base case in §5. The general situation with $k \geqslant 2$ is analysed in §§6-9, with an initial conditioning step in §6, the extraction of strong congruence constraints in §7, and iterative procedures in §8. The proof of the key Theorem 3.3 is then concluded in §9. We advance in §10 to derive consequences of Theorem 3.3 for mean values and equations. This work provides the conclusion embodied in Theorem 1.1 and its corollaries. In §11 we describe how to adapt our basic methods so as to derive conclusions analogous to Theorem 1.1 for number fields, and in §12 we provide a similar discussion for function fields. Finally, in §13, we provide an appendix demonstrating how rather more general bivariate translation-dilation invariant systems may be interpreted in the framework provided by congruences over $\mathbb{Z}[t]$.

Some notational conventions will streamline our exposition. Throughout, we make liberal use of vector notation in settings not always conventional in nature. Thus, for example, we may write $1 \leqslant \mathbf{x} \leqslant X$ to denote that every coordinate x_i of $\mathbf{x}$ satisfies

$1 \leqslant x_i \leqslant X$, and $\mathbf{x} \equiv \xi \pmod{p^h}$ to denote that $x_i \equiv \xi \pmod{p^h}$ for all indices i. Also, we adopt the convention that when $F : [0,1)^n \to \mathbb{C}$ is integrable, then

$$\oint F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = \int_{[0,1)^n} F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}.$$

Finally, given a situation in which the parameter ε has not already been fixed, in any statement involving the letter ε, it is implicitly asserted that the statement holds for each $\varepsilon > 0$. In such circumstances, implicit constants in Vinogradov's notation $\ll$ and $\gg$ may depend on ε.

Work on this paper was conducted while the author was supported by NSF grants DMS-2001549 and DMS-2502625, and by Simons Fellowship in Mathematics SFM-00011955. The author is grateful to the Institute for Advanced Study, Princeton, for hosting his sabbatical, during which period this paper was completed.

2. Fourier analysis in $\mathbb{Z}[t]/t^r\mathbb{Z}[t]$

A feature of the work presented in this memoir is that we require the use of Fourier analysis applicable in the setting of $\mathbb{Z}[t]/t^2\mathbb{Z}[t]$. The basic foundations of this Fourier analysis are simple to formulate in the more general setting $\mathbb{Z}[t]/t^r\mathbb{Z}[t]$, with r any fixed natural number. We discuss such matters in this section, though in the remainder of this memoir we restrict attention to the case $r = 2$. Workers familiar with the application of the circle method in $\mathbb{F}_q[t]$ will experience no difficulty in deriving for themselves the necessary infrastructure for such endeavours. It is surely of assistance to the reader, however, to expend a modicum of effort reviewing such ideas in order to fix notation.

We shall be counting solutions of equations defined over $\mathbb{Z}[t]/t^r\mathbb{Z}[t]$, a ring that we abbreviate to $\mathfrak{Z}(t^r)$. A typical element of this ring $\mathfrak{Z}(t^r)$ takes the form

$$n_0 + n_1 t + \ldots + n_{r-1}t^{r-1},$$

where $n_i \in \mathbb{Z}$ $(0 \leqslant i < r)$. With the possibility of confusion an omnipresent hazard, we shall write such a polynomial as n, relying on context to disambiguate this polynomial from a natural number. The need for myriad items of notation forces such expedience upon us.

As usual, we write $e(z)$ for $\mathrm{e}^{2\pi \mathrm{i} z}$ when $z \in \mathbb{R}$, noting the familiar relation

$$\int_0^1 e(h\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } h = 0, \\ 0, & \text{when } h \in \mathbb{Z} \setminus \{0\}, \end{cases}$$

that forms the foundation of Fourier analysis. This orthogonality relation detects vanishing in $\mathbb{Z}$. An analogous relation appropriate for $\mathfrak{Z}(t^r)$ makes use of the set

$$\mathfrak{T}(t^r) = \Big\{ \frac{\alpha_1}{t} + \frac{\alpha_2}{t^2} + \ldots + \frac{\alpha_r}{t^r} : (\alpha_1, \ldots, \alpha_r) \in [0,1)^r \Big\}.$$

The set $\mathfrak{T}(t^r)$ forms a subset of the field of formal Laurent series

$$\mathbb{R}((1/t)) = \Big\{ \sum_{m > -\infty} \frac{\alpha_m}{t^m} : \alpha_m \in \mathbb{R} \text{ for } m \in \mathbb{Z} \Big\}.$$

When $\xi \in \mathbb{R}((1/t))$, we define the *residue* of ξ, written $\mathrm{res}(\xi)$, to be the coefficient ξ_1 of $1/t$ in the Laurent series expansion of ξ. We then define the exponential function $E : \mathbb{R}((1/t)) \to \mathbb{C}$ by putting

$$E(\xi) = e(\mathrm{res}(\xi)).$$

Thus, when

$$n = n_0 + n_1 t + \ldots + n_{r-1}t^{r-1} \in \mathfrak{Z}(t^r) \quad \text{and} \quad \alpha = \frac{\alpha_1}{t} + \frac{\alpha_2}{t^2} + \ldots + \frac{\alpha_r}{t^r} \in \mathfrak{T}(t^r),$$

one finds that

$$\mathrm{res}(n\alpha) = n_0\alpha_1 + n_1\alpha_2 + \ldots + n_{r-1}\alpha_r,$$

and hence

$$\int_0^1 \ldots \int_0^1 E(n\alpha)\,\mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_r = \begin{cases} 1, & \text{when } n_i = 0 \ (0 \leqslant i < r), \\ 0, & \text{otherwise.} \end{cases}$$

By adopting the convention that for integrable functions $F : \mathfrak{T}(t^r) \to \mathbb{C}$, we write

$$\int_{\mathfrak{T}(t^r)} F(\alpha)\,\mathrm{d}\alpha = \int_0^1 \ldots \int_0^1 F\Big(\frac{\alpha_1}{t} + \ldots + \frac{\alpha_r}{t^r}\Big)\,\mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_r,$$

we find that

$$\int_{\mathfrak{T}(t^r)} E(n\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } n = 0, \\ 0, & \text{when } n \in \mathfrak{Z}(t^r) \setminus \{0\}. \end{cases}$$

This discussion generalises at once to consider orthogonality in the ring $\mathbb{Z}[t]$ modulo t^r. By this we mean that when $m \in \mathbb{Z}[t]$ is a polynomial having degree R, in which R might conceivably be larger than $r-1$, then a moment's reflection reveals that one has

$$\int_{\mathfrak{T}(t^r)} E(m\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } m \equiv 0 \pmod{t^r}, \\ 0, & \text{when } m \not\equiv 0 \pmod{t^r}. \end{cases} \tag{2.1}$$

Now consider a prime number p and a positive integer b. We write (p^b, t^r) for the ideal of $\mathbb{Z}[t]$ generated by p^b and t^r. In order to avoid ambiguity with the superficial appearance of a numerical value of a greatest common divisor, we note that, in concrete terms, one of course has

$$(p^b, t^r) = \{zp^b + wt^r : z, w \in \mathbb{Z}\}.$$

Much of our discussion will occur in the module

$$\mathbb{Z}[t]/(p^b, t^r) \cong (\mathbb{Z}/p^b\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/p^b\mathbb{Z}),$$

with basis elements $1, t, \ldots, t^{r-1}$. When $u \in \mathbb{Z}$ and $q \in \mathbb{N}$, write $e_q(u) = e(u/q)$. Then a little thought reveals that arguments very similar to those above lead from the fundamental orthogonality relation

$$\frac{1}{p^b}\sum_{a=1}^{p^b} e_{p^b}(ua) = \begin{cases} 1, & \text{when } u \equiv 0 \pmod{p^b}, \\ 0, & \text{when } u \not\equiv 0 \pmod{p^b}, \end{cases}$$

to an orthogonality relation relevant for polynomials $m \in \mathbb{Z}[t]$, namely

$$\frac{1}{p^{rb}} \sum_{a_1=1}^{p^b} \dots \sum_{a_r=1}^{p^b} e_{p^b}\Big(\operatorname{res}\Big(m\Big(\frac{a_1}{t} + \dots + \frac{a_r}{t^r}\Big)\Big)\Big) = \begin{cases} 1, & \text{when } m \equiv 0 \pmod{(p^b, t^r)}, \\ 0, & \text{when } m \not\equiv 0 \pmod{(p^b, t^r)}. \end{cases} \tag{2.2}$$

We seek to think of the relation (2.2) as an orthogonality relation streamlined as in (2.1). Thus, we adopt the convention that given $F : \mathfrak{T}(t^r) \to \mathbb{C}$, we write

$$\oint_{p^b} F(\alpha^{(r)})\, \mathrm{d}\alpha^{(r)} = \frac{1}{p^{rb}} \sum_{a_1=1}^{p^b} \dots \sum_{a_r=1}^{p^b} F\Big(\frac{1}{p^b}\Big(\frac{a_1}{t} + \dots + \frac{a_r}{t^r}\Big)\Big).$$

We then have

$$\oint_{p^b} E(m\alpha^{(r)})\, \mathrm{d}\alpha^{(r)} = \begin{cases} 1, & \text{when } m \equiv 0 \pmod{(p^b, t^r)}, \\ 0, & \text{when } m \not\equiv 0 \pmod{(p^b, t^r)}. \end{cases} \tag{2.3}$$

In circumstances in which confusion is easily avoided, it may be expedient to suppress mention of the superscript (r) associated with the implicit modulus t^r from this notation. Indeed, for the remainder of this memoir, we shall take $r = 2$ and drop mention of this index from our notation.

3. The apparatus for nested efficient congruencing

Before embarking on details of the nested efficient congruencing argument, we first assemble the apparatus required for our proof of Theorem 1.1. This is inspired by our previous work on efficient congruencing and its nested variant (see, for example, [7, 9, 11]). A number of modifications are necessary to accommodate the present application, so we will provide a complete account rather than cut corners in our exposition.

Let k be an integer, and consider polynomials $\varphi_1(u), \dots, \varphi_k(u) \in \mathbb{Z}[t, u]$. We fix a prime number p with $p > k$, and a large positive integer B. As in the discussion of [11], we require these polynomials $\varphi_j(u)$ to be sufficiently independent of one another for $1 \leqslant j \leqslant k$. Thus, we impose the condition that the system of polynomials $\boldsymbol{\varphi}$ is *p^c-spaced* for an appropriate positive integer c, in the sense that

$$\varphi_j(u) \equiv u^j \pmod{(p^c, t)} \quad (1 \leqslant j \leqslant k). \tag{3.1}$$

It follows that, given a p^c-spaced system of polynomials $\boldsymbol{\varphi}$, the Wronskian $W(u; \boldsymbol{\varphi})$, defined via (1.2), is non-zero modulo t. Indeed, one has

$$W(u; \boldsymbol{\varphi}) \equiv \prod_{j=1}^{k} j! \not\equiv 0 \pmod{(p, t)}.$$

We next define the exponential sums and mean values that feature prominently in our discussion. We consider bounded complex weights $\mathfrak{a}_n$ with $n \in \mathfrak{Z}(t^2)$. When $q \in (0, \infty)$, we define the norms

$$\|\mathfrak{a}\|_q = \lim_{T \to \infty} \Big(\sum_{|n_0| \leqslant T} \sum_{|n_1| \leqslant T} |\mathfrak{a}_{n_0 + n_1 t}|^q \Big)^{1/q}.$$

We extend this definition in the conventional manner by putting

$$\|\mathfrak{a}\|_0 = \lim_{q\to 0+} \|\mathfrak{a}\|_q \quad \text{and} \quad \|\mathfrak{a}\|_\infty = \lim_{q\to\infty} \|\mathfrak{a}\|_q = \sup_{n\in\mathfrak{Z}(t^2)} |\mathfrak{a}_n|.$$

We shall restrict attention to complex weights $\mathfrak{a}_n$ with $\|\mathfrak{a}\|_0 < \infty$. We note for future reference that we have in mind the situation in which the weights $\mathfrak{a}_n$ are supported only for $n = n_0 + n_1 t$, with $|n_0| \leqslant N$ and $|n_1| \leqslant N$, with roughly equal weight attached to each $n \in \mathfrak{Z}(t^2)$ thus prescribed. Next, when h is a non-negative integer and $\xi \in \mathfrak{Z}(t^2)$, we introduce the subsequence of weights

$$\mathfrak{a}_h(\xi) = \big(\mathfrak{a}_n : n \equiv \xi \pmod{(p^h, t^2)}\big),$$

and then define the normalising weights $\rho_h(\xi) = \rho_h(\xi; \mathfrak{a})$ by putting

$$\rho_h(\xi; \mathfrak{a}) = \|\mathfrak{a}_h(\xi)\|_0^{1/2} \cdot \|\mathfrak{a}_h(\xi)\|_\infty. \tag{3.2}$$

It is convenient to associate the restricted subsequence of weights $\mathfrak{b}$ to $\mathfrak{a}_h(\xi)$ by putting

$$\mathfrak{b}_n = \mathfrak{a}_{p^h n+\xi} \quad (n \in \mathfrak{Z}(t^2)).$$

Temporarily, fix a choice of $\xi \in \mathfrak{Z}(t^2)$. Then we note that, in the scenario outlined above, there are roughly $(2N+1)^2$ non-zero values of $\mathfrak{a}_n$ each of size approximately $\|\mathfrak{a}\|_\infty$, so that $\rho_h(\xi; \mathfrak{a})$ has size corresponding in rough terms to square-root cancellation amongst the weights $\mathfrak{a}_n$ constrained by the congruence condition $n \equiv \xi \pmod{(p^h, t^2)}$.

We impose an important hypothesis on the distribution of the weights $\mathfrak{a}_n$ for $n \in \mathfrak{Z}(t^2)$, which, fortunately, is easily checked in the situations of greatest interest for us.

Hypothesis 3.1. *There exists a large positive integer B_0 and a small positive number ω for which the collection of weights $(\mathfrak{a})$ satisfies the following properties:*

(i) *one has $p^{2B_0-2} < \|\mathfrak{a}\|_0 \leqslant p^{2B_0}$;*

(ii) *when ν is a non-negative integer with $\nu \leqslant \omega B_0$ and $\zeta_0 \in \mathbb{Z}$, then for each $\varepsilon > 0$, one has*

$$\sum_{\eta=1}^{p^\nu} \|\mathfrak{a}_\nu(\zeta_0 + \eta t)\|_0 \ll (p^\nu)^{\varepsilon-1} \sum_{\zeta=1}^{p^\nu} \sum_{\eta=1}^{p^\nu} \|\mathfrak{a}_\nu(\zeta + \eta t)\|_0.$$

We shall need to make use of this hypothesis also when the sequence $(\mathfrak{a})$ is restricted to particular congruence classes modulo p^h that arise from our inductive procedures. We therefore extend Hypothesis 3.1 to an analogue with uniformity across such restrictions.

Hypothesis 3.2. *Suppose that B_1 is a large positive integer having the property that the collection of weights $(\mathfrak{a})$ satisfies the condition $p^{2B_1-2} < \|\mathfrak{a}\|_0 \leqslant p^{2B_1}$. Then, there is a positive number δ having the property that whenever h is an integer with $0 \leqslant h \leqslant (1-\delta)B_1$ and $\xi \in \mathfrak{Z}(t^2)$, then the collection of weights $(\mathfrak{b}) = (\mathfrak{b}_h(\xi))$ satisfies Hypothesis 3.1.*

Observe that Hypothesis 3.2 has a nested property. Thus, if the collection of weights $(\mathfrak{a})$ satisfies Hypothesis 3.2, then the weights $(\mathfrak{b}) = (\mathfrak{b}_h(\xi))$ occurring in the definition must also satisfy Hypothesis 3.2, though with adjusted choices for B_1 and δ. We shall make use of this nested property, with a large but finite number of nested levels, in our inductive argument.

These hypotheses assert that the support for the weights $\mathfrak{a}_n$ is not overly concentrated on particular residue classes $\zeta_0 \pmod{(p^\nu,t)}$, for $1 \leqslant \nu \leqslant \lfloor \omega B \rfloor$. We record for future reference that the conclusion of this hypothesis may be reintrepreted in the form

$$\sum_{\substack{\xi \pmod{(p^\nu,t^2)}\\ \xi \equiv \zeta_0 \pmod{(p^\nu,t)}}} \rho_\nu(\xi)^2 \ll p^{\varepsilon-\nu}\rho_0(1)^2.$$

Consider temporarily the scenario in which $p^B \leqslant N$ and

$$\mathfrak{a}_n = \begin{cases} 1, & \text{when } n = n_0 + n_1 t, \text{ with } |n_0| \leqslant N \text{ and } |n_1| \leqslant N,\\ 0, & \text{otherwise.} \end{cases}$$

Then one sees that Hypothesis 3.1 is transparently satisfied, for we have

$$\sum_{\substack{\xi \pmod{(p^\nu,t^2)}\\ \xi \equiv \zeta_0 \pmod{(p^\nu,t)}}} \rho_\nu(\xi)^2 = \sum_{\eta=1}^{p^\nu} \Big(\frac{2N}{p^\nu} + O(1) \Big)^2 \ll p^{-\nu}(2N)^2,$$

whilst

$$p^{-\nu}\rho_0(1)^2 = p^{-\nu}(2N + O(1))^2.$$

A similar thought experiment applies in similar fashion for Hypothesis 3.2. It is these and closely allied scenarios that will most likely find application, and so the Hypothesis 3.2 does not restrict our freedom of manoeuvre. The inclusion of the weights $\rho_h(\xi)$ assists us in correctly pursuing the nested iterative procedure as one investigates congruence classes modulo various powers of p. Thus, even though one could avoid Hypotheses 3.1 and 3.2 for the situations of greatest interest to us, the extra flexibility added would seem to be of value.

Next, when $n \in \mathfrak{Z}(t^2)$ and $\alpha_1, \dots, \alpha_k \in \mathfrak{T}(t^2)$, we write

$$\psi(n; \boldsymbol{\alpha}) = \alpha_1\varphi_1(n) + \dots + \alpha_k\varphi_k(n). \tag{3.3}$$

When h is a non-negative integer and $\xi \in \mathfrak{Z}(t^2)$, we define the exponential sum

$$\mathfrak{f}_h(\boldsymbol{\alpha}; \xi) = \mathfrak{f}_h(\boldsymbol{\alpha}; \xi; \mathfrak{a}; \boldsymbol{\varphi})$$

as follows. When $\|\mathfrak{a}\|_\infty > 0$, we put

$$\mathfrak{f}_h(\boldsymbol{\alpha}; \xi) = \rho_h(\xi)^{-1} \sum_{n \equiv \xi \pmod{(p^h,t^2)}} \mathfrak{a}_n E(\psi(n; \boldsymbol{\alpha})), \tag{3.4}$$

where, here and elsewhere, the summation over n is implicitly taken over all $n \in \mathfrak{Z}(t^2)$ constrained by the explicit congruence condition. For completeness, when $\|\mathfrak{a}\|_\infty = 0$, we instead put $\mathfrak{f}_h(\boldsymbol{\alpha}; \xi) = 0$. For brevity, we write $f_{\mathfrak{a}}(\boldsymbol{\alpha})$ for $\mathfrak{f}_0(\boldsymbol{\alpha}; \xi)$. Note that in the scenario outlined in the previous paragraph, one has

$$(2N+1)f_{\mathfrak{a}}(\boldsymbol{\alpha}) = \sum_{|n_0| \leqslant N} \sum_{|n_1| \leqslant N} E\big(\alpha_1\varphi_1(n_0 + n_1 t) + \dots + \alpha_k\varphi_k(n_0 + n_1 t)\big).$$

Specialising the notation from §2 to the case $r = 2$, when B is a positive integer and $F : \mathfrak{T}(t^2)^k \to \mathbb{C}$, we write

$$\oint_{p^B} F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = (p^2)^{-kB} \sum_{u_1 \pmod{(p^B,t^2)}} \cdots \sum_{u_k \pmod{(p^B,t^2)}} F\Big(\frac{u_1}{p^B},\dots,\frac{u_k}{p^B}\Big), \tag{3.5}$$

where the summations are taken over complete sets of elements of $\mathfrak{Z}(t^2)$ modulo p^B. Thus, for example, the summation over u_1 may be construed as running over all elements $v+wt$ with $1 \leqslant v, w \leqslant p^B$. We then define the mean value $U_{s,k}^B(\mathfrak{a}) = U_{s,k}^{B,\boldsymbol{\varphi}}(\mathfrak{a})$ by putting

$$U_{s,k}^B(\mathfrak{a}) = \oint_{p^B} |f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s}\,\mathrm{d}\boldsymbol{\alpha}. \tag{3.6}$$

By orthogonality, the mean value $U_{s,k}^B(\mathfrak{a})$ counts the integral solutions of the simultaneous congruences

$$\sum_{i=1}^{s} (\varphi_j(x_i) - \varphi_j(y_i)) \equiv 0 \pmod{(p^B,t^2)} \quad (1 \leqslant j \leqslant k), \tag{3.7}$$

with $\mathbf{x}, \mathbf{y} \in \mathfrak{Z}(t^2)$, and with each solution $\mathbf{x}, \mathbf{y}$ being counted with weight

$$\rho_0(1)^{-2s} \prod_{i=1}^{s} \mathfrak{a}_{x_i} \overline{\mathfrak{a}}_{y_i}.$$

A variant of $U_{s,k}^B(\mathfrak{a})$, in which the underlying variables are restricted to a common congruence class ξ modulo (p^h, t^2), is defined by putting $U_{s,k}^{B,h}(\mathfrak{a}) = U_{s,k}^{B,h,\boldsymbol{\varphi}}(\mathfrak{a})$, where

$$U_{s,k}^{B,h,\boldsymbol{\varphi}}(\mathfrak{a}) = \rho_0(1)^{-2} \sum_{\xi \pmod{(p^h,t^2)}} \rho_h(\xi)^2 \oint_{p^B} |\mathfrak{f}_h(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}. \tag{3.8}$$

By orthogonality, once again, the integral on the right hand side of (3.8) counts the solutions $\mathbf{x}, \mathbf{y} \in \mathfrak{Z}(t^2)^s$ of the system (3.7) satisfying $\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{(p^h, t^2)}$ with weight

$$\rho_h(\xi)^{-2s} \prod_{i=1}^{s} \mathfrak{a}_{x_i} \overline{\mathfrak{a}}_{y_i}.$$

We briefly discuss a trivial estimate for the mean value $U_{s,k}^{B,h}(\mathfrak{a})$ in order to motivate the analysis to come. Our starting point is a decomposition of the exponential sum $f_{\mathfrak{a}}(\boldsymbol{\alpha})$ into the residue classes modulo (p^H, t^2) of the summands. Thus, from (3.4), we find that

$$\begin{aligned} f_{\mathfrak{a}}(\boldsymbol{\alpha}) &= \rho_0(1)^{-1} \sum_{\xi \pmod{(p^H,t^2)}} \sum_{n \equiv \xi \pmod{(p^H,t^2)}} \mathfrak{a}_n E(\psi(n;\boldsymbol{\alpha})) \\ &= \rho_0(1)^{-1} \sum_{\xi \pmod{(p^H,t^2)}} \rho_H(\xi) \mathfrak{f}_H(\boldsymbol{\alpha};\xi). \end{aligned}$$

Since

$$\sum_{\xi \pmod{(p^H,t^2)}} \rho_H(\xi)^2 = \sum_{\xi \pmod{(p^H,t^2)}} \|\mathfrak{a}_H(\xi)\|_0 \cdot \|\mathfrak{a}_H(\xi)\|_\infty^2 \leqslant \|\mathfrak{a}\|_0 \cdot \|\mathfrak{a}\|_\infty^2 = \rho_0(1)^2,$$

an application of Hölder's inequality reveals that $|f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s}$ is bounded above by

$$\rho_0(1)^{-2s}\bigg(\sum_{\xi\ (\mathrm{mod}\ (p^H,t^2))}1\bigg)^s\bigg(\sum_{\xi\ (\mathrm{mod}\ (p^H,t^2))}\rho_H(\xi)^2\bigg)^{s-1}\sum_{\xi\ (\mathrm{mod}\ (p^H,t^2))}\rho_H(\xi)^2|\mathfrak{f}_H(\boldsymbol{\alpha};\xi)|^{2s}$$
$$\ll (p^{2H})^s\rho_0(1)^{-2}\sum_{\xi\ (\mathrm{mod}\ (p^H,t^2))}\rho_H(\xi)^2|\mathfrak{f}_H(\boldsymbol{\alpha};\xi)|^{2s}. \tag{3.9}$$

Thus, on recalling (3.6) and (3.8), we infer that

$$U^B_{s,k}(\mathfrak{a})\leqslant (p^{2H})^sU^{B,H}_{s,k}(\mathfrak{a}). \tag{3.10}$$

As in the analogous discussion of [11], we are consequently justified in seeking an exponent λ having the property that, for each $\varepsilon>0$, one has

$$U^B_{s,k}(\mathfrak{a})\ll (p^{2H})^{\lambda+\varepsilon}U^{B,H}_{s,k}(\mathfrak{a}), \tag{3.11}$$

with as much uniformity as is feasible to establish in the various parameters. A comparison of (3.10) and (3.11) makes it apparent already that such an exponent λ exists with $\lambda\leqslant s$.

We now discuss a number of helpful simplifications. We observe first that the definition (3.4) of $\mathfrak{f}_h(\boldsymbol{\alpha};\xi)$ ensures that we have scale invariance with repect to the coefficient weights $\mathfrak{a}$. Thus, if $\gamma>0$ and $\mathfrak{a}$ is replaced by $\gamma\mathfrak{a}$, then since $\rho_h(\gamma\mathfrak{a})=\gamma\rho_h(\mathfrak{a})$, the exponential sum $\mathfrak{f}_h(\boldsymbol{\alpha};\xi)$ remains unchanged. The exponential sum $f_{\mathfrak{a}}(\boldsymbol{\alpha})$ and the mean values $U^B_{s,k}(\mathfrak{a})$ and $U^{B,h}_{s,k}(\mathfrak{a})$ all inherit this scale invariance property. Denote by $\mathbb{D}(B)$ the set of sequences $(\mathfrak{a}_n)_{n\in\mathfrak{Z}(t^2)}$ satisfying Hypothesis 3.2 with $|\mathfrak{a}_n|\leqslant 1$ ($n\in\mathfrak{Z}(t^2)$) and

$$p^{2B-2}<\|\mathfrak{a}\|_0<p^{2B}.$$

Also, write $\mathbb{D}_0(B)=\mathbb{D}(B)\cup\{\mathbf{0}\}$. Then, in view of the scale invariance just discussed, we are at liberty to restrict our deliberations to sequences $(\mathfrak{a}_n)$ lying in $\mathbb{D}(B)$.

We next provide a precise definition of a real number tantamount to the exponent λ discussed above. When $\tau>0$, we denote by $\Phi_\tau(B)$ the set of p^c-spaced k-tuples of polynomials $\boldsymbol{\varphi}(u)$, with $c\geqslant\tau B$. The upper bound (3.10) ensures that for each fixed $B\in\mathbb{N}$ and $\boldsymbol{\varphi}(u)\in\Phi_\tau(B)$, and for every non-negative integer H, one has

$$\sup_{(\mathfrak{a})\in\mathbb{D}(B)}\frac{\log\big(U^B_{s,k}(\mathfrak{a})/U^{B,H}_{s,k}(\mathfrak{a})\big)}{\log(p^{2H})}\leqslant s.$$

Now, given $s>0$, $\theta\geqslant 1$ and $\tau>0$, we write $H=\lceil B/\theta\rceil$, and define

$$\lambda^*(s,\theta;\tau)=\limsup_{B\to\infty}\sup_{\boldsymbol{\varphi}\in\Phi_\tau(B)}\sup_{(\mathfrak{a})\in\mathbb{D}(B)}\frac{\log\big(U^B_{s,k}(\mathfrak{a})/U^{B,H}_{s,k}(\mathfrak{a})\big)}{\log(p^{2H})}. \tag{3.12}$$

We shall be focused on the limiting exponent

$$\lambda(s,\theta)=\limsup_{\tau\to 0+}\lambda^*(s,\theta;\tau). \tag{3.13}$$

Since it is apparent from the discussion above that $\lambda^*(s,\theta;\tau)\leqslant s$, we deduce that

$$\lambda(s,\theta)\leqslant s. \tag{3.14}$$

The main conclusion of this memoir is described in the following theorem.

Theorem 3.3. *Suppose that $k \in \mathbb{N}$ and that p is a prime with $p > k$. Then one has $\lambda(k(k+1)/2, k) \leqslant 0$.*

The utility of this theorem is made transparent in the following corollary.

Corollary 3.4. *Suppose that $k \in \mathbb{N}$ and that p is a prime number with $p > k$. In addition, let $\tau > 0$ and $\varepsilon > 0$. Finally, let B be sufficiently large in terms of k, τ and ε. Put $s = k(k+1)/2$ and $H = \lceil B/k \rceil$. Then for every $\boldsymbol{\varphi} \in \Phi_\tau(B)$, and every sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, one has*

$$U_{s,k}^B(\mathfrak{a}) \ll (p^B)^\varepsilon U_{s,k}^{B,H}(\mathfrak{a}). \tag{3.15}$$

It is apparent from the relation (3.15) that in a certain sense, one can assume an additional constraint within the underlying mean value (3.6) that effectively concentrates the underlying variables towards the same congruence class modulo (p^H, t^2). In the model situation in which $\mathfrak{a}_n$ is supported only when $n = n_0 + n_1 t$ with $|n_0| \leqslant N$ and $|n_1| \leqslant N$, we shall see that when B is large enough that $p^B > N^k$, then one has $U_{s,k}^{B,H}(\mathfrak{a}) \ll p^{B\varepsilon}$, and hence also $U_{s,k}^B(\mathfrak{a}) \ll p^{2B\varepsilon}$.

Our next step is to introduce auxiliary mean values that form the important cogs in our nested iterative machine. Throughout, we fix $s = k(k+1)/2$. Let a, b, c and ν be non-negative integers. We consider a fixed p^c-spaced k-tuple of polynomials $\boldsymbol{\varphi} \in \mathbb{Z}[t,u]^k$, and we fix a complex sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$. When $0 \leqslant r \leqslant k$, we define the mean value $K_{a,b}^r = K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a})$ by putting

$$K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a}) = \rho_0(1)^{-4} \sum_{\xi \pmod{(p^a,t^2)}} \sum_{\substack{\eta \pmod{(p^b,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_a(\xi)^2 \rho_b(\eta)^2 K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta), \tag{3.16}$$

in which

$$K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta) = \oint_{p^B} |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2R} \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}| \, \mathrm{d}\boldsymbol{\alpha} \tag{3.17}$$

and $R = r(r+1)/2$. The inclusion of the superscript ν in this notation is intended to remind us of the assumption in the second summation of (3.16) that $p^\nu \nmid (\eta_0 - \xi_0)$, in which we have written $\xi = \xi_0 + \xi_1 t$ and $\eta = \eta_0 + \eta_1 t$, with $\xi_i, \eta_i \in \mathbb{Z}$. The reader may care to note, for future reference, that this condition ensures that $\eta - \xi$ is approximately a unit in the ring $\mathbb{Z}[t]/(p^B, t^2)$. For future reference, we note that as a consequence of orthogonality, the mean value $K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta)$ counts the solutions in $\mathfrak{Z}(t^2)$ of the simultaneous congruences

$$\sum_{i=1}^{R} \big(\varphi_j(x_i) - \varphi_j(y_i)\big) \equiv \sum_{l=1}^{s-R} \big(\varphi_j(v_l) - \varphi_j(w_l)\big) \pmod{(p^B,t^2)} \quad (1 \leqslant j \leqslant k), \tag{3.18}$$

satisfying

$$\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{(p^a,t^2)} \quad \text{and} \quad \mathbf{v} \equiv \mathbf{w} \equiv \eta \pmod{(p^b,t^2)}, \tag{3.19}$$

with each solution being counted with weight

$$\rho_a(\xi)^{-2R} \rho_b(\eta)^{2R-2s} \Big(\prod_{i=1}^{R} \mathfrak{a}_{x_i} \overline{\mathfrak{a}}_{y_i} \Big) \Big(\prod_{l=1}^{s-R} \mathfrak{a}_{v_l} \overline{\mathfrak{a}}_{w_l} \Big). \tag{3.20}$$

We note that the relations (3.18), (3.19) and (3.20) require careful interpretation. Indeed, each variable x_i, y_i, v_l, w_l is an element of $\mathfrak{Z}(t^2)$. Thus, for example, one should think of

x_i as being of the shape $u+vt$, with $u,v\in\mathbb{Z}$. Likewise, one should think of ξ and η as lying in $\mathfrak{Z}(t^2)$, with similar associated comments.

As in our previous work [11] on nested efficient congruencing, we find it useful to introduce notation making the size of a mean value relative to its conjectured size more readily transparent. Following this previous path, when $1\leqslant r\leqslant k-1$ and Δ is a positive number, we define

$$[[K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a})]]_\Delta=\left(\frac{K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a})}{(p^{2H})^\Delta U_{s,k}^{B,H}(\mathfrak{a})}\right)^{\frac{k-1}{r(k-r)}}. \tag{3.21}$$

Much of our discussion in the coming sections is largely independent of the parameters ν and c, the sequence $\mathfrak{a}$, and the polynomial system $\boldsymbol{\varphi}$. Hence, when ambiguity is easily avoided, we shall feel free to omit explicit mention of such notational decorations. We note also that the exponent

$$\frac{k-1}{r(k-r)},$$

as in the analogous treatment of [11], serves to streamline the nested iteration by enabling a simplified single branch version to be utilised in place of the more complicated multi-branch process immediately to hand.

4. Uniform estimates for translation-dilation invariant families

As explained in [11, §4], a p^c-spaced system of polynomials $\boldsymbol{\varphi}$ may be thought of as approximating the special system in which $\varphi_j(u)=u^j$ $(1\leqslant j\leqslant k)$. The system of congruences

$$\sum_{i=1}^s\varphi_j(x_i)\equiv\sum_{i=1}^s\varphi_j(y_i)\ (\mathrm{mod}\ (p^B,t^2))\quad (1\leqslant j\leqslant k) \tag{4.1}$$

is then translation-dilation invariant. Thus, whenever $\mathbf{x},\mathbf{y}$ is a solution of (4.1), then so too is $q\mathbf{x}+a,q\mathbf{y}+a$, for any $q,a\in\mathbb{Z}[t]$. This property permits a certain scaling property to be established for the mean value $U_{s,k}^{B,h}(\mathfrak{a})$. In advance of the announcement and proof of this scaling property, we pause to establish two basic invertibility properties of elements in $\mathbb{Z}[t]/(p^B,t^d)$ and associated matrices.

Lemma 4.1. *Let d be a natural number, and suppose that $n\in\mathbb{Z}[t]/(p^B,t^d)$. Let n_0 be an integer having the property that $n\equiv n_0\ (\mathrm{mod}\ (p^B,t))$, and suppose that $(n_0,p)=1$. Then n possesses a multiplicative inverse n^{-1} lying in $\mathbb{Z}[t]/(p^B,t^d)$.*

Proof. Since $(n_0,p)=1$, there exists an integer m_0 having the property that one has $m_0n_0\equiv 1\ (\mathrm{mod}\ p^B)$. On observing that $m_0n-1\equiv 0\ (\mathrm{mod}\ (p^B,t))$, we see that for suitable elements $\chi,\omega\in\mathbb{Z}[t]/(p^B,t)$, one has

$$m_0n=1+p^B\chi+t\omega.$$

We now define the polynomial

$$m=1-(p^B\chi+t\omega)+(p^B\chi+t\omega)^2-\ldots+(-1)^{d-1}(p^B\chi+t\omega)^{d-1}.$$

One sees that

$$m(m_0n)=1+(-1)^{d-1}(p^B\chi+t\omega)^d\equiv 1+(-1)^{d-1}(t\omega)^d\equiv 1\ (\mathrm{mod}\ (p^B,t^d)).$$

Hence, the element n has the multiplicative inverse $n^{-1} = m_0 m$ modulo (p^B, t^d). □

In the next lemma, and later, we denote the $k \times k$ identity matrix over the ring $\mathbb{Z}[t]/(p^B, t^d)$ by I_k.

Lemma 4.2. *Let d be a natural number, and suppose that $A = (a_{ij})_{1 \leqslant i,j \leqslant k}$ is a matrix with entries in $\mathbb{Z}[t]/(p^B, t^d)$ having the property that $A \equiv I_k \pmod{(p,t)}$. Then A has an inverse matrix A^{-1} in $\mathbb{Z}[t]/(p^B, t^d)$ satisfying $A^{-1} \equiv I_k \pmod{(p,t)}$.*

Proof. By appealing to the reader's knowledge of standard linear algebra, the existence of A^{-1} is assured provided one is able to apply elementary row operations to obtain I_k from A. We first show that a sequence of elementary row operations may be employed to transform A into lower triangular form $A^{(0)}$ with $A^{(0)} \equiv I_k \pmod{(p,t)}$. This we establish in the familiar inductive manner. We suppose at stage r that A has been transformed into a matrix $A^{(r)}$, with $A^{(r)} \equiv I_k \pmod{(p,t)}$, having the property that the columns with index exceeding r are already in lower triangular form. This of course holds trivially when $r = k$ with $A^{(k)} = A$. We then seek to establish that the same conclusion can be obtained for all columns with index exceeding $r-1$. For this purpose, it suffices to observe that, in view of Lemma 4.1, the diagonal entry $a_{rr}^{(r)}$ possesses a multiplicative inverse in $\mathbb{Z}[t]/(p^B, t^d)$, an element we label as $(a_{rr}^{(r)})^{-1}$. We subtract $a_{ir}^{(r)}(a_{rr}^{(r)})^{-1}$ times the r-th row from the i-th row, for $1 \leqslant i < r$. In this way, we obtain a new matrix $A^{(r-1)}$ having lower triangular form amongst the columns with index exceeding $r-1$. Since $a_{ir}^{(r)} \equiv 0 \pmod{(p,t)}$ for $1 \leqslant i < r$, moreover, we see that this new matrix remains congruent to I_k modulo (p,t). This completes the inductive step, so that we may now work with the lower triangular matrix $A^{(0)}$.

The next step is to convert the matrix $A^{(0)}$ from lower triangular form to diagonal form $D^{(k)}$ via elementary row operations, again with $D^{(k)} \equiv I_k \pmod{(p,t)}$. This we achieve by reversing course, again applying induction. We suppose at stage r that $A^{(0)}$ has been transformed into a matrix $D^{(r-1)}$, with $D^{(r-1)} \equiv I_k \pmod{(p,t)}$, having the property that the columns with index smaller than r are already in diagonal form. This holds trivially when $r = 1$ with $D^{(0)} = A^{(0)}$. We then seek to establish that the same conclusion can be obtained for all columns with index smaller than $r+1$. In this instance, we subtract $d_{ir}^{(r)}(d_{rr}^{(r)})^{-1}$ times the r-th row from the i-th row, for $r < i \leqslant k$. In this way, we obtain a new matrix $D^{(r)}$ having diagonal form amongst the columns with index smaller than $r+1$. Since $d_{ir}^{(r)} \equiv 0 \pmod{(p,t)}$ for $r < i \leqslant k$, moreover, we again see that this new matrix remains congruent to I_k modulo (p,t). This completes the inductive step in this second phase, and so we may now work with the diagonal matrix $D^{(k)}$.

Finally, by multiplying the r-th row through by $(d_{rr}^{(k)})^{-1}$ for $1 \leqslant r \leqslant k$, we transform the diagonal matrix $D^{(k)}$ into I_k. We have thus shown that the matrix A may be converted to I_k through elementary row operations defined over $\mathbb{Z}[t]/(p^B, t^d)$, and thus A possesses a multiplicative inverse A^{-1} having entries in the same ring. Finally, since $A \equiv I_k \pmod{(p,t)}$, we must have $A^{-1} \equiv I_k \pmod{(p,t)}$. This completes the proof of the lemma. □

It is useful also to have an extension of this result applicable to triangular matrices.

Lemma 4.3. *Let d be a natural number, and suppose that $A = (a_{ij})_{1\leqslant i,j\leqslant k}$ is a matrix with entries in $\mathbb{Z}[t]/(p^B, t^d)$ having the property that*

$$a_{ij} \equiv \begin{cases} 0 \pmod{(p,t)}, & \text{when } i > j, \\ 1 \pmod{(p,t)}, & \text{when } i = j. \end{cases}$$

Then A has an inverse matrix A^{-1} in $\mathbb{Z}[t]/(p^B, t^d)$.

Proof. We adopt the inductive approach of the proof of the previous lemma, applying elementary row operations to transform the matrix A into a new matrix C in which $C \equiv I_k \pmod{(p,t)}$. The matrix A has an inverse matrix A^{-1}, with entries in $\mathbb{Z}[t]/(p^B, t)$, if and only if C is invertible in the latter ring. However, the invertibility of C is guaranteed by the conclusion of Lemma 4.2, and thus the desired conclusion follows. This completes the proof of the lemma. □

With these preliminaries in hand, we are now equipped to establish the main conclusion of this section.

Lemma 4.4. *Suppose that $k \in \mathbb{N}$ and that p is a prime number with $p > k$. Let τ, ε and δ be positive numbers with $\varepsilon < \tau < \delta < 1$, and let B be sufficiently large in terms of s, k and ε. Write $H = \lceil B/k \rceil$. Then for every $\boldsymbol{\varphi} \in \Phi_\tau(B)$, every sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, and every non-negative integer h with $h \leqslant (1-\delta)H$, one has*

$$U_{s,k}^{B,h}(\mathfrak{a}) \ll (p^{2(H-h)})^{\lambda(s,k)+\varepsilon} U_{s,k}^{B,H}(\mathfrak{a}).$$

Proof. The argument required in our proof is a mild adjustment of that applied to establish [11, Lemma 4.1], with a small number of critical adjustments. Since the setting is somewhat alien, however, at the risk of being seemingly repetitive in places, we provide fairly complete details.

Consider a p^c-spaced k-tuple of polynomials $\boldsymbol{\varphi}$ with $c \geqslant \tau B$, and a complex sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, with associated parameters satisfying the statement of the lemma. As in the proof of [11, Lemma 4.1], we let h be an integer with $0 \leqslant h \leqslant (1-\delta)H$. Then it follows from (3.4) that

$$\mathfrak{f}_h(\boldsymbol{\alpha}; \xi) = \rho_h(\xi)^{-1} \sum_{y \in \mathfrak{Z}(t^2)} \mathfrak{b}_y(\xi) E(\psi(p^h y + \xi; \boldsymbol{\alpha})), \tag{4.2}$$

with $\psi(n; \boldsymbol{\alpha})$ defined by (3.3), and where

$$\mathfrak{b}_y(\xi) = \mathfrak{a}_{p^h y + \xi} \quad (y \in \mathfrak{Z}(t^2)). \tag{4.3}$$

An appeal to orthogonality reveals that the mean value on the right hand side of (3.8) counts the solutions $\mathbf{y}, \mathbf{z} \in \mathfrak{Z}(t^2)$ of the simultaneous congruences

$$\sum_{i=1}^{s} \varphi_j(p^h y_i + \xi) \equiv \sum_{i=1}^{s} \varphi_j(p^h z_i + \xi) \pmod{(p^B, t^2)} \quad (1 \leqslant j \leqslant k), \tag{4.4}$$

with each solution being counted with weight

$$\rho_h(\xi)^{-2s} \prod_{i=1}^{s} \mathfrak{b}_{y_i} \overline{\mathfrak{b}}_{z_i}. \tag{4.5}$$

Since the system $\boldsymbol{\varphi}$ is p^c-spaced, we find from (3.1) that for suitable polynomials $\psi_j(u), \chi_j(u) \in \mathbb{Z}[t,u]$, one may write

$$\varphi_j(u) = \sum_{i=1}^{k} \omega_{ij} u^i + u^{k+1}\big(p^c\psi_j(u) + t\chi_j(u)\big) \quad (1 \leqslant j \leqslant k),$$

for some coefficient matrix $A_1 = (\omega_{ij})_{1\leqslant i,j\leqslant k}$ congruent modulo (p^c,t) to the $k \times k$ identity matrix I_k. Since $A_1 \equiv I_k \pmod{(p^c,t)}$, it follows from Lemma 4.2 that A_1 possesses a multiplicative inverse A_1^{-1} modulo (p^B,t^2), having coefficients lying in $\mathbb{Z}[t]/(p^B,t^2)$, and satisfying $A_1^{-1} \equiv I_k \pmod{(p,t)}$. We replace $\boldsymbol{\varphi}$ by $A_1^{-1}\boldsymbol{\varphi}$, likewise $\boldsymbol{\psi}$ by $A_1^{-1}\boldsymbol{\psi}$, and also $\boldsymbol{\chi}$ by $A_1^{-1}\boldsymbol{\chi}$. In so doing, we are effectively taking suitable integral linear combinations of the congruences comprising (4.4). In this way, we see that there is no loss of generality in supposing that for $1 \leqslant j \leqslant k$, one has

$$\varphi_j(u) = u^j + u^{k+1}\big(p^c\psi_j(u) + t\chi_j(u)\big) \quad (1 \leqslant j \leqslant k). \tag{4.6}$$

The polynomials $\varphi_j(u)$ defined as in (4.6) are now in a convenient form with which to apply the binomial theorem. Thus, for suitable polynomials $\Psi_j(u), \mathrm{X}_j(u) \in \mathbb{Z}[t,u]$, one has

$$\varphi_j(p^h y + \xi) - \varphi_j(\xi) = \Phi_j(p^h y),$$

in which

$$\Phi_j(w) = \sum_{i=1}^{k} \Omega_{ij} w^i + w^{k+1}\big(p^c\Psi_j(w) + t\mathrm{X}_j(w)\big) \quad (1 \leqslant j \leqslant k),$$

and the coefficients $\Omega_{ij} \in \mathbb{Z}[t]$ satisfy

$$\Omega_{ij} \equiv \binom{j}{i}\xi^{j-i} \pmod{(p^c,t)} \quad (1 \leqslant i,j \leqslant k).$$

As usual here, we adopt the convention that the binomial coefficient $\binom{j}{i}$ is equal to 0 for $i > j$. The matrix $A_2 = (\Omega_{ij})_{1\leqslant i,j\leqslant k}$ satisfies the property that

$$\Omega_{ij} \equiv \begin{cases} 0 \pmod{(p,t)}, & \text{when } i > j, \\ 1 \pmod{(p,t)}, & \text{when } i = j. \end{cases}$$

Since we assume that $p > k$, we find from Lemma 4.3 that the matrix A_2 possesses a multiplicative inverse A_2^{-1} in $\mathbb{Z}[t]/(p^B,t^2)$. We now replace $\boldsymbol{\Phi}$ by $A_2^{-1}\boldsymbol{\Phi}$, likewise $\boldsymbol{\Psi}$ by $A_2^{-1}\boldsymbol{\Psi}$, and also $\mathbf{X}$ by $A_2^{-1}\mathbf{X}$. This transformation again corresponds to taking linear combinations of the congruences comprising (4.4). In this way, we see that there is no loss of generality in supposing that the coefficient matrix A_2 is equal to I_k. Consequently, there exist polynomials $\Upsilon_j(u), \Theta_j(u) \in \mathbb{Z}[t,u]$ having the property that whenever the system (4.4) is satisfied, then

$$\sum_{i=1}^{s} (p^h)^j\big(\Phi_j(y_i) - \Phi_j(z_i)\big) \equiv 0 \pmod{(p^B,t^2)} \quad (1 \leqslant j \leqslant k), \tag{4.7}$$

in which $\Phi_j(u)$ has been redefined by putting

$$\Phi_j(u) = u^j + p^h u^{k+1}\big(p^c\Upsilon_j(u) + t\Theta_j(u)\big). \tag{4.8}$$

At the conclusion of this first phase of the argument, we have shown that the solutions $\mathbf{y}, \mathbf{z} \in \mathfrak{Z}(t^2)$ of the system of congruences (4.4), counted with weight (4.5) associated with the definition (3.8) of $U_{s,k}^{B,h}(\mathfrak{a})$, are constrained by an additional system of congruences. Thus, we have

$$\sum_{i=1}^{s} \Phi_j(y_i) \equiv \sum_{i=1}^{s} \Phi_j(z_i) \pmod{(p^{B-kh}, t^2)} \quad (1 \leqslant j \leqslant k). \tag{4.9}$$

The condition (4.9) can be incorporated into the mean value $U_{s,k}^{B,h}(\mathfrak{a})$. When $\boldsymbol{\beta} \in \mathfrak{T}(t^2)^k$, we define

$$\mathfrak{g}_h(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi) = \rho_h(\xi)^{-1} \sum_{y \in \mathfrak{Z}(t^2)} \mathfrak{c}_y(\xi; \boldsymbol{\alpha}) E(\psi^*(y; \boldsymbol{\beta})), \tag{4.10}$$

where

$$\mathfrak{c}_y(\xi; \boldsymbol{\alpha}) = \mathfrak{b}_y(\xi) E(\psi(p^h y + \xi; \boldsymbol{\alpha})), \tag{4.11}$$

with the coefficient $\mathfrak{b}_y(\xi)$ defined in (4.3), and

$$\psi^*(y; \boldsymbol{\beta}) = \beta_1 \Phi_1(y) + \ldots + \beta_k \Phi_k(y).$$

It then follows via orthogonality that

$$\oint_{p^B} |\mathfrak{f}_h(\boldsymbol{\alpha}; \xi)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} = \oint_{p^B} \oint_{p^{B-kh}} |\mathfrak{g}_h(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi)|^{2s} \, \mathrm{d}\boldsymbol{\beta} \, \mathrm{d}\boldsymbol{\alpha}. \tag{4.12}$$

The polynomial system $\boldsymbol{\Phi}$ defined in (4.8) is p^{c+h}-spaced. Moreover, we assume that $h \leqslant (1 - \delta)H$, and hence $B - kh \geqslant \delta B - k$. We may therefore assume that $B - kh$ is sufficiently large in terms of s, k and ε. In view of (4.3), (4.11) and Hypothesis 3.2, moreover, we may assume that the set of weights $(\mathfrak{c}_y(\xi; \boldsymbol{\alpha}))$ satisfies Hypothesis 3.2. Thus, we deduce from (3.12) and (3.13) that

$$U_{s,k}^{B-kh}(\mathfrak{c}) \ll \big(p^{2(H-h)}\big)^{\lambda(s,k)+\varepsilon} U_{s,k}^{B-kh,H-h}(\mathfrak{c}).$$

We therefore deduce from (3.8) and (4.10) that one has the bound

$$\oint_{p^{B-kh}} |\mathfrak{g}_h(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi)|^{2s} \, \mathrm{d}\boldsymbol{\beta} \ll \big(p^{2(H-h)}\big)^{\lambda(s,k)+\varepsilon} I_1, \tag{4.13}$$

where

$$I_1 = \rho_h(\xi)^{-2} \sum_{\eta \pmod{(p^{H-h}, t^2)}} \rho_{H-h}(p^h \eta + \xi)^2 \oint_{p^{B-kh}} |\mathfrak{g}_{H-h}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi, \eta)|^{2s} \, \mathrm{d}\boldsymbol{\beta},$$

and

$$\mathfrak{g}_{H-h}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi, \eta) = \rho_{H-h}(p^h \eta + \xi)^{-1} \sum_{y \equiv \eta \pmod{(p^{H-h}, t^2)}} \mathfrak{c}_y(\xi; \boldsymbol{\alpha}) E(\psi^*(y; \boldsymbol{\beta})).$$

The direct correspondence between residues ζ modulo (p^H, t^2) and pairs (ξ, η) of residues modulo (p^h, t^2), and modulo (p^{H-h}, t^2), respectively, via the relation $\zeta = p^h \eta + \xi$, reveals that

$$\mathfrak{g}_{H-h}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}; \xi, \eta) = \rho_H(\zeta)^{-1} \sum_{\substack{y \in \mathfrak{Z}(t^2) \\ p^h y + \xi \equiv \zeta \pmod{(p^H, t^2)}}} \mathfrak{a}_{p^h y + \xi} E\big(\psi(p^h y + \xi; \boldsymbol{\alpha}) + \psi^*(y; \boldsymbol{\beta})\big).$$

In particular, we deduce from (4.12) and (4.13) that

$$\sum_{\xi \pmod{(p^h,t^2)}} \rho_h(\xi)^2 \oint_{p^B} |\mathfrak{f}_h(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}$$
$$\ll \big(p^{2(H-h)}\big)^{\lambda(s,k)+\varepsilon} \sum_{\substack{\zeta \pmod{(p^H,t^2)}\\ \zeta=p^h\eta+\xi}} \rho_H(\zeta)^2 \oint_{p^B}\oint_{p^{B-kh}} |\mathfrak{g}^*_{H-h}(\boldsymbol{\alpha},\boldsymbol{\beta};\xi,\eta)|^{2s}\,\mathrm{d}\boldsymbol{\beta}\,\mathrm{d}\boldsymbol{\alpha}. \tag{4.14}$$

By orthogonality, the mean value on the right hand side of (4.14) counts solutions of the system of congruences (4.4), with each solution being counted with weight (4.5), but subject to the additional condition that

$$p^h\mathbf{y}+\xi \equiv p^h\mathbf{z}+\xi \equiv \zeta \pmod{(p^H,t^2)},$$

and further, subject to the additional congruence conditions (4.9). Note that the latter congruence conditions are generated by the integral over $\boldsymbol{\beta}$ in the mean value on the right hand side of (4.14). The conditions (4.9) are implied by (4.4), as we have shown above. Note also that when $\zeta = p^h\eta+\zeta$, one has

$$\mathfrak{g}^*_{H-h}(\boldsymbol{\alpha},\mathbf{0};\xi,\eta) = \rho_H(\zeta)^{-1} \sum_{n\equiv\zeta \pmod{(p^H,t^2)}} \mathfrak{a}_n e(\psi(n;\boldsymbol{\alpha})) = \mathfrak{f}_H(\boldsymbol{\alpha};\zeta).$$

Then, since the conditions (4.9) may be omitted, the definition (3.8) leads us to the conclusion that

$$U^{B,h}_{s,k}(\mathfrak{a}) \ll \big(p^{2(H-h)}\big)^{\lambda(s,k)+\varepsilon}\rho_0(1)^{-2} \sum_{\zeta \pmod{(p^H,t^2)}} \rho_H(\zeta)^2 \oint_{p^B} |\mathfrak{f}_H(\boldsymbol{\alpha};\zeta)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}$$
$$= \big(p^{2(H-h)}\big)^{\lambda(s,k)+\varepsilon} U^{B,H}_{s,k}(\mathfrak{a}).$$

This completes the proof of the lemma. □

We require a crude estimate for $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})$. This we obtain by applying Hölder's inequality in combination with Lemma 4.4.

Lemma 4.5. *Suppose that $k \in \mathbb{N}$ and that p is a prime number with $p > k$. Let τ, ε and δ be positive numbers with $\varepsilon < \tau < \delta < 1$, and let B be sufficiently large in terms of s, k and ε. Write $H = \lceil B/k \rceil$ and suppose that r and ν are non-negative integers with $1 \leqslant r \leqslant k-1$. In addition, suppose that $0 < \Lambda \leqslant \lambda(s,k)$. Then for every $\boldsymbol{\varphi} \in \Phi_\tau(B)$, every sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, and all non-negative integers a and b satisfying $\max\{a,b\} \leqslant (1-\delta)H$, one has*

$$[[K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})]]_\Lambda \ll (p^{2H})^{\lambda(s,k)-\Lambda+\varepsilon}.$$

Proof. A comparison with the statement and proof of [11, Lemma 4.2] reveals that the same argument as was applied to prove the latter remains valid, *mutatis mutandis*, in the present situation. It is important to note from the preamble to (3.9) that one has

$$\sum_{\zeta \pmod{(p^h,t^2)}} \rho_h(\zeta)^2 \leqslant \rho_0(1)^2,$$

in alignment with the corresponding relation applied in the proof of [11, Lemma 4.2]. Moreover, in the conclusion of Lemma 4.4 above, we have a power of $p^{2(H-h)}$ in place of the corresponding power of p^{H-h} in the conclusion of [11, Lemma 4.1]. Equipped with these observations, the reader will experience no difficulties in tracking through the argument of the proof of [11, Lemma 4.2] to obtain the conclusion of the present lemma. □

5. The base case $k = 1$: a variant of Hensel's lemma

The base case for our nested induction is that in which $k = 1$. The proof of Theorem 3.3 in this case is tantamount to a special case of Hensel's lemma in the ring $\mathbb{Z}[t]/(p^B, t^2)$, as we now explain.

Lemma 5.1. *For any prime number p, one has $\lambda(1, 1) = 0$.*

Proof. Let τ be a small positive number, and let B be a positive integer sufficiently large in terms of τ. Consider any sequence $(\mathfrak{a}) \in \mathbb{D}(B)$ and polynomial $\varphi \in \Phi_\tau(B)$. We suppose that $\varphi(u)$ is a p^c-spaced polynomial for some $c \geqslant \tau B$, so that

$$\varphi(u) = u + p^c\psi(u) + t\chi(u),$$

for suitable polynomials $\psi(u), \chi(u) \in \mathbb{Z}[t, u]$. We observe that the mean value $U^B_{1,1}(\mathfrak{a})$ counts the solutions of the congruence

$$\varphi(x) \equiv \varphi(y) \pmod{(p^B, t^2)}, \tag{5.1}$$

with each solution $x, y \in \mathfrak{Z}(t^2)$ being counted with weight $\rho_0(1)^{-2}\mathfrak{a}_x\overline{\mathfrak{a}}_y$. By writing the congruence (5.1) in the form

$$x - y + p^c(\psi(x) - \psi(y)) + t(\chi(x) - \chi(y)) \equiv 0 \pmod{(p^B, t^2)}, \tag{5.2}$$

we see that

$$x - y \equiv 0 \pmod{(p^B, p^c, t)}. \tag{5.3}$$

Note here that the ideal (p^B, p^c, t) is, of course, equal to $(p^{\min\{B,c\}}, t)$, and we have chosen the former as a less awkward avatar of the latter.

Since $x - y$ divides both $\psi(x) - \psi(y)$ and $\chi(x) - \chi(y)$, it follows by substituting (5.3) into the right hand side of (5.2) that

$$x - y \equiv 0 \pmod{(p^B, p^{2c}, p^ct, t^2)}. \tag{5.4}$$

By repeating this argument with (5.4) in place of (5.3), and embarking on the inductive argument to hand, we find that for each non-negative integer m, one has

$$x - y \equiv 0 \pmod{(p^B, p^{(m+1)c}, p^{mc}t, t^2)}.$$

We take $m = \lceil 1/\tau \rceil$, and conclude that in fact $x - y \equiv 0 \pmod{(p^B, t^2)}$. Thus, the solutions of (5.2) may be classified according to the common congruence class ξ modulo (p^B, t^2) of x and y. Making use of the definitions (3.4), (3.6) and (3.8), we deduce via orthogonality that

$$U^B_{1,1}(\mathfrak{a}) = \rho_0(1)^{-2} \sum_{\xi \pmod{(p^B,t^2)}} \rho_B(\xi)^2 \oint_{p^B} |\mathfrak{f}_B(\alpha; \xi)|^2 \, \mathrm{d}\alpha = U^{B,B}_{1,1}(\mathfrak{a}).$$

Thus, we have

$$\log\big(U^B_{1,1}(\mathfrak{a})/U^{B,B}_{1,1}(\mathfrak{a})\big) = 0,$$

and so it follows from the definitions (3.12) and (3.13) that one has $\lambda^*(1,1;\tau)=0$, and hence $\lambda(1,1)=0$. This completes the proof of the lemma. □

6. Initial conditioning

We continue our campaign on the proof of Theorem 3.3 in the case $k \geqslant 2$, assuming its validity for exponents smaller than k. Our initial step is to bound $U_{s,k}^B(\mathfrak{a})$ in terms of a mean value of the shape $K_{a,b,c}^{\tau,\boldsymbol{\varphi},\nu}(\mathfrak{a})$. This section is devoted to the preliminary manoeuvres required for establishing such a bound. In this step, we encounter significant complications relative to the corresponding situation encountered in [11] when handling efficient congruencing over the simpler ring $\mathbb{Z}$. We note, in particular, that it is in this initial conditioning process that we are forced to make use of the Hypothesis 3.2.

Recall the definitions (3.12) and (3.13). We fix a prime p with $p>k$, also fix the parameter $s=k(k+1)/2$, and seek to establish that $\lambda(s,k)=0$. In order to confirm the latter, we proceed by deriving a contradiction to the assertion that $\lambda(s,k)=\Lambda>0$. In view of the upper bound (3.14), we may suppose throughout that

$$0<\Lambda\leqslant s. \tag{6.1}$$

Recall that we are implicitly assuming Hypothesis 3.2, which asserts, via the implicit reference to Hypothesis 3.1, that there exists a small positive number ω for which the conclusion of the hypothesis holds. The inductive argument calls for the assumption of this hypothesis in a nested form with a large, but finite, number of levels. We fix an admissible value for the smallest of the values ω that occur in this collection of levels, and introduce a heierarchy of sufficiently small positive numbers ε, τ, δ and μ with

$$\varepsilon<\tau<\delta<\mu<\omega<1. \tag{6.2}$$

We suppose that each element in the heierarchy is sufficiently small in terms of k, Λ and the larger elements of the heierarchy. Thus, for example, we are at liberty to assume that

$$\varepsilon<k\Lambda\omega/8. \tag{6.3}$$

By reference to the definition (3.13), there is no loss of generality in supposing that $\lambda^*(s,k;\tau)\geqslant\Lambda-\varepsilon/2$. By virtue of (3.12), there consequently exists a sequence $(B_m)_{m=1}^\infty$, with $B_m\to\infty$ as $m\to\infty$, having the property that whenever m is sufficiently large, there exists $\boldsymbol{\varphi}_m\in\Phi_\tau(B_m)$ and $(\mathfrak{a}^{(m)})\in\mathbb{D}(B_m)$ for which

$$U_{s,k}^{B_m}(\mathfrak{a}^{(m)})\geqslant(p^{2H_m})^{\Lambda-\varepsilon}U_{s,k}^{B_m,H_m}(\mathfrak{a}^{(m)}), \tag{6.4}$$

in which $H_m=\lceil B_m/k\rceil$. We now fix any such integer m having the property that $B=B_m$ is sufficiently large in terms of k, Λ, μ, δ, τ, ε and ω. We suppress the index m from this point on, so as to streamline our notation. We remark that since B is supposed to be sufficiently large in terms of the aforementioned collection of parameters, then we may suppose that εB is also sufficiently large with respect to the same set of parameters.

On recalling Lemma 4.4, we perceive that there is no loss of generality in supposing that, for every non-negative integer h with $h\leqslant(1-\delta)H$, uniformly in $\boldsymbol{\varphi}'\in\Phi_\tau(B)$ and $(\mathfrak{a}')\in\mathbb{D}_0(B)$, one has

$$U_{s,k}^{B,h}(\mathfrak{a}')\leqslant\big(p^{2(H-h)}\big)^{\lambda+\varepsilon}U_{s,k}^{B,H}(\mathfrak{a}'). \tag{6.5}$$

We are almost ready to announce our preliminary bound on $U_{s,k}^B(\mathfrak{a})$ in terms of mean values of the shape $K_{a,b,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a})$. Here, we fix a choice for the parameter ν for future use by setting

$$\nu = \lceil 8\varepsilon H/\Lambda \rceil. \tag{6.6}$$

Notice that the assumption (6.3) ensures that one then has $\nu < \lfloor \omega B \rfloor$. Since we may suppose that $\boldsymbol{\varphi} \in \Phi_\tau(B)$, it follows that there exists an integer c with $c \geqslant \tau B$ having the property that $\boldsymbol{\varphi}$ is p^c-spaced.

We first prepare an auxiliary estimate for a mean value associated with the exponential sum

$$T_1(\boldsymbol{\alpha}) = \rho_0(1)^{-2s} \sum_{\zeta=1}^{p^\nu} \Big| \sum_{\substack{\xi \pmod{(p^\nu,t^2)} \\ \xi \equiv \zeta \pmod{(p^\nu,t)}}} \rho_\nu(\xi) \mathfrak{f}_\nu(\boldsymbol{\alpha};\xi) \Big|^{2s}.$$

Lemma 6.1. *One has*

$$\oint_{p^B} T_1(\boldsymbol{\alpha})\, \mathrm{d}\boldsymbol{\alpha} \ll p^{s\nu\varepsilon} U_{s,k}^{B,\nu}(\mathfrak{a}).$$

Proof. We begin by examining the mean value

$$\oint_{p^B} \Big| \sum_{\substack{\xi \pmod{(p^\nu,t^2)} \\ \xi \equiv \zeta \pmod{(p^\nu,t)}}} \rho_\nu(\xi) \mathfrak{f}_\nu(\boldsymbol{\alpha};\xi) \Big|^{2s} \mathrm{d}\boldsymbol{\alpha} = \sum_{\boldsymbol{\xi}} I(\boldsymbol{\xi}) \prod_{i=1}^{2s} \rho_\nu(\xi_i),$$

where

$$I(\boldsymbol{\xi}) = \oint_{p^B} \prod_{i=1}^{s} \mathfrak{f}_\nu(\boldsymbol{\alpha};\xi_i) \overline{\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi_{s+i})}\, \mathrm{d}\boldsymbol{\alpha}.$$

Here, the summation over $\boldsymbol{\xi}$ is taken over ξ_i modulo (p^ν,t^2) with $\xi_i \equiv \zeta \pmod{(p^\nu,t)}$ for $1 \leqslant i \leqslant 2s$. The mean value $I(\boldsymbol{\xi})$ counts the solutions of the simultaneous congruences (3.7) with $\mathbf{x},\mathbf{y} \in \mathfrak{Z}(t^2)$ satisfying the congruence conditions

$$x_i \equiv \xi_i \pmod{(p^\nu,t^2)} \quad \text{and} \quad y_i \equiv \xi_{s+i} \pmod{(p^\nu,t^2)} \quad (1 \leqslant i \leqslant s),$$

and with each solution counted with weight

$$\Big(\prod_{i=1}^{s} \rho_\nu(\xi_i)^{-1} \mathfrak{a}_{x_i} \Big) \Big(\prod_{i=1}^{s} \rho_\nu(\xi_{s+i})^{-1} \overline{\mathfrak{a}}_{y_i} \Big).$$

Observe that $\boldsymbol{\varphi}$ is a p^c-spaced system, so it follows as in the argument of the proof of Lemma 4.4 leading to (4.6) that, in the first instance, there is no loss of generality in supposing that

$$\varphi_j(u) = u^j + u^{k+1}\big(p^c \psi_j(u) + t\chi_j(u)\big) \quad (1 \leqslant j \leqslant k),$$

for appropriate polynomials $\psi_j(u), \chi_j(u) \in \mathbb{Z}[t,u]$. Our assumptions on ν ensure that ν is small compared to c. Thus, it follows from the congruence in (3.7) corresponding to $j = 1$ that

$$\sum_{i=1}^{s} \varphi_1^*(x_i) \equiv \sum_{i=1}^{s} \varphi_1^*(x_{s+i}) \pmod{(p^\nu,t^2)},$$

in which we have written

$$\varphi_1^*(u) = u + tu^{k+1}\chi_1(u).$$

Consequently, one has a solution of (3.7) to be counted by the mean value $I(\boldsymbol{\xi})$ only when

$$\sum_{i=1}^{s}\big(\varphi_1^*(\xi_i) - \varphi_1^*(\xi_{s+i})\big) \equiv 0 \ (\mathrm{mod}\ (p^\nu, t^2)).$$

Note here that for $1 \leqslant i \leqslant 2s$, one has $\xi_i \equiv \zeta \ (\mathrm{mod}\ (p^\nu, t))$, and thus

$$\varphi_1^*(\xi_i) \equiv \xi_i + t\zeta^{k+1}\chi_1(\zeta) \ (\mathrm{mod}\ (p^\nu, t^2)).$$

Then we may conclude that one has a solution of (3.7) to be counted by $I(\boldsymbol{\xi})$ only when

$$\sum_{i=1}^{s}\big(\xi_i - \xi_{s+i}\big) \equiv 0 \ (\mathrm{mod}\ (p^\nu, t^2)). \tag{6.7}$$

Recalling again that for $1 \leqslant i \leqslant 2s$, we have $\xi_i \equiv \zeta \ (\mathrm{mod}\ (p^\nu, t))$, we note that the congruence (6.7) serves only to constrain the congruence classes of the coefficients of t in the variables ξ_i.

Working backwards from orthogonality, we may incorporate the condition (6.7) into the mean value to be estimated. Here, it is useful to observe that when $I(\boldsymbol{\xi})$ is non-zero, it follows from the elementary inequality $|z_1 \cdots z_n| \leqslant |z_1|^n + \ldots + |z_n|^n$ that

$$I(\boldsymbol{\xi})\prod_{i=1}^{2s}\rho_\nu(\xi_i) \leqslant \sum_{i=1}^{2s}\oint_{p^B}|\widetilde{\rho}_{\nu,i}(\boldsymbol{\xi})\widetilde{\mathfrak{f}}_{\nu,i}(\boldsymbol{\alpha};\boldsymbol{\xi})|^{2s/(2s-1)},$$

where

$$\widetilde{\rho}_{\nu,i}(\boldsymbol{\xi}) = \prod_{\substack{1\leqslant j\leqslant 2s\\ j\neq i}}\rho_\nu(\xi_j) \quad \text{and} \quad \widetilde{\mathfrak{f}}_{\nu,i}(\boldsymbol{\alpha};\boldsymbol{\xi}) = \prod_{\substack{1\leqslant j\leqslant 2s\\ j\neq i}}\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi_j).$$

Thus, we infer that

$$\begin{aligned}\oint_{p^B}\Big|\sum_{\substack{\xi \ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta \ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)\Big|^{2s}\,\mathrm{d}\boldsymbol{\alpha}&\\ \leqslant \sum_{i=1}^{2s}\sum_{\substack{\boldsymbol{\xi} \ (\mathrm{mod}\ (p^\nu,t^2))\\ \boldsymbol{\xi}\equiv\zeta \ (\mathrm{mod}\ (p^\nu,t))\\ \xi_1+\ldots+\xi_s\equiv\xi_{s+1}+\ldots+\xi_{2s} \ (\mathrm{mod}\ (p^\nu,t^2))}}&\oint_{p^B}|\widetilde{\rho}_{\nu,i}(\boldsymbol{\xi})\widetilde{\mathfrak{f}}_{\nu,i}(\boldsymbol{\alpha};\boldsymbol{\xi})|^{2s/(2s-1)}\,\mathrm{d}\boldsymbol{\alpha}.\end{aligned}$$

By fixing the residue class of any ξ_j modulo (p^ν, t) for $2s-1$ distinct choices of j with $1 \leqslant j \leqslant 2s$, the final class is fixed within the summation over $\boldsymbol{\xi}$. Thus, on employing

symmetry amongst the indices, we see that

$$\oint_{p^B}\Big|\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)\Big|^{2s}\,\mathrm{d}\boldsymbol{\alpha}$$
$$\ll\oint_{p^B}\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}|\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s/(2s-1)}\Big)^{2s-1}\,\mathrm{d}\boldsymbol{\alpha}.\tag{6.8}$$

By applying Hölder's inequality, we find that

$$\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}|\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s/(2s-1)}\Big)^{2s-1}$$
$$\leqslant\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)\Big)^{2s-2}\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)^2|\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s}\Big).$$

It is at this point that we make use of Hypothesis 3.1. By making use of the latter in combination with (3.2) and Cauchy's inequality, we see that

$$\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)\Big)^2\leqslant p^\nu\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)^2$$
$$=p^\nu\sum_{\eta_1=1}^{p^\nu}\|\mathfrak{a}_\nu(\zeta+\eta_1t)\|_0\cdot\|\mathfrak{a}_\nu(\zeta+\eta_1t)\|_\infty^2$$
$$\ll p^{\nu\varepsilon}\|\mathfrak{a}_0(1)\|_\infty^2\sum_{\eta_0=1}^{p^\nu}\sum_{\eta_1=1}^{p^\nu}\|\mathfrak{a}_\nu(\eta_0+\eta_1t)\|_0.$$

Thus, we infer that

$$\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)\Big)^2\ll p^{\nu\varepsilon}\|\mathfrak{a}_0(1)\|_\infty^2\cdot\|\mathfrak{a}_0(1)\|_0=p^{\nu\varepsilon}\rho_0(1)^2,$$

whence

$$\Big(\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}|\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s/(2s-1)}\Big)^{2s-1}$$
$$\ll\big(p^{\nu\varepsilon}\rho_0(1)^2\big)^{s-1}\sum_{\substack{\xi\ (\mathrm{mod}\ (p^\nu,t^2))\\ \xi\equiv\zeta\ (\mathrm{mod}\ (p^\nu,t))}}\rho_\nu(\xi)^2|\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s}.$$

By substituting this last upper bound into (6.8), we arrive at the estimate

$$\sum_{\zeta=1}^{p^\nu}\oint_{p^B}\Big|\sum_{\substack{\xi \pmod{(p^\nu,t^2)}\\ \xi\equiv\zeta \pmod{(p^\nu,t)}}}\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)\Big|^{2s}\,\mathrm{d}\boldsymbol{\alpha}$$
$$\ll p^{s\nu\varepsilon}\rho_0(1)^{2s-2}\sum_{\xi \pmod{(p^\nu,t^2)}}\rho_\nu(\xi)^2\oint_{p^B}|\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}.$$

On recalling the definition of $T_1(\boldsymbol{\alpha})$ together with (3.8), we therefore conclude that

$$\oint_{p^B}T_1(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}\ll p^{s\nu\varepsilon}\rho_0(1)^{-2}\sum_{\xi \pmod{(p^\nu,t^2)}}\rho_\nu(\xi)^2\oint_{p^B}|\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}=p^{s\nu\varepsilon}U_{s,k}^{B,\nu}(\mathfrak{a}).$$

This completes the proof of the lemma. □

We are now equipped to establish the first of our conditioning lemmata.

Lemma 6.2. *One has* $U_{s,k}^B(\mathfrak{a})\ll(p^{2\nu})^sK_{\nu,\nu,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a})$.

Proof. Using the definition of $f_{\mathfrak{a}}(\boldsymbol{\alpha})$ and the definition (3.4), one sees that

$$\rho_0(1)^{2s}f_{\mathfrak{a}}(\boldsymbol{\alpha})^{2s}=\sum_{\xi \pmod{(p^\nu,t^2)}}\rho_\nu(\xi)\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)\big(\rho_0(1)\mathfrak{f}_{\mathfrak{a}}(\boldsymbol{\alpha})\big)^{2s-1}.\tag{6.9}$$

Moreover, for each residue ξ modulo (p^ν,t^2), one has

$$\rho_0(1)f_{\mathfrak{a}}(\boldsymbol{\alpha})=\sum_{\substack{\eta \pmod{(p^\nu,t^2)}\\ \eta\equiv\xi \pmod{(p^\nu,t)}}}\rho_\nu(\eta)\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)+\sum_{\substack{\eta \pmod{(p^\nu,t^2)}\\ \eta\not\equiv\xi \pmod{(p^\nu,t)}}}\rho_\nu(\eta)\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta),\tag{6.10}$$

whence

$$|\rho_0(1)f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s-1}\ll\Big|\sum_{\substack{\eta \pmod{(p^\nu,t^2)}\\ \eta\equiv\xi \pmod{(p^\nu,t)}}}\rho_\nu(\eta)\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)\Big|^{2s-1}+\Big|\sum_{\substack{\eta \pmod{(p^\nu,t^2)}\\ \eta\not\equiv\xi \pmod{(p^\nu,t)}}}\rho_\nu(\eta)\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)\Big|^{2s-1}.\tag{6.11}$$

By substituting (6.11) into (6.9) and recalling the definition of $T_1(\boldsymbol{\alpha})$ from the preamble to Lemma 6.1, we arrive at the relation

$$|f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s}\ll T_1(\boldsymbol{\alpha})+T_2(\boldsymbol{\alpha}),\tag{6.12}$$

where

$$T_2(\boldsymbol{\alpha})=\rho_0(1)^{-2s}\sum_{\xi \pmod{(p^\nu,t^2)}}\rho_\nu(\xi)|\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|\,\Big|\sum_{\substack{\eta \pmod{(p^\nu,t^2)}\\ \eta\not\equiv\xi \pmod{(p^\nu,t)}}}\rho_\nu(\eta)\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)\Big|^{2s-1}.\tag{6.13}$$

We must double up the number of generating functions $\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)$ in the mean value augured by (6.13). This we achieve with a swift application of Cauchy's inequality, obtaining the bound

$$T_2(\boldsymbol{\alpha})\leqslant T_3(\boldsymbol{\alpha})^{1/2}T_4(\boldsymbol{\alpha})^{1/2},\tag{6.14}$$

where

$$T_3(\boldsymbol{\alpha}) = \rho_0(1)^{-2s} \sum_{\xi \pmod{(p^\nu,t^2)}} \rho_\nu(\xi)^2 |\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^2 \Big| \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta) \mathfrak{f}_\nu(\boldsymbol{\alpha};\eta) \Big|^{2s-2} \tag{6.15}$$

and

$$T_4(\boldsymbol{\alpha}) = \rho_0(1)^{-2s} \sum_{\xi \pmod{(p^\nu,t^2)}} \Big| \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta) \mathfrak{f}_\nu(\boldsymbol{\alpha};\eta) \Big|^{2s}. \tag{6.16}$$

We next analyse the expression $T_4(\boldsymbol{\alpha})$, first removing the awkward summation restriction $\eta \not\equiv \xi \pmod{(p^\nu,t)}$. Thus, reversing the relation (6.10), we see that

$$\Big| \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta) \mathfrak{f}_\nu(\boldsymbol{\alpha};\eta) \Big|^{2s} \ll |\rho_0(1) f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s} + \Big| \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta) \mathfrak{f}_\nu(\boldsymbol{\alpha};\eta) \Big|^{2s}.$$

Hence, we see from (6.16) and the preamble to Lemma 6.1 that

$$T_4(\boldsymbol{\alpha}) \ll \sum_{\xi \pmod{(p^\nu,t^2)}} |f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s} + p^\nu T_1(\boldsymbol{\alpha}),$$

whence, as a consequence of (3.6) and Lemma 6.1,

$$\oint_{p^B} T_4(\boldsymbol{\alpha}) \, \mathrm{d}\boldsymbol{\alpha} \ll p^{2\nu} U_{s,k}^B(\mathfrak{a}) + p^{\nu + s\nu\varepsilon} U_{s,k}^{B,\nu}(\mathfrak{a}). \tag{6.17}$$

Next, we find through an application of Hölder's inequality that

$$\begin{aligned}
&\Big| \sum_{\substack{\eta \pmod{(p^\nu.t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta) \mathfrak{f}_\nu(\boldsymbol{\alpha};\eta) \Big|^{2s-2} \\
&\leqslant \Big(\sum_{\eta \pmod{(p^\nu,t^2)}} \rho_\nu(\eta)^2 \Big)^{s-2} \Big(\sum_{\eta \pmod{(p^\nu,t^2)}} 1 \Big)^{s-1} \Big(\sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta)^2 |\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)|^{2s-2} \Big) \\
&\leqslant \rho_0(1)^{2s-4} (p^{2\nu})^{s-1} \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\eta)^2 |\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)|^{2s-2}.
\end{aligned}$$

Then we deduce from (6.15) that

$$T_3(\boldsymbol{\alpha}) \leqslant \rho_0(1)^{-4} (p^{2\nu})^{s-1} \sum_{\xi \pmod{(p^\nu,t^2)}} \sum_{\substack{\eta \pmod{(p^\nu,t^2)} \\ \eta \not\equiv \xi \pmod{(p^\nu,t)}}} \rho_\nu(\xi)^2 \rho_\nu(\eta)^2 |\mathfrak{f}_\nu(\boldsymbol{\alpha};\xi)|^2 |\mathfrak{f}_\nu(\boldsymbol{\alpha};\eta)|^{2s-2}.$$

We therefore conclude from (3.16) that

$$\oint_{p^B} T_3(\boldsymbol{\alpha}) \, \mathrm{d}\boldsymbol{\alpha} \leqslant (p^{2\nu})^{s-1} K_{\nu,\nu,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a}). \tag{6.18}$$

On substituting (6.17) and (6.18) into (6.14), we find via Schwarz's inequality that

$$\begin{aligned}\oint_{p^B} T_2(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} &\leqslant \biggl(\oint_{p^B} T_3(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}\biggr)^{1/2}\biggl(\oint_{p^B} T_4(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}\biggr)^{1/2}\\ &\ll \bigl((p^{2\nu})^{s-1}K^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})\bigr)^{1/2}\bigl(p^{2\nu}U^B_{s,k}(\mathfrak{a})+p^{\nu+s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})\bigr)^{1/2}.\end{aligned}$$

Consequently, on recalling Lemma 6.1 and (6.12), we obtain the upper bound

$$\begin{aligned}\oint_{p^B} |f_{\mathfrak{a}}(\boldsymbol{\alpha})|^{2s}\,\mathrm{d}\boldsymbol{\alpha} &\ll \oint_{p^B} T_1(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}+\oint_{p^B} T_2(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}\\ &\ll p^{s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})+(p^{\nu})^{s-1}\bigl(K^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})\bigr)^{1/2}\bigl(p^{2\nu}U^B_{s,k}(\mathfrak{a})+p^{\nu+s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})\bigr)^{1/2}.\end{aligned}$$

Thus, from (3.6), we deduce that

$$U^B_{s,k}(\mathfrak{a})\ll p^{s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})+(p^{\nu})^{s-1}\bigl(K^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})\bigr)^{1/2}\bigl(p^{2\nu}U^B_{s,k}(\mathfrak{a})+p^{\nu+s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})\bigr)^{1/2},$$

whence

$$\begin{aligned}U^B_{s,k}(\mathfrak{a}) &\ll p^{s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})+(p^{2\nu})^sK^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})+(p^{\nu})^{s-1}\bigl(K^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})\bigr)^{1/2}\bigl(p^{\nu+s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})\bigr)^{1/2}\\ &\ll p^{s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})+(p^{2\nu})^sK^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a}).\end{aligned}\tag{6.19}$$

We now make use of the estimate (6.5) to obtain the bound

$$U^{B,\nu}_{s,k}(\mathfrak{a})\leqslant\bigl(p^{2(H-\nu)}\bigr)^{\Lambda+\varepsilon}U^{B,H}_{s,k}(\mathfrak{a}).$$

Since the definition (6.6) ensures that

$$s\nu\varepsilon+2(\Lambda+\varepsilon)(H-\nu)-2(\Lambda-\varepsilon)H<4\varepsilon H-(2\Lambda-s\varepsilon)\nu<-4\varepsilon H,$$

we discern via (6.4) that

$$p^{s\nu\varepsilon}U^{B,\nu}_{s,k}(\mathfrak{a})\leqslant p^{-4\varepsilon H}(p^{2H})^{\Lambda-\varepsilon}U^{B,H}_{s,k}(\mathfrak{a})\leqslant p^{-4\varepsilon H}U^B_{s,k}(\mathfrak{a}).$$

Thus, we infer from (6.19) that

$$U^B_{s,k}(\mathfrak{a})\ll p^{-4\varepsilon H}U^B_{s,k}(\mathfrak{a})+(p^{2\nu})^sK^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a}),$$

whence

$$U^B_{s,k}(\mathfrak{a})\ll(p^{2\nu})^sK^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a}).$$

This completes the proof of the lemma. □

We amplify the congruence condition implicit in the mean value $K^{1,\boldsymbol{\varphi},\nu}_{\nu,\nu,c}(\mathfrak{a})$ in order to gain sufficient traction to pursue our main iteration. At this point, we introduce the last of our small quantities, namely the parameter θ, defined by putting

$$\theta=\lceil\mu H\rceil.\tag{6.20}$$

An essentially trivial bound presented in the next lemma eases our discussion.

Lemma 6.3. *Suppose that a and b are non-negative integers with $a\leqslant b$. Then for any positive number w and any $\xi\in\mathbb{Z}[t]$, one has*

$$\rho_a(\xi)^2|\mathfrak{f}_a(\boldsymbol{\alpha};\xi)|^{2w}\leqslant(p^{2b-2a})^w\sum_{\substack{\zeta\ (\mathrm{mod}\ (p^b,t^2))\\ \zeta\equiv\xi\ (\mathrm{mod}\ (p^a,t^2))}}\rho_b(\zeta)^2|\mathfrak{f}_b(\boldsymbol{\alpha};\zeta)|^{2w}.$$

Proof. By applying Hölder's inequality together with (3.4), we see that

$$\rho_a(\xi)^{2w}|\mathfrak{f}_a(\boldsymbol{\alpha};\xi)|^{2w} = \Big| \sum_{\substack{\zeta \pmod{(p^b,t^2)}\\ \zeta\equiv\xi \pmod{(p^a,t^2)}}} \rho_b(\zeta)\mathfrak{f}_b(\boldsymbol{\alpha};\zeta)\Big|^{2w}$$
$$\leqslant V_1^w V_2^{w-1} \sum_{\substack{\zeta \pmod{(p^b,t^2)}\\ \zeta\equiv\xi \pmod{(p^a,t^2)}}} \rho_b(\zeta)^2|\mathfrak{f}_b(\boldsymbol{\alpha};\zeta)|^{2w}, \tag{6.21}$$

where

$$V_1 = \sum_{\substack{\zeta \pmod{(p^b,t^2)}\\ \zeta\equiv\xi \pmod{(p^a,t^2)}}} 1 \quad \text{and} \quad V_2 = \sum_{\substack{\zeta \pmod{(p^b,t^2)}\\ \zeta\equiv\xi \pmod{(p^a,t^2)}}} \rho_b(\zeta)^2.$$

However, we have $V_1 = p^{2b-2a}$, and in view of the definition (3.2),

$$V_2 \leqslant \|\mathfrak{a}_a(\xi)\|_\infty^2 \sum_{\substack{\zeta \pmod{(p^b,t^2)}\\ \zeta\equiv\xi \pmod{(p^a,t^2)}}} \|\mathfrak{a}_b(\zeta)\|_0 \leqslant \|\mathfrak{a}_a(\xi)\|_\infty^2 \cdot \|\mathfrak{a}_a(\xi)\|_0 = \rho_a(\xi)^2.$$

The conclusion of the lemma follows on substituting these relations into (6.21). □

We at last reach the primary objective of this section.

Lemma 6.4. *One has* $U_{s,k}^B(\mathfrak{a}) \ll p^{2s\theta} K_{\theta,\theta,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a})$.

Proof. By appealing to (3.17), we find via two applications of Lemma 6.3 that

$$\rho_\nu(\xi)^2\rho_\nu(\eta)^2 K_{\nu,\nu,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta)$$
$$\leqslant (p^{2\theta-2\nu})^s \sum_{\xi',\eta' \pmod{(p^\theta,t^2)}} \oint_{p^B} \rho_\theta(\xi')^2\rho_\theta(\eta')^2|\mathfrak{f}_\theta(\boldsymbol{\alpha};\xi')^2\mathfrak{f}_\theta(\boldsymbol{\alpha};\eta')^{2s-2}|\,\mathrm{d}\boldsymbol{\alpha},$$

where the summation over ξ' and η' is subject to the conditions

$$\xi' \equiv \xi \pmod{p^\nu} \quad \text{and} \quad \eta' \equiv \eta \pmod{p^\nu}.$$

We therefore deduce from (3.16) that

$$K_{\nu,\nu,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a}) \leqslant \rho_0(1)^{-4}(p^{2\theta-2\nu})^s \sum_{\xi' \pmod{(p^\theta,t^2)}} \sum_{\substack{\eta' \pmod{(p^\theta,t^2)}\\ \eta'\not\equiv\xi' \pmod{(p^\nu,t)}}} \rho_\theta(\xi')^2\rho_\theta(\eta')^2 K_{\theta,\theta,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi',\eta')$$
$$= (p^{2\theta-2\nu})^s K_{\theta,\theta,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a}).$$

Therefore, by substituting this bound into the estimate supplied by Lemma 6.2, we obtain

$$U_{s,k}^B(\mathfrak{a}) \ll (p^{2\theta-2\nu})^s (p^{2\nu})^s K_{\theta,\theta,c}^{1,\boldsymbol{\varphi},\nu}(\mathfrak{a}).$$

The conclusion of the lemma follows. □

7. Congruencing operations

Throughout, we suppose that $k \geqslant 2$, and we assume the validity of Theorem 3.3 for exponents smaller than k. We continue to make use of the conventions of the previous section, and in particular we write $R = r(r+1)/2$.

Lemma 7.1. *Suppose that a, b and r are integers with*

$$1 \leqslant r \leqslant k-1, \quad a \geqslant \delta\theta, \quad b \geqslant \delta\theta \quad \text{and} \quad ra \leqslant (k-r+1)b \leqslant B. \tag{7.1}$$

Put

$$b' = \lceil (k-r+1)b/r \rceil. \tag{7.2}$$

Then one has

$$K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a}) \ll \big(p^{2\nu}\big)^{2k^2} K^{r,\boldsymbol{\varphi},\nu}_{b',b,c}(\mathfrak{a}).$$

Proof. The essential strategy of the proof of this lemma follows the plan adopted in the corresponding proof of [11, Lemma 7.1]. However, the fact that we are now working in $\mathbb{Z}[t]/(p^B, t^2)$ in place of $\mathbb{Z}$ leads to significant complications that warrant a detailed account. We begin by examining the definition (3.16) of the mean value $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)$, in which we suppose that $\eta \not\equiv \xi \pmod{(p^\nu, t)}$. The latter condition offers us permission to assume that for some non-negative integer γ with $\gamma < \nu$, one has

$$\xi \equiv \eta \pmod{(p^\gamma, t)} \quad \text{and} \quad \xi \not\equiv \eta \pmod{(p^{\gamma+1}, t)}.$$

Write $\xi = \xi_0 + \xi_1 t$ and $\eta = \eta_0 + \eta_1 t$ with $\xi_i, \eta_i \in \mathbb{Z}$. We define the integer ω by putting $\omega = (\xi_0 - \eta_0)p^{-\gamma}$, so that $(\omega, p) = 1$. It is convenient for future use to introduce the parameter

$$B' = (k-r+1)b - ra - 2(k-r)\gamma. \tag{7.3}$$

We find it useful to provide sufficient room in which to work, and therefore explore the contrary situation in which $B' \leqslant \nu$. In such circumstances, we find from (7.3) that

$$(k-r+1)b - ra \leqslant \nu + 2(k-r)\gamma \leqslant 2k\nu.$$

In view of the definition (7.2), we then have

$$b' - a \leqslant 1 + 2k\nu/r. \tag{7.4}$$

Moreover, an application of Lemma 6.3 delivers the bound

$$\rho_a(\xi)^2 |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)|^{2R} \leqslant (p^{2b'-2a})^R \sum_{\substack{\zeta \pmod{(p^{b'},t^2)} \\ \zeta \equiv \xi \pmod{(p^a,t^2)}}} \rho_{b'}(\zeta)^2 |\mathfrak{f}_{b'}(\boldsymbol{\alpha};\zeta)|^{2R}.$$

Since we have $R = r(r+1)/2 < kr/2$, we deduce from (7.4), (3.16) and (3.17) that

$$K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a}) \leqslant (p^{2\nu})^{2k^2} K^{r,\boldsymbol{\varphi},\nu}_{b',b,c}(\mathfrak{a}).$$

This bound establishes the conclusion of the lemma when $B' \leqslant \nu$.

We now turn to address the situation in which

$$B' > \nu. \tag{7.5}$$

Recall that, by orthogonality and the definition (3.17), the mean value $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)$ counts the solutions in $\mathfrak{Z}(t^2)$ of the simultaneous congruences (3.18), with the accompanying conditions (3.19), and with each solution being counted with the weight (3.20). In

the first phase of our argument, we seek to extract from these congruences an underlying additional congruence condition on a subset of the variables that may subsequently be exploited.

We begin by examining the right hand side of the system (3.18). Observe that $\boldsymbol{\varphi}$ is a p^c-spaced system, so it follows as in the argument of the proof of Lemma 4.4 leading to (4.6) that there is no loss of generality in supposing that

$$\varphi_j(u) = u^j + u^{k+1}\big(p^c\psi_j(u) + t\chi_j(u)\big) \quad (1 \leqslant j \leqslant k),$$

for appropriate polynomials $\psi_j(u), \chi_j(u) \in \mathbb{Z}[t,u]$. In view of (3.19), we may substitute

$$v_l = p^b u_l + \eta \quad \text{and} \quad w_l = p^b z_l + \eta \quad (1 \leqslant l \leqslant s-R),$$

and then (3.18) is transformed into the new system

$$\sum_{i=1}^{R}\big(\varphi_j(x_i)-\varphi_j(y_i)\big) \equiv \sum_{l=1}^{s-R}\big(\varphi_j(p^bu_l+\eta)-\varphi_j(p^bz_l+\eta)\big) \pmod{(p^B,t^2)} \quad (1 \leqslant j \leqslant k). \tag{7.6}$$

Next, as in the argument of the proof of Lemma 4.4 leading from (4.6) to (4.7) and (4.8), we may take appropriate integral linear combinations of the congruences comprising (7.6) to deduce that there exist polynomials $\Upsilon_j(u), \Theta_j(u) \in \mathbb{Z}[t,u]$ for which

$$\sum_{i=1}^{R}\big(\Phi_j(x_i-\eta)-\Phi_j(y_i-\eta)\big) \equiv \sum_{l=1}^{s-R}\big(\Phi_j(p^bu_l)-\Phi_j(p^bz_l)\big) \pmod{(p^B,t^2)} \quad (1 \leqslant j \leqslant k),$$

in which

$$\Phi_j(u) = u^j + u^{k+1}\big(p^c\Upsilon_j(u) + t\Theta_j(u)\big). \tag{7.7}$$

In particular, the system $\boldsymbol{\Phi}$ is p^c-spaced, and one has

$$\sum_{i=1}^{R}\Phi_j(x_i-\eta) \equiv \sum_{i=1}^{R}\Phi_j(y_i-\eta) \pmod{(p^{jb},p^B,t^2)} \quad (1 \leqslant j \leqslant k). \tag{7.8}$$

Our next step is to extract from (7.8) a system related to the Vinogradov systems central to this memoir. Of necessity, we recycle variable names despite the risk of confusion. Recall from (3.20) that in the solutions of (3.19) of interest to us, we have

$$\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{(p^a,t^2)}.$$

Then we may substitute

$$x_i \equiv p^au_i + \xi \pmod{(p^B,t^2)} \quad \text{and} \quad y_i \equiv p^az_i + \xi \pmod{(p^B,t^2)} \quad (1 \leqslant i \leqslant R). \tag{7.9}$$

We can say more concerning the element $\xi - \eta \in \mathbb{Z}[t]/(p^B,t^2)$ implicit in (7.8). We recall that $\xi = \xi_0 + \xi_1 t$ and $\eta = \eta_0 + \eta_1 t$ with $\xi_0 - \eta_0 = \omega p^\gamma$, and that we may suppose that $B \geqslant (k-r+1)b$. Then by ignoring in (7.8) those congruences with index j satisfying $1 \leqslant j \leqslant k-r$, and substituting (7.9) into (7.8), we find that for $k-r+1 \leqslant j \leqslant k$, one has

$$\sum_{i=1}^{R}\Phi_j\big(p^au_i+\omega p^\gamma+(\xi_1-\eta_1)t\big) \equiv \sum_{i=1}^{R}\Phi_j\big(p^az_i+\omega p^\gamma+(\xi_1-\eta_1)t\big) \pmod{(p^{(k-r+1)b},t^2)}. \tag{7.10}$$

Just as in the corresponding argument in the proof of [11, Lemma 7.1], the system (7.10) can be analysed by using an argument paralleling that leading from (4.6) to (4.7)

and (4.8). We apply the binomial theorem within (7.7). Thus, when $1 \leqslant l \leqslant r$, we find that for suitable polynomials $\Gamma_l(u) \in \mathbb{Z}[t,u]$, one has

$$\Phi_{k-r+l}\big(p^a y + \omega p^\gamma + (\xi_1 - \eta_1)t\big) - \Phi_{k-r+l}\big(\omega p^\gamma + (\xi_1 - \eta_1)t\big) = \mathrm{H}_l(p^a y),$$

in which

$$\mathrm{H}_l(u) = \sum_{i=1}^{r} \Omega_{il}\big(\omega p^\gamma + (\xi_1 - \eta_1)t\big)^{k-r+l-i} u^i + u^{r+1}\Gamma_l(u), \tag{7.11}$$

and the $\mathbb{Z}[t]$-coefficients Ω_{il} satisfy the congruences

$$\Omega_{il} \equiv \binom{k-r+l}{i} \pmod{(p^c,t)} \quad (1 \leqslant i,l \leqslant r).$$

As in the argument of the proof of [8, Lemma 3.2], our hypothesis $p > k$ ensures that the matrix $A = (\Omega_{il})_{1\leqslant i,l\leqslant r}$ satisfies the property that $\det(A) \not\equiv 0 \pmod{(p,t)}$. It follows that A possesses an approximate multiplicative inverse A_0^{-1} modulo (p,t) having coefficients in $\mathbb{Z}$ with the property that $A_0^{-1}A \equiv I_r \pmod{(p,t)}$. We replace $\mathbf{\Phi}$ by $A_0^{-1}\mathbf{\Phi}$, and likewise $\mathbf{\Gamma}$ by $A_0^{-1}\mathbf{\Gamma}$. This transformation once again corresponds to taking linear combinations of the congruences comprising (7.10). In this way, we find that there is no loss of generality in supposing that $\mathbf{H}$ takes the shape defined by (7.11), but with $A = (\Omega_{il})_{1\leqslant i,l\leqslant r}$ constrained to satisfy $A \equiv I_r \pmod{(p,t)}$. We therefore infer from Lemma 4.2 that this new matrix A possesses a multiplicative inverse A^{-1} modulo $(p^{(k-r+1)b}, t^2)$ having coefficients in $\mathbb{Z}[t]/(p^B, t^2)$.

We now replace $\mathbf{\Phi}$ by $A^{-1}\mathbf{\Phi}$, and likewise $\mathbf{\Gamma}$ by $A^{-1}\mathbf{\Gamma}$. This, yet again, amounts to taking suitable linear combinations of the congruences comprising (7.10). In this way, one sees that there is no loss of generality in supposing that the coefficient matrix A is equal to I_r. Since $(\omega, p) = 1$, moreover, there exists an integral multiplicative inverse ω^{-1} for ω modulo $p^{(k-r+1)b}$. This observation, in turn, implies that

$$\begin{aligned}\big((\omega^{-1})^2(\omega p^\gamma - (\xi_1 - \eta_1)t)\big)\big(\omega p^\gamma + (\xi_1 - \eta_1)t\big) &= \omega^{-2}\big(\omega^2 p^{2\gamma} - (\xi_1 - \eta_1)^2 t^2\big)\\ &\equiv p^{2\gamma} \pmod{(p^{(k-r+1)b}, t^2)}.\end{aligned}$$

Consequently, there exist polynomials $\Delta_l \in \mathbb{Z}[t,u]$ having the property that whenever the system (7.10) is satisfied, then

$$(p^{2\gamma})^{k-r} \sum_{i=1}^{R} (p^a)^l \big(\Psi_l(u_i) - \Psi_l(z_i)\big) \equiv 0 \pmod{(p^{(k-r+1)b}, t^2)} \quad (1 \leqslant l \leqslant r),$$

in which

$$\Psi_l(u) = u^l + p^{a-2(k-r)\gamma}\Delta_l(u). \tag{7.12}$$

Notice here that, since we may suppose from (7.1) that $a \geqslant \delta\theta$ and $\gamma \leqslant \nu$, our hypotheses concerning the heierarchy (6.2) combines with (6.6) and (6.20) to give

$$2k\gamma \leqslant 2k\lceil 8\varepsilon H\Lambda^{-1}\rceil < \delta^2\lceil \mu H\rceil \leqslant \delta a,$$

whence

$$a - 2(k-r)\gamma > (1-\delta)a \geqslant \delta(1-\delta)\mu H > \tau B.$$

We therefore perceive that the exponent of p on the right hand side of (7.12) is positive, and moreover the system $\mathbf{\Psi}$ is p^c-spaced for some $c > \tau(k-r+1)b$.

The discussion thus far shows that the $\mathfrak{Z}(t^2)$-solutions $\mathbf{x} = p^a\mathbf{u}+\xi$, $\mathbf{y} = p^a\mathbf{z}+\xi$, $\mathbf{v}$, $\mathbf{w}$ of the original system of congruences (3.18), counted with weight (3.20) associated with the definition (3.17) of $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)$, are constrained by the additional system of congruences

$$\sum_{i=1}^{R}\Psi_l(u_i) \equiv \sum_{i=1}^{R}\Psi_l(z_i) \pmod{(p^{B'},t^2)} \quad (1 \leqslant l \leqslant r), \tag{7.13}$$

in which B' is defined via (7.3). In the final phase of our argument, our goal is to apply the grand inductive hypothesis, by which we mean the conclusion of Theorem 3.3 with k replaced by r, so as to extract congruence information from the relations (7.13).

Recall that in view of (7.5), one has $B' > \nu$, and write $H' = \lceil B'/r\rceil$. In view of (7.2) and (7.3), one has

$$b' - H' \leqslant a + 1 + 2(k-r)\gamma/r. \tag{7.14}$$

From (6.6), moreover, we have $B' > \nu \geqslant 8\varepsilon H\Lambda^{-1}$. Thus, our hypotheses concerning B and the heierarchy (6.2) ensure that B' is sufficiently large in terms of k, Λ, μ, τ, δ and ε. We construe the definition (3.4) of $\mathfrak{f}_h(\boldsymbol{\alpha};\xi)$ in the form (4.2), so that

$$\mathfrak{f}_a(\boldsymbol{\alpha};\xi) = \rho_a(\xi)^{-1}\sum_{y\in\mathfrak{Z}(t^2)}\mathfrak{c}_y(\boldsymbol{\alpha}), \tag{7.15}$$

where

$$\mathfrak{c}_y(\boldsymbol{\alpha}) = \mathfrak{a}_{p^ay+\xi}E(\psi(p^ay+\xi;\boldsymbol{\alpha})),$$

and $\psi(n;\boldsymbol{\alpha})$ is defined by means of (3.3). Note that, in view of (3.2), the latter definition yields the relation

$$\rho_0(1;\mathfrak{c}) = \|\mathfrak{c}\|_0^{1/2}\cdot\|\mathfrak{c}\|_\infty = \|\mathfrak{a}_a(\xi)\|_0^{1/2}\cdot\|\mathfrak{a}_a(\xi)\|_\infty = \rho_a(\xi). \tag{7.16}$$

We also define the exponential sum

$$\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \rho_0(1;\mathfrak{c})^{-1}\sum_{y\in\mathfrak{Z}(t^2)}\mathfrak{c}_y(\boldsymbol{\alpha})E(\beta_1\Psi_1(y)+\ldots+\beta_r\Psi_r(y)), \tag{7.17}$$

and the mean value

$$J(\boldsymbol{\alpha}) = \oint_{p^{B'}}|\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha},\boldsymbol{\beta})|^{2R}\,\mathrm{d}\boldsymbol{\beta}.$$

By orthogonality, the mean value $J(\boldsymbol{\alpha})$ counts the $\mathfrak{Z}(t^2)$-solutions of the system of congruences (7.13), with each solution $\mathbf{u},\mathbf{z}$ being counted with weight

$$\begin{aligned}&\rho_0(1;\mathfrak{c})^{-2R}\prod_{i=1}^{R}\mathfrak{c}_{u_i}(\boldsymbol{\alpha})\overline{\mathfrak{c}}_{z_i}(\boldsymbol{\alpha})\\ &\qquad = \rho_a(\xi)^{-2R}\Big(\prod_{i=1}^{R}\mathfrak{a}_{p^au_i+\xi}\overline{\mathfrak{a}}_{p^az_i+\xi}\Big)E\Big(\sum_{i=1}^{R}\big(\psi(p^au_i+\xi;\boldsymbol{\alpha})-\psi(p^az_i+\xi;\boldsymbol{\alpha})\big)\Big).\end{aligned}$$

The initial phase of our discussion revealed that the conditions (7.13) on $\mathbf{x} = p^a\mathbf{u}+\xi$ and $\mathbf{y} = p^a\mathbf{z}+\xi$ are implicitly implied by (3.18). Consequently, since (7.15), (7.16) and (7.17) yield the relation

$$\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha},\mathbf{0}) = \mathfrak{f}_a(\boldsymbol{\alpha};\xi),$$

we deduce that

$$\oint_{p^B} |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2R}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}|\,\mathrm{d}\boldsymbol{\alpha} = \oint_{p^B}\oint_{p^{B'}} |\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha},\boldsymbol{\beta})^{2R}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}|\,\mathrm{d}\boldsymbol{\beta}\,\mathrm{d}\boldsymbol{\alpha}. \tag{7.18}$$

Thus, we arrive at the relation

$$K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta) = \oint_{p^B} J(\boldsymbol{\alpha})|\mathfrak{f}_b(\boldsymbol{\alpha};\eta)|^{2s-2R}\,\mathrm{d}\boldsymbol{\alpha}. \tag{7.19}$$

We emphasise that the inner integral over $\boldsymbol{\beta}$ on the right hand side of (7.18) is, on a fundamental level, content-free, since the integral over $\boldsymbol{\alpha}$ restricts the variables underlying the factor $|\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha},\boldsymbol{\beta})|^{2R}$ so as to satisfy the system of congruences (7.13) automatically.

In the next phase of our argument, we finally apply our inductive hypothesis. The key observation is that the mean value $J(\boldsymbol{\alpha})$ is amenable to Corollary 3.4 to Theorem 3.3. The system $\boldsymbol{\Psi}$ is p^c-spaced for some $c \geqslant \tau B'$, and B' is sufficiently large in terms of k, τ and ε^2. In view of Hypothesis 3.2 for the collection of weights $(\mathfrak{a})$, moreover, we may assume that the collection of weights $(\mathfrak{c}_y(\boldsymbol{\alpha}))$ satisfies Hypothesis 3.2. Hence, we have

$$\begin{aligned} J(\boldsymbol{\alpha}) = U_{R,r}^{B'}(\mathfrak{c}) &\ll p^{B'\varepsilon^2}U_{R,r}^{B',H'}(\mathfrak{c}) \\ &= p^{B'\varepsilon^2}\rho_0(1;\mathfrak{c})^{-2}\sum_{\zeta\ (\mathrm{mod}\ (p^{H'},t^2))}\rho_{H'}(\zeta;\mathfrak{c})^2\oint_{p^{B'}}|\mathfrak{g}_{\mathfrak{c}'}(\boldsymbol{\alpha},\boldsymbol{\beta})|^{2R}\,\mathrm{d}\boldsymbol{\beta}, \end{aligned} \tag{7.20}$$

in which $\mathfrak{c}' = \mathfrak{c}'(\boldsymbol{\alpha})$ is defined by putting

$$\mathfrak{c}'_n(\boldsymbol{\alpha}) = \begin{cases} \mathfrak{c}_n(\boldsymbol{\alpha}), & \text{when } n \equiv \zeta\ (\mathrm{mod}\ (p^{H'},t^2)), \\ 0, & \text{otherwise.} \end{cases}$$

Note that $\rho_0(1;\mathfrak{c}) = \rho_a(\xi)$. Moreover, on putting $\kappa = p^a\zeta + \xi$, we find that

$$\begin{aligned} \rho_{H'}(\zeta;\mathfrak{c}) &= \|(\mathfrak{a}_{p^ay+\xi} : y \equiv \zeta\ (\mathrm{mod}\ (p^{H'},t^2)))\|_0^{1/2}\cdot\|(\mathfrak{a}_{p^ay+\xi} : y \equiv \zeta\ (\mathrm{mod}\ (p^{a+H'},t^2)))\|_\infty \\ &= \rho_{a+H'}(\kappa). \end{aligned}$$

Thus, on substituting (7.20) into (7.19), we infer that

$$\begin{aligned} &\rho_a(\xi)^2K_{a,b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a};\xi,\eta) \\ &\quad\ll p^{B'\varepsilon^2}\sum_{\substack{\kappa\ (\mathrm{mod}\ (p^{a+H'},t^2))\\ \kappa\equiv\xi\ (\mathrm{mod}\ (p^a,t^2))}}\rho_{a+H'}(\kappa)^2\oint_{p^B}\oint_{p^{B'}}|\mathfrak{g}_{\mathfrak{c}'}(\boldsymbol{\alpha},\boldsymbol{\beta})^{2R}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}|\,\mathrm{d}\boldsymbol{\beta}\,\mathrm{d}\boldsymbol{\alpha}. \end{aligned} \tag{7.21}$$

Having extracted our strong congruence constraint on a subset of the implicit variables, our next task is to reverse course so as to relate the mean value on the right hand side of (7.21) to simpler mean values closer in spirit to the target $K_{b',b,c}^{r,\boldsymbol{\varphi},\nu}(\mathfrak{a})$. We begin by observing that the mean value

$$\oint_{p^{B'}}|\mathfrak{g}_{\mathfrak{c}'}(\boldsymbol{\alpha},\boldsymbol{\beta})|^{2R}\,\mathrm{d}\boldsymbol{\beta}$$

counts the $\mathfrak{Z}(t^2)$-solutions of the system of equations (7.13), with each solution $\mathbf{u}$, $\mathbf{z}$ being counted with weight

$$\rho_0(1;\mathfrak{c}')^{-2R}\prod_{i=1}^R \mathfrak{c}'_{u_i}(\boldsymbol{\alpha})\overline{\mathfrak{c}}'_{z_i}(\boldsymbol{\alpha})$$
$$= \rho_{a+H'}(\kappa)^{-2R}\Big(\prod_{i=1}^R \mathfrak{a}_{p^a u_i+\xi}\overline{\mathfrak{a}}_{p^a z_i+\xi}\Big)E\Big(\sum_{i=1}^R\big(\psi(p^a u_i+\xi;\boldsymbol{\alpha})-\psi(p^a z_i+\xi;\boldsymbol{\alpha})\big)\Big),$$

but now subject to the constraint $\mathbf{u}\equiv\mathbf{z}\equiv\zeta \pmod{p^{H'}}$. Note that the conditions (7.13) on $\mathbf{x}=p^a\mathbf{u}+\xi$ and $\mathbf{y}=p^a\mathbf{z}+\xi$ are again automatically implied by (3.18). Consequently, since we have $\mathfrak{g}_{\mathfrak{c}'}(\boldsymbol{\alpha},\mathbf{0})=\mathfrak{f}_{a+H'}(\boldsymbol{\alpha};\kappa)$, we perceive that

$$\oint_{p^B}\oint_{p^{B'}}|\mathfrak{g}_{\mathfrak{c}'}(\boldsymbol{\alpha},\boldsymbol{\beta})^{2R}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}|\,\mathrm{d}\boldsymbol{\beta}\,\mathrm{d}\boldsymbol{\alpha}=\oint_{p^B}|\mathfrak{f}_{a+H'}(\boldsymbol{\alpha};\kappa)^{2R}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2R}|\,\mathrm{d}\boldsymbol{\alpha}. \tag{7.22}$$

By reference to Lemma 6.3, moreover, we obtain the upper bound

$$\rho_{a+H'}(\kappa)^2|\mathfrak{f}_{a+H'}(\boldsymbol{\alpha};\kappa)|^{2R}\leqslant(p^{2b'-2(a+H')})^R\sum_{\substack{\xi' \pmod{(p^{b'},t^2)}\\ \xi'\equiv\kappa \pmod{(p^{a+H'},t^2)}}}\rho_{b'}(\xi')|\mathfrak{f}_{b'}(\boldsymbol{\alpha};\xi')|^{2R}. \tag{7.23}$$

Therefore, by substituting (7.23) into (7.22), and the resulting bound into (7.21), we arrive at the estimate

$$\rho_a(\xi)^2K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a};\xi,\eta)\ll p^{B'\varepsilon^2+2R(b'-(a+H'))}\sum_{\substack{\xi' \pmod{(p^{b'},t^2)}\\ \xi'\equiv\xi \pmod{(p^a,t^2)}}}\rho_{b'}(\xi')^2K^{r,\boldsymbol{\varphi},\nu}_{b',b,c}(\mathfrak{a};\xi',\eta).$$

This upper bound may now, in turn, be substituted into the definition (3.16), and thus we find that

$$\rho_0(1)^4K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})$$
$$\ll p^{B'\varepsilon^2+2R(b'-(a+H'))}\sum_{\xi' \pmod{(p^{b'},t^2)}}\sum_{\substack{\eta \pmod{(p^{b'},t^2)}\\ \eta\not\equiv\xi' \pmod{(p^\nu,t)}}}\rho_{b'}(\xi')^2\rho_b(\eta)^2K^{r,\boldsymbol{\varphi},\nu}_{b',b,c}(\mathfrak{a};\xi',\eta),$$

and hence

$$K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})\ll p^{B'\varepsilon^2+2R(b'-(a+H'))}K^{r,\boldsymbol{\varphi},\nu}_{b',b,c}(\mathfrak{a}). \tag{7.24}$$

The proof of the lemma is now swiftly made complete. We observe that, as a consequence of (7.14), one has

$$2R(b'-a-H')=r(r+1)(b'-a-H')\leqslant(r+1)(r+2(k-r)\gamma)<2k^2\nu.$$

Consequently, on recalling the definition (6.6) and the heierarchy of small quantities (6.2), we find that

$$B'\varepsilon^2+2R(b'-a-H')<\nu+2k^2\nu<3k^2\nu.$$

The conclusion of the lemma therefore follows from (7.24) in this situation in which we assume that $B'>\nu$. □

8. The iterative process

The work of the previous section, in common with [11, §7] in its own setting, shows how to generate powerful congruence constraints on the variables underlying the mean value $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})$. In all essentials, the conclusion of our own Lemma 7.1 provides a relation more or less identical to that of [11, Lemma 7.1], save that we work in $\mathbb{Z}[t]/t^2\mathbb{Z}[t]$ instead of in $\mathbb{Z}$. The subtle differences in the definitions of $K^{r,\boldsymbol{\varphi},\nu}_{a,b,c}(\mathfrak{a})$ in the respective situations do not obstruct us from drawing the same conclusions. We therefore provide only a sketch of the argument, noting the very few differences encountered as the argument is pursued. At this point, the parameters $\boldsymbol{\varphi}$, ν and c have ceased to possess any particular significance, and henceforth we may safely omit their mention in our various notations. Also, throughout this section, we suppose that a, b and r are integers satisfying (7.1), and we define b' via (7.2). Our first step is to interchange the roles of b' and b in the conclusion of Lemma 7.1

Lemma 8.1. *When $r \geqslant 2$, one has*

$$K^r_{a,b}(\mathfrak{a}) \ll (p^{2\nu})^{2k^2} K^{k-r}_{b,b'}(\mathfrak{a})^{\frac{1}{k-r+1}} K^{r-1}_{b',b}(\mathfrak{a})^{\frac{k-r}{k-r+1}}.$$

Meanwhile, when $r = 1$, one instead has

$$K^1_{a,b}(\mathfrak{a}) \ll (p^{2\nu})^{2k^2} K^{k-1}_{b,kb}(\mathfrak{a})^{1/k} U^{B,b}_{s,k}(\mathfrak{a})^{1-1/k}.$$

Proof. Both conclusions follow by pursuing the argument of the proof of [11, Lemma 8.1], mutatis mutandis. The factor $p^{k^2\nu}$ in the latter is here replaced by the factor $(p^{2\nu})^{2k^2}$ from the conclusion of Lemma 7.1 throughout. Moreover, the condition $\xi \not\equiv \eta \pmod{p^\nu}$ in [11] is replaced in the present context by $\xi \not\equiv \eta \pmod{(p^\nu, t)}$. In all other respects, the argument follows almost word for word as in the proof of [11, Lemma 8.1]. □

By employing the definition (3.21), the conclusion of Lemma 8.1 may be converted into a normalised analogue.

Lemma 8.2. *Suppose that $b \leqslant (1-\delta)B/k$. Then, when $r \geqslant 2$, one has*

$$[[K^r_{a,b}(\mathfrak{a})]]_\Lambda \ll (p^{2\nu})^{2k^2} [[K^{k-r}_{b,b'}(\mathfrak{a})]]_\Lambda^{\frac{1}{k-r+1}} [[K^{r-1}_{b',b}(\mathfrak{a})]]_\Lambda^{1-1/r}.$$

Meanwhile, when $r = 1$, one instead has

$$[[K^1_{a,b}(\mathfrak{a})]]_\Lambda \ll (p^{2\nu})^{4k^2} [[K^{k-1}_{b,kb}(\mathfrak{a})]]_\Lambda^{1/k} \big(p^{-2b}\big)^{\Lambda(1-1/k)}. \tag{8.1}$$

Proof. The proof follows that of [11, Lemma 8.2], mutatis mutandis. In our setting, the upper bound (6.5) contains an extra factor of 2 in the exponent relative to its analogue in [11], and hence one obtains an extra factor 2 in the exponent of p on the right hand side of (8.1) in the final factor. □

At this point, we streamline our notation further by writing

$$\widetilde{K}^r_{a,b} = [[K^r_{a,b}(\mathfrak{a})]]_\Lambda.$$

Also, when $1 \leqslant j \leqslant k-1$, we write

$$\rho_j = \frac{j}{k-j+1} \quad \text{and} \quad b_j = \left\lceil \frac{b}{\rho_j} \right\rceil.$$

Lemma 8.3. *Suppose that*

$$1 \leqslant r \leqslant k-1, \quad a \geqslant \delta\theta, \quad b \geqslant k^2\delta\theta \quad \text{and} \quad ra \leqslant (k-r+1)b. \tag{8.2}$$

Then, whenever $k^2b \leqslant (1-\delta)B$, there exist integers a', b', r', and there exists a positive number ρ, having the property that

$$\widetilde{K}^r_{a,b} \ll \big(\widetilde{K}^{r'}_{a',b'}\big)^{\rho}\big(p^{-2b}\big)^{\Lambda/(2k)},$$

with

$$a' \geqslant \delta\theta, \quad b' \geqslant k^2\delta\theta, \quad r'a' \leqslant (k-r'+1)b', \quad 1 \leqslant r' \leqslant k-1,$$
$$0 < \rho < (1-1/k)^2, \quad (1+2/k)b \leqslant b' \leqslant k^2b, \quad b' = \left\lceil \frac{r'+1}{k-r'} \right\rceil, \quad \rho b' \geqslant b.$$

Proof. Under the hypothesis (8.2), the argument of the proof of [11, Lemma 9.1] applies, essentially verbatim, to show that whenever $kb \leqslant (1-\delta)B$, then

$$\widetilde{K}^r_{a,b} \ll p^{4(r+1)k^2\nu}\big(p^{-2b}\big)^{(1-1/k)\Lambda/r}\prod_{j=1}^{r}\big(\widetilde{K}^{k-j}_{b,b_j}\big)^{\rho_j/r}.$$

Under the same hypotheses, it follows from the argument of the proof of [11, Lemma 9.2], again applied almost verbatim, that there exists an integer r' with $1 \leqslant r' \leqslant r$ having the property that

$$\widetilde{K}^r_{a,b} \ll \big(\widetilde{K}^{k-r'}_{b,b_{r'}}\big)^{\rho_{r'}}\big(p^{-2b}\big)^{\Lambda/(2k)}.$$

The conclusion of the present lemma then follows from this estimate by applying the argument of the proof of [11, Lemma 9.3], without any essential alteration. □

9. The proof of Theorem 3.3

The conclusion of Lemma 8.3 facilitates the same kind of p-adic concentration argument as was made available by [11, Lemma 9.3]. Indeed, our proof of Theorem 3.3 may be engineered essentially verbatim as in the corresponding argument of [11, §10]. For this reason, we shall be extremely economical on details, since it suffices to sketch out differences only.

The proof of Theorem 3.3. In view of the conclusion of Lemma 5.1, we may suppose throughout this section that k is a natural number with $k \geqslant 2$. In addition, we put $s = k(k+1)/2$. We may suppose that the conclusion of Theorem 3.3 has already been established for exponents smaller than k. By way of seeking a contradiction, we suppose that $\lambda(s,k) = \Lambda$ with $\Lambda > 0$. We initiate our iterative method by appealing to Lemma 6.4, which shows that

$$U^B_{s,k}(\mathfrak{a}) \ll p^{2s\theta}K^1_{\theta,\theta}(\mathfrak{a}).$$

In view of the assumption (6.4), we deduce from (3.21) that

$$[[K^1_{\theta,\theta}(\mathfrak{a})]]_\Lambda \gg \frac{p^{-2s\theta}U^B_{s,k}(\mathfrak{a})}{(p^{2H})^\Lambda U^{B,H}_{s,k}(\mathfrak{a})} \geqslant p^{-2s\theta-2H\varepsilon}.$$

The heierarchy (6.2) consequently combines with (6.20) to reveal that

$$\widetilde{K}^1_{\theta,\theta} \gg p^{-4s\theta}. \tag{9.1}$$

Next, we apply Lemma 8.3 repeatedly. Put

$$N = \lceil 16sk/\Lambda \rceil. \tag{9.2}$$

Our assumption that B, and hence also H, is sufficiently large in terms of our heierarchy of parameters (6.2) ensures that $2k^{2N+2}\theta < H$. We cliam that the sequences (a_n), (b_n), (r_n), (ρ_n) may be defined for $0 \leqslant n \leqslant N$ in such a manner that

$$1 \leqslant r_n \leqslant k-1, \quad k^2\delta\theta \leqslant b_n \leqslant k^{2n+2}\theta,$$
$$\delta\theta \leqslant a_n \leqslant (k-r_n+1)b_n/r_n,$$
$$0 < \rho_n < (1-1/k)^2, \quad \rho_n b_n \geqslant b_{n-1} \quad (n \geqslant 1),$$

and so that

$$\widetilde{K}^1_{\theta,\theta} \ll \big(\widetilde{K}^{r_n}_{a_n,b_n}\big)^{\rho_1\cdots\rho_n}\big(p^{-\Lambda/(2k)}\big)^{2nb_0}. \tag{9.3}$$

We initiate these sequences by putting $a_0 = b_0 = \theta$ and $\rho_0 = r_0 = 1$, so that (9.3) is immediate in the case $n = 0$.

The confirmation of this claim is essentially a numerical check that follows via an argument identical to that bridging [11, equation (10.6)] and [11, equation (10.9)], mutatis mutandis. From here, by combining (9.1) and (9.3), we find that

$$p^{-4s\theta} \ll \widetilde{K}^1_{\theta,\theta} \ll \big(\widetilde{K}^{r_N}_{a_N,b_N}\big)^{\rho}\big(p^{-\Lambda/(2k)}\big)^{2N\theta}, \tag{9.4}$$

where $\rho = \rho_1\cdots\rho_N < 1$. On recalling the definition (3.21) and the assumption that $\lambda(s,k) = \Lambda$, the conclusion of Lemma 4.5 shows that

$$[[K^{r_N}_{a_N,b_N}]]_\Lambda \ll p^{2H\varepsilon}.$$

Then, again employing the properties of the heierarchy (6.2), we may suppose that $\widetilde{K}^{r_N}_{a_N,b_N} \ll p^\theta$, and thus (9.4) delivers the bound

$$p^{-4s\theta} \ll p^{\theta(1-N\Lambda/k)},$$

and hence

$$(p^\theta)^{8s} \gg (p^\theta)^{N\Lambda/k}. \tag{9.5}$$

The definition (6.20) of θ shows that p^θ is sufficiently large in terms of s, k and Λ. Hence, the upper bound (9.5) can hold only when $8s \geqslant N\Lambda/k$. In view of (9.2), we therefore obtain the bound

$$\Lambda \leqslant 8sk/N \leqslant \Lambda/2,$$

yielding a contradiction to the assumption (6.1) that $\Lambda > 0$.

This discussion forces us to conclude that Λ cannot be positive, and thus $\lambda(s,k) \leqslant 0$. This completes the proof of Theorem 3.3 for the exponent k, and the theorem therefore follows in full by induction on k. □

The proof of Corollary 3.4. The conclusion of Corollary 3.4 follows from Theorem 3.3 by simply interpreting the definitions (3.12) and (3.13) of $\lambda^*(s,\theta;\tau)$ and $\lambda(s,\theta)$. Thus, since $\lambda(s,k) \leqslant 0$, we may suppose that for every $\varepsilon > 0$, whenever $\tau > 0$ is sufficiently small, one has $\lambda^*(s,k;\tau) < \varepsilon$. But then, for each $\varepsilon > 0$, one has

$$U^B_{s,k}(\mathfrak{a}) \ll p^{(\lambda^*(s,k;\tau)+\varepsilon)H}U^{B,H}_{s,k}(\mathfrak{a})$$

for all coefficient weights $(\mathfrak{a}) \in \mathbb{D}$, all $\boldsymbol{\varphi} \in \Phi_\tau(B)$ and all large enough values of B. The corresponding conclusion for the situation with coefficient weights $(\mathbf{0})$ all equal to zero is of course, trivial. $\square$

10. Mean values of exponential sums

Our goal in this section is to establish the main conclusions from the introduction by application of Theorem 3.3 and its corollary. In pursuit of this objective, we follow closely the path laid down in the classical case associated with $\mathbb{Z}$ described in [11, §12].

The proof of Theorem 1.1. Let $\varphi_j \in \mathbb{Z}[t,u]$ $(1 \leqslant j \leqslant k)$ be polynomials with the Wronskian $W(u;\boldsymbol{\varphi})$ non-vanishing modulo t, and let $\varepsilon > 0$ be a small positive number. Let $\mathcal{Z}$ denote the set of zeros of the congruence

$$W(u;\boldsymbol{\varphi}) \equiv 0 \pmod{t},$$

with $u \in \mathbb{Z}$, and let X be a positive integer sufficiently large in terms of $\boldsymbol{\varphi}$, s, k and ε. We note that the non-vanishing of $W(u;\boldsymbol{\varphi})$ modulo t implies that the expression $W(u;\boldsymbol{\varphi}) \pmod t$ is a non-zero polynomial having degree bounded in terms of $\boldsymbol{\varphi}$ and k. Hence

$$\operatorname{card}(\mathcal{Z}) \leqslant \deg\big(W(u;\boldsymbol{\varphi}) \pmod t\big) \ll 1. \tag{10.1}$$

We suppose that $s = k(k+1)/2$. Finally, when $(\mathfrak{a})$ is a set of complex weights with $|\mathfrak{a}_{n_0+n_1t}| = 1$ for $|n_0| \leqslant X$ and $|n_1| \leqslant X$, and $\mathfrak{a}_{n_0+n_1t} = 0$ otherwise, we write

$$F(\boldsymbol{\alpha};X) = (2X+1)^{-1} \sum_{|n_0|\leqslant X} \sum_{|n_1|\leqslant X} \mathfrak{a}_{n_0+n_1t} E\big(\psi(n_0+n_1t;\boldsymbol{\alpha})\big)$$

and

$$F_0(\boldsymbol{\alpha};X) = (2X+1)^{-1} \sum_{\substack{|n_0|\leqslant X\\ n_0\notin\mathcal{Z}}} \sum_{|n_1|\leqslant X} \mathfrak{a}_{n_0+n_1t} E\big(\psi(n_0+n_1t;\boldsymbol{\alpha})\big),$$

where $\psi(n;\boldsymbol{\alpha})$ is defined as in (3.3). We frequently find it convenient to abbreviate n_0+n_1t simply to n, with similar conventions applied with related notation.

As a consequence of the triangle inequality, one has

$$\Big| \sum_{\substack{|n_0|\leqslant X\\ n_0\in\mathcal{Z}}} \sum_{|n_1|\leqslant X} \mathfrak{a}_{n_0+n_1t} E\big(\psi(n_0+n_1t;\boldsymbol{\alpha})\big) \Big| \leqslant (2X+1)\operatorname{card}(\mathcal{Z}),$$

and thus, it follows from (10.1) that

$$|F(\boldsymbol{\alpha};X)| \ll 1 + |F_0(\boldsymbol{\alpha};X)|.$$

Thus, one has

$$\oint |F(\boldsymbol{\alpha};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha} \ll 1 + \oint |F_0(\boldsymbol{\alpha};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}. \tag{10.2}$$

In this way, it is apparent that it suffices to restrict attention to mean values in which the underlying variables possess non-vanishing Wronskians modulo t. By orthogonality, the mean value on the right hand side of (10.2) counts the number of integral solutions

of the system of equations (1.3) with $|u_i|, |v_i| \leqslant X$ and $u_i \notin \mathcal{Z} \pmod t$ $(1 \leqslant i \leqslant 2s)$, and with each solution being counted with weight

$$(2X+1)^{-2s} \prod_{i=1}^{s} \mathfrak{a}_{u_i+v_it} \overline{\mathfrak{a}}_{u_{s+i}+v_{s+i}t}. \tag{10.3}$$

Our next step is to shift from non-vanishing of Wronskians modulo t to corresponding non-vanishing modulo (p,t), for a suitable prime number p. When $n \in \mathbb{Z}[t]$, denote by $W_t(n;\boldsymbol{\varphi})$ the integer congruent modulo t to $W(n;\boldsymbol{\varphi})$. Given a solution $\mathbf{u}, \mathbf{v}$ of the system (1.3) of the type just described, the integer

$$\Xi(\mathbf{u}) = \prod_{i=1}^{2s} W_t(u_i;\boldsymbol{\varphi})$$

is non-zero. Moreover, one has $|\Xi(\mathbf{u})| \leqslant CX^D$, for some $C > 0$ depending at most on s, k and the coefficients of $\boldsymbol{\varphi}$, and D a positive integer with

$$D \leqslant 2s \sum_{j=1}^{k} \deg(\varphi_j).$$

Let $\mathcal{P}$ denote the set of primes p with $(\log X)^2 < p \leqslant 3(\log X)^2$. Thus, when X is large, it is a consequence of the prime number theorem that

$$\prod_{p \in \mathcal{P}} p > (\log X)^{(\log X)^2/\log\log X} > CX^D.$$

We therefore deduce that for each solution $\mathbf{u}, \mathbf{v}$ of the system (1.3) counted by the integral on the right hand side of (10.2), there exists a prime $p \in \mathcal{P}$ with

$$\prod_{i=1}^{2s} W_t(u_i;\boldsymbol{\varphi}) \not\equiv 0 \pmod p.$$

In particular, one has

$$\oint |F_0(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha} \leqslant \sum_{p \in \mathcal{P}} \oint |F_p(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha},$$

where

$$F_p(\boldsymbol{\alpha};X) = (2X+1)^{-1} \sum_{W(n;\boldsymbol{\varphi}) \not\equiv 0 \pmod{(p,t)}} |\mathfrak{a}_n| E\big(\psi(n;\boldsymbol{\alpha})\big). \tag{10.4}$$

Thus, we conclude from (10.2) that

$$\oint |F(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha} \ll 1 + (\log X)^2 \max_{p \in \mathcal{P}} \oint |F_p(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha}. \tag{10.5}$$

We seek to establish that for each fixed prime $p \in \mathcal{P}$, one has

$$\oint |F_p(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha} \ll X^{\varepsilon/2}. \tag{10.6}$$

Granted this estimate, it follows from (10.5) that

$$\oint |F(\boldsymbol{\alpha};X)|^{2s} \,\mathrm{d}\boldsymbol{\alpha} \ll 1 + X^{\varepsilon/2}(\log X)^2 \ll X^{\varepsilon},$$

whence

$$\oint \Big| \sum_{|n_0| \leqslant X} \sum_{|n_1| \leqslant X} \mathfrak{a}_{n_0+n_1t} E\big(\psi(n_0+n_1t;\boldsymbol{\alpha})\big) \Big|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \ll X^{2s+\varepsilon}. \tag{10.7}$$

By specialising the coefficient weights $\mathfrak{a}_{n_0+n_1t}$ to be 1 for $|n_0| \leqslant X$ and $|n_1| \leqslant X$, we find via orthogonality that this establishes the upper bound $\Upsilon_{s,k}(X) \ll X^{2s+\varepsilon}$ claimed in equation (1.4) of the statement of Theorem 1.1 in the special case $s = k(k+1)/2$. The desired conclusion for smaller values of s follows by applying Hölder's inequality.

We henceforth focus on the proof of the estimate (10.6). We put

$$B = \left\lceil \frac{k \log X}{\log p} \right\rceil.$$

Thus, we have $X^k \leqslant p^B \leqslant pX^k$. Next, by orthogonality, we observe that the mean value on the left hand side of (10.6) is equal to a weighted count of the solutions to the system of equations (1.3) over $\mathfrak{Z}(t^2)$, with each weight non-negative. An upper bound for this count is given by replacing the equations by corresponding congruences modulo p^B. Thus, by reversing our earlier observation utilising orthogonality, one obtains the upper bound

$$\oint |F_p(\boldsymbol{\alpha};X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \leqslant \oint_{p^B} |F_p(\boldsymbol{\alpha};X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}. \tag{10.8}$$

The next step towards the proof of (10.6) is the preparation of a p^c-spaced system associated with $\boldsymbol{\varphi}$. In view of the definition (10.4), we may suppose that $\mathfrak{a}_n = 1$ for each n. The mean value on the left hand side of (10.6) counts the $\mathfrak{Z}(t^2)$-solutions of the system of equations (1.3) with $|\mathbf{u}|, |\mathbf{v}| \leqslant X$ satisfying

$$\prod_{i=1}^{2s} W_t(u_i;\boldsymbol{\varphi}) \not\equiv 0 \pmod{p},$$

in which each solution is counted with weight (10.3), namely $(2X+1)^{-2s}$. Suppose that $\tau > 0$ is sufficiently small in terms of s and k. We suppose also that B is sufficiently large in terms of τ, as well as s, k and ε. Such is permissible, since we may suppose that X is likewise sufficiently large. We put $c = \lceil \tau B \rceil$. We next sort the implicit summation defining $F_p(\boldsymbol{\alpha};X)$ into congruence classes modulo (p^c, t^2). In view of our assumptions concerning the sequence $(\mathfrak{a})$ implied by (10.4), we may suppose that $\mathfrak{a}_n = 0$ whenever $n \equiv \xi \pmod{(p^c, t^2)}$ and

$$W_t(\xi;\boldsymbol{\varphi}) \equiv 0 \pmod{p}.$$

For such values of ξ, one then has $\rho_c(\xi) = 0$. With this assumption, one finds that

$$F_p(\boldsymbol{\alpha};X) = (2X+1)^{-1} \sum_{\xi \pmod{(p^c,t^2)}} \rho_c(\xi) \mathfrak{f}_c(\boldsymbol{\alpha};\xi),$$

and hence Lemma 6.3 delivers the bound

$$\rho_0(1)^2 |F_p(\boldsymbol{\alpha};X)|^{2s} \leqslant (p^{2c})^s \sum_{\xi \pmod{(p^c,t^2)}} \rho_c(\xi)^2 |\mathfrak{f}_c(\boldsymbol{\alpha};\xi)|^{2s}.$$

Thus, we obtain the estimate

$$\oint_{p^B} |F_p(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \leqslant (p^{2c})^s \rho_0(1)^{-2} \sum_{\xi \ (\mathrm{mod}\ (p^c, t^2))} \rho_c(\xi)^2 I_p(\xi), \tag{10.9}$$

where

$$I_p(\xi) = \oint_{p^B} |\mathfrak{f}_c(\boldsymbol{\alpha}; \xi)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}.$$

The mean value $I_p(\xi)$ counts the solutions $\mathbf{y}, \mathbf{z} \in \mathfrak{Z}(t^2)$ of the system of congruences

$$\sum_{i=1}^{s} \big(\varphi_j(p^c y_i + \xi) - \varphi_j(p^c z_i + \xi)\big) \equiv 0 \ (\mathrm{mod}\ (p^B, t^2)) \quad (1 \leqslant j \leqslant k), \tag{10.10}$$

with each solution being counted with weight

$$\rho_c(\xi)^{-2s} \prod_{i=1}^{s} \mathfrak{a}_{p^c y_i + \xi} \overline{\mathfrak{a}}_{p^c z_i + \xi}. \tag{10.11}$$

Here, we note that we may restrict attention to the situation in which

$$W_t(\xi; \boldsymbol{\varphi}) \not\equiv 0 \ (\mathrm{mod}\ p) \quad \text{and} \quad \rho_c(\xi) > 0.$$

In particular, it follows from (3.8) and (10.9) that

$$\oint_{p^B} |F_p(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \leqslant (p^{2c})^s U_{s,k}^{B,c}(\mathfrak{a}).$$

We now reinterpret the system of congruences (10.10) by applying Taylor's theorem to expand the expression $\varphi_j(p^c v + \xi)$. When $1 \leqslant j \leqslant k$, we find that for suitable polynomials $\Phi_j(u) \in \mathbb{Z}[t, u]$, one has

$$\varphi_j(p^c v + \xi) - \varphi_j(\xi) \equiv \sum_{l=1}^{k} \omega_{lj} (p^c v)^l + (p^c v)^{k+1} \Phi_j(p^c v) \ (\mathrm{mod}\ (p^B, t^2)),$$

in which the $\mathbb{Z}[t]$-coefficients ω_{lj} are defined by taking

$$\omega_{lj} = (l!)^{-1} \varphi_j^{(l)}(\xi) \quad (1 \leqslant l, j \leqslant k).$$

Notice that these coefficients lie in $\mathbb{Z}[t]$, because $l!$ divides the l-th differential of a polynomial with coefficients lying in $\mathbb{Z}[t]$.

The determinant of the coefficient matrix $\Omega = (\omega_{lj})_{1 \leqslant l, j \leqslant k}$ is given by the formula

$$\det(\Omega) = W(\xi; \boldsymbol{\varphi}) \bigg(\prod_{l=1}^{k} l! \bigg)^{-1}.$$

Since we may suppose that $p > k$, the hypothesis that $W(\xi; \boldsymbol{\varphi}) \not\equiv 0 \ (\mathrm{mod}\ (p, t))$ permits us to conclude that $\det(\Omega) \not\equiv 0 \ (\mathrm{mod}\ (p, t))$, and thus it follows that a multiplicative inverse Ω^{-1} modulo (p, t) exists having coefficients in $\mathbb{Z}$. We now replace $\boldsymbol{\varphi}$ by $\Omega^{-1}\boldsymbol{\varphi}$ and $\boldsymbol{\Phi}$ by $\Omega^{-1}\boldsymbol{\Phi}$. This amounts to taking appropriate integral linear combinations of the congruences comprising (10.10). Proceeding in this manner, we see that there is no loss of generality in supposing that the original coefficient matrix Ω is congruent to I_k modulo (p, t). Assuming now that this assumption applies ab initio, it follows from Lemma 4.2 that the matrix of coefficients Ω has an inverse matrix Ω^{-1} in $\mathbb{Z}[t]/(p^B, t^2)$

satisfying $\Omega^{-1} \equiv I_k \pmod{(p,t)}$. In this new scenario, we again replace $\boldsymbol{\varphi}$ by $\Omega^{-1}\boldsymbol{\varphi}$ and $\boldsymbol{\Phi}$ by $\Omega^{-1}\boldsymbol{\Phi}$. This process permits us the assumption that the coefficient matrix Ω is in fact equal to I_k. Hence, there exist polynomials $\Xi_j(u) \in \mathbb{Z}[t,u]$ having the property that whenever the system of congruences (10.10) is satisfied, then

$$\sum_{i=1}^{s} (p^c)^j \big(\Psi_j(y_i) - \Psi_j(z_i) \big) \equiv 0 \pmod{(p^B, t^2)} \quad (1 \leqslant j \leqslant k),$$

in which $\Psi_j(u) = u^j + p^c \Xi_j(u)$. In particular, the system of polynomials $\boldsymbol{\Psi}$ is p^c-spaced.

The discussion of the previous paragraph shows that in any solution $\mathbf{y}, \mathbf{z}$ of the system (10.10), counted with weight (10.11), one has the additional constraints

$$\sum_{i=1}^{s} \big(\Psi_j(y_i) - \Psi_j(z_i) \big) \equiv 0 \pmod{(p^{B-kc}, t^2)} \quad (1 \leqslant j \leqslant k).$$

Define the coefficients

$$\mathfrak{c}_y(\boldsymbol{\alpha}) = \mathfrak{a}_{p^c y + \xi} E\big(\psi(p^c y + \xi; \boldsymbol{\alpha})\big).$$

Also, write

$$\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \rho_0(1; \mathfrak{c})^{-1} \sum_{y \in \mathbb{Z}} \mathfrak{c}_y(\boldsymbol{\alpha}) E\big(\beta_1 \Psi_1(y) + \ldots + \beta_k \Psi_k(y)\big),$$

and define the mean value

$$J(\boldsymbol{\alpha}) = \oint_{p^{B-kc}} |\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha}, \boldsymbol{\beta})|^{2s} \, \mathrm{d}\boldsymbol{\beta}.$$

Note that $\rho_0(1; \mathfrak{c}) = \rho_c(\xi; \mathfrak{a})$. Then, just as in the argument leading to (7.19) above, one sees that

$$I_p(\xi) = \oint_{p^B} |\mathfrak{g}_{\mathfrak{c}}(\boldsymbol{\alpha}; \mathbf{0})|^{2s} \, \mathrm{d}\boldsymbol{\alpha} = \oint_{p^B} J(\boldsymbol{\alpha}) \, \mathrm{d}\boldsymbol{\alpha}. \tag{10.12}$$

Observe next that, when written in the notation defined in (3.6), one has

$$J(\boldsymbol{\alpha}) = U_{s,k}^{B-kc, \boldsymbol{\Psi}}(\mathfrak{c}).$$

Moreover, the system $\boldsymbol{\Psi}$ is p^c-spaced and $B - kc$ is sufficiently large in terms of k, τ and ε. Notice that, as essentially noted in the discussion following the statement of Hypothesis 3.2, the coefficient weights $(\mathfrak{a}_{\boldsymbol{n}})$ with which we are working automatically satisfy both Hypotheses 3.1 and 3.2 with $\varepsilon = 0$, and so likewise do the coefficients $(\mathfrak{c}_y(\boldsymbol{\alpha}))$. Then Corollary 3.4 supplies the bound

$$J(\boldsymbol{\alpha}) \ll p^{B\varepsilon} U_{s,k}^{B-kc, H, \boldsymbol{\Psi}}(\mathfrak{c}),$$

where $H = \lceil B/k \rceil - c$. On substituting this bound into (10.12), and from there into (10.9), we infer that

$$\oint_{p^B} |F_p(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \ll (p^{2c})^s p^{B\varepsilon} \rho_0(1; \mathfrak{a})^{-2} \sum_{\xi \pmod{(p^c, t^2)}} \rho_c(\xi; \mathfrak{a})^2 U_{s,k}^{B-kc, H, \boldsymbol{\Psi}}(\mathfrak{c}). \tag{10.13}$$

For ease of exposition, we temporarily abbreviate $\mathfrak{f}_H(\boldsymbol{\beta}; \eta; \mathfrak{c}; \boldsymbol{\Psi})$ to $\mathfrak{f}_H^*(\boldsymbol{\beta}; \eta)$. Thus, we have

$$\mathfrak{f}_H^*(\boldsymbol{\beta}; \eta) = \rho_H(\eta; \mathfrak{c})^{-1} \sum_{y \equiv \eta \pmod{(p^H, t^2)}} \mathfrak{c}_y(\boldsymbol{\alpha}) E\big(\beta_1 \Psi_1(y) + \ldots + \beta_k \Psi_k(y)\big).$$

Note here that the coefficients $\mathfrak{c}_y(\boldsymbol{\alpha})$ are 0 unless $p^cy+\xi=n_0+n_1t$, with the integers n_0 and n_1 satisfying $|n_i|\leqslant X$. This condition we abbreviate by writing $|p^cy+\xi|\leqslant X$. As a consequence of the triangle inequality, one consequently has

$$\rho_H(\eta;\mathfrak{c})|\mathfrak{f}_H^*(\boldsymbol{\beta};\eta)|\leqslant \sum_{\substack{y\equiv\eta\ (\mathrm{mod}\ (p^H,t^2))\\ |p^cy+\xi|\leqslant X}}|\mathfrak{c}_y(\boldsymbol{\alpha})|\leqslant \left(\frac{2X+1}{p^{c+H}}+1\right)^2.$$

Moreover, a similar computation reveals that

$$\rho_H(\eta;\mathfrak{c})=\frac{2X+1}{p^{c+H}}+O(1).$$

Since $c+H=\lceil B/k\rceil$, the definition (3.8) yields

$$\begin{aligned}U_{s,k}^{B-kc,H,\boldsymbol{\Psi}}(\mathfrak{c})&\ll \rho_0(1;\mathfrak{c})^{-2}\sum_{\eta\ (\mathrm{mod}\ (p^c,t^2))}\rho_c(\eta;\mathfrak{c})^2\big(1+X/p^{c+H}\big)^{2s}\\ &\ll (1+X/p^{B/k})^{2s}.\end{aligned}$$

Hence, we deduce from (10.13) that

$$\begin{aligned}\oint_{p^B}|F_p(\boldsymbol{\alpha};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}&\ll p^{2(cs+B\varepsilon)}(1+X/p^{B/k})^{2s}\rho_0(1;\mathfrak{a})^{-2}\sum_{\xi\ (\mathrm{mod}\ (p^c,t^2))}\rho_c(\xi;\mathfrak{a})^2\\ &\ll p^{(4s\tau+2\varepsilon)B}\big(1+X/p^{B/k}\big)^{2s}.\end{aligned}$$

Recall that τ was chosen sufficiently small in terms of s and k. Moreover, we are at liberty to choose B to satisfy the bounds $X^k\leqslant p^B<pX^k$. Then we conclude that, for each positive number δ, one has

$$\oint_{p^B}|F_p(\boldsymbol{\alpha};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}\ll p^{B\delta}\ll X^{2k\delta}.$$

In view of (10.8), this establishes the upper bound (10.6) for each positive number ε, and thus we may conclude that the estimate (10.7) does indeed hold. □

With Theorem 1.1 now established, it is a relatively simple matter to derive the corollaries announced in §1, as we now show.

The proof of Corollary 1.2. We consider a k-tuple of polynomials $\varphi_j\in\mathbb{Z}[u]$ having the property that $W(u;\boldsymbol{\varphi})$ is non-zero as a polynomial in u. Then one has

$$\varphi_j(x+yt)\equiv\varphi_j(x)\ (\mathrm{mod}\ t)\quad(1\leqslant j\leqslant k),$$

so that $W_t(u;\boldsymbol{\varphi})$ is non-zero as a polynomial in u. Thus, as a consequence of orthogonality in combination with Theorem 1.1, we have

$$\oint\Big|\sum_{|n_0|\leqslant X}\sum_{|n_1|\leqslant X}E\big(\psi(n_0+n_1t;\boldsymbol{\alpha})\big)\Big|^{2s}\,\mathrm{d}\boldsymbol{\alpha}=\Upsilon_{s,k}(X;\boldsymbol{\varphi})\ll X^{2s+\varepsilon}.$$

However, an application of Taylor's theorem reveals that

$$\varphi_j(x+yt)\equiv\varphi_j(x)+y\varphi_j'(x)t\ (\mathrm{mod}\ t^2)\quad(1\leqslant j\leqslant t).$$

Thus, the definitions of §2 ensure that with

$$\boldsymbol{\alpha} = \Big(\frac{\beta_1}{t} + \frac{\gamma_1}{t^2}, \dots , \frac{\beta_k}{t} + \frac{\gamma_k}{t^2} \Big),$$

one has

$$\sum_{|n_0| \leqslant X} \sum_{|n_1| \leqslant X} E(\psi(n_0 + n_1 t; \boldsymbol{\alpha})) = \sum_{|n_0| \leqslant X} \sum_{|n_1| \leqslant X} e(\Omega(\mathbf{n}; \boldsymbol{\beta}, \boldsymbol{\gamma})),$$

where

$$\Omega(\mathbf{n}; \boldsymbol{\beta}, \boldsymbol{\gamma}) = \sum_{i=1}^{k} \big(\beta_i \varphi_i(n_0) + \gamma_i n_1 \varphi_i'(n_0) \big).$$

In particular, it follows via orthogonality that

$$\begin{aligned} \Upsilon_{s,k}(X; \boldsymbol{\varphi}) &= \oint \Big| \sum_{|n_0| \leqslant X} \sum_{|n_1| \leqslant X} E(\psi(n_0 + n_1 t; \boldsymbol{\alpha})) \Big|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \\ &= \oint \oint \Big| \sum_{|n_0| \leqslant X} \sum_{|n_1| \leqslant X} e(\Omega(\mathbf{n}; \boldsymbol{\beta}, \boldsymbol{\gamma})) \Big|^{2s} \, \mathrm{d}\boldsymbol{\beta} \, \mathrm{d}\boldsymbol{\gamma}. \end{aligned}$$

By orthogonality, the mean value on the right hand side counts the integral solutions of the system of equations

$$\left. \begin{aligned} \sum_{i=1}^{s} \big(\varphi_j(z_i) - \varphi_j(z_{i+s}) \big) &= 0 \\ \sum_{i=1}^{s} \big(h_i \varphi_j'(z_i) - h_{i+s} \varphi_j'(z_{i+s}) \big) &= 0 \end{aligned} \right\} \quad (1 \leqslant j \leqslant k),$$

with $|\mathbf{z}|, |\mathbf{h}| \leqslant X$. On invoking the conclusion of Theorem 1.1, we have therefore shown that

$$\Upsilon_{s,k}^*(X; \boldsymbol{\varphi}) = \Upsilon_{s,k}(X; \boldsymbol{\varphi}) \ll X^{2s+\varepsilon},$$

completing the proof of the corollary. □

A specialisation of the polynomials $\varphi_j(u)$ occurring in Corollary 1.2 yields the conclusion of Corollary 1.3.

The proof of Corollary 1.3. We may suppose that $d_1, \dots , d_k$ are integers with

$$1 \leqslant d_1 < d_2 < \dots < d_k.$$

A comparison of the systems (1.5) and (1.7) shows that the quantity $\Upsilon_{s,k}^+(X; \mathbf{d})$ central to Corollary 1.3 is equal to the quantity $\Upsilon_{s,k}^*(X; \boldsymbol{\varphi})$ estimated in Corollary 1.2, provided that one sets $\varphi_j(u) = u^{d_j}$ $(1 \leqslant j \leqslant k)$. In order to apply Corollary 1.2, all that must be verified is that $W(u; \boldsymbol{\varphi})$ is non-zero as a polynomial in u. However, one has

$$W(u; \boldsymbol{\varphi}) = \det \big(d_j (d_j - 1) \cdots (d_j - i + 1) u^{d_j - i} \big)_{1 \leqslant i,j \leqslant k}.$$

Every monomial in this polynomial is a multiple of u^D, where

$$D = \Big(\sum_{j=1}^{k} d_j \Big) - k(k+1)/2 = \sum_{j=1}^{k} (d_j - j).$$

Thus $W(u;\boldsymbol{\varphi}) = u^D \det(\Omega)$, where

$$\Omega = \big(d_j(d_j-1)\cdots(d_j-i+1)\big)_{1\leqslant i,j\leqslant k}.$$

However, as was shown in the proof of Corollary 1.2 of [11, §12], we have

$$\det(\Omega) = d_1\cdots d_k \prod_{1\leqslant i<j\leqslant k}(d_i-d_j) \neq 0.$$

Therefore, one has $W(u;\boldsymbol{\varphi}) \neq 0$. Thus, we may conclude from Corollary 1.2 that

$$\Upsilon^+_{s,k}(X;\mathbf{d}) = \Upsilon^*_{s,k}(X;\boldsymbol{\varphi}) \ll X^{2s+\varepsilon},$$

completing the proof of the corollary. □

Finally, the proof of Corollary 1.4 is essentially a specialisation of Corollary 1.3.

The proof of Corollary 1.4. A comparison of the systems (1.7) and (1.8) reveals that on putting $\mathbf{d} = (1,2,\dots,k)$, one has $J^*_{s,k}(X) = \Upsilon^*_{s,k}(X;\mathbf{d})$. Thus we deduce from Corollary 1.3 that with $s_0 = k(k+1)/2$, one has

$$J^*_{s_0,k}(X) \ll X^{2s_0+\varepsilon} = X^{k(k+1)+\varepsilon}. \tag{10.14}$$

Put

$$\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{j=1}^{k}\big(u^j\alpha_j + vu^{j-1}\beta_j\big),$$

and

$$w_k(\boldsymbol{\alpha},\boldsymbol{\beta};X) = \sum_{|u|\leqslant X}\sum_{|v|\leqslant X} e(\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta})).$$

Then it follows via orthogonality that

$$J^*_{s,k}(X) = \oint\cdots\oint |w_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta}.$$

When $s > s_0$, we may make use of the trivial estimate

$$|w_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)| \leqslant (2X+1)^2$$

in combination with (10.14) to deduce that

$$\begin{aligned} J^*_{s,k}(X) &\ll (X^2)^{2s-2s_0}\oint\cdots\oint |w_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)|^{2s_0}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta}\\ &= (X^2)^{2s-k(k+1)}J_{s_0,k}(X) \ll X^{4s-k(k+1)+\varepsilon}. \end{aligned}$$

This confirms the conclusion of Corollary 1.4 when $s > s_0$. Meanwhile, when $0 < s \leqslant s_0$, we may apply Hölder's inequality to deduce in like manner that

$$\begin{aligned} J^*_{s,k}(X) &\ll \bigg(\oint\cdots\oint |w_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)|^{2s_0}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta}\bigg)^{s/s_0}\\ &= \big(J_{s_0,k}(X)\big)^{s/s_0} \ll X^{2s+\varepsilon}. \end{aligned}$$

The conclusion of Corollary 1.4 consequently holds for all positive values of s. □

11. A number field variant

The main conclusions of §1 all have their natural analogues in algebraic number fields. A key advantage of our efficient congruencing approach, with regard to such variants, is that the proofs of such conclusions proceed without any significant alteration of the accompanying argument, once the associated infrastructure has been adjusted.

We begin by modifying the infrastructure necessary to describe our number field variants. We consider an algebraic extension K of degree n over K. We write $\mathfrak{O}_K$ for the ring of integers of K, and we fix a basis $\Omega = \{\omega_1, \dots, \omega_n\}$ for $\mathfrak{O}_K$ over $\mathbb{Z}$. When X is a large positive number, we define the box $\mathcal{B}(X) \subset \mathfrak{O}_K$ given by

$$\mathcal{B}(X) = \{r_1\omega_1 + \dots + r_n\omega_n : r_i \in \big[-\tfrac{1}{2}X^{1/n}, \tfrac{1}{2}X^{1/n}\big) \cap \mathbb{Z}\ (1 \leqslant i \leqslant n)\}.$$

One then has $\mathrm{card}(\mathcal{B}(X)) \asymp X$. We consider the system of congruences (1.1) with

$$x_i = u_i + v_i t \quad (1 \leqslant i \leqslant 2s),$$

and denote by $\Upsilon_{s,k}(X; \boldsymbol{\varphi}; K)$ the number of solutions of (1.1) with $\mathbf{u}, \mathbf{v} \in \mathcal{B}(X)$.

The analogue of Theorem 1.1 for number fields may now be announced.

Theorem 11.1. *Suppose that $\varphi_j(u) \in \mathfrak{O}_K[t, u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u; \boldsymbol{\varphi}) \not\equiv 0 \pmod t$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, one has $\Upsilon_{s,k}(X; \boldsymbol{\varphi}; K) \ll X^{2s+\varepsilon}$.*

Analogues of Corollaries 1.2 and 1.3 relevant for number fields follow so directly that the need for elaboration is rendered void. We content ourselves by recording an analogue of Corollary 1.4 that counts solutions of the system of equations (1.8) with $u_i, v_i \in \mathcal{B}(X)$ $(1 \leqslant i \leqslant 2s)$, a number we denote by $J^*_{s,k}(X; K)$.

Corollary 11.2. *Let s be a positive integer. Then for each $\varepsilon > 0$, one has*

$$J^*_{s,k}(X; K) \ll X^{\varepsilon}(X^{2s} + X^{4s-k(k+1)}).$$

The conclusion of Theorem 11.1 follows by applying an analogue of Theorem 3.3. The latter requires the introduction of further infrastructure. In the setting described above, we denote by $K^{(l)}$ $(1 \leqslant l \leqslant n_1)$ the real conjugate fields associated with K, and by $K^{(m)}$ and $K^{(m+n_2)}$ $(n_1 + 1 \leqslant m \leqslant n_1 + n_2)$ the pairs of complex conjugate fields associated with K. Thus, one has $n = n_1 + 2n_2$. When $\gamma \in K$, we denote by $\gamma^{(i)}$ the conjugates of γ, where $\gamma^{(i)} \in K^{(i)}$ $(1 \leqslant i \leqslant n)$. Then, the trace map of relevance to us is given by

$$\mathrm{Tr}_{K/\mathbb{Q}}(\gamma) = \gamma^{(1)} + \dots + \gamma^{(n)}.$$

When $\gamma_j \in K$ and $\theta_j \in \mathbb{R}$ for $1 \leqslant j \leqslant n$, and

$$\lambda(\boldsymbol{\theta}) = \theta_1\gamma_1 + \dots + \theta_n\gamma_n,$$

we define

$$\lambda^{(i)}(\boldsymbol{\theta}) = \theta_1\gamma_1^{(i)} + \dots + \theta_n\gamma_n^{(i)} \quad (1 \leqslant i \leqslant n).$$

The trace map on K then extends to the map defined by

$$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda(\boldsymbol{\theta})) = \lambda^{(1)}(\boldsymbol{\theta}) + \dots + \lambda^{(n)}(\boldsymbol{\theta}),$$

and our basic exponential function is then given by

$$\mathcal{E}(\lambda(\theta)) = e\big(\mathrm{Tr}_{K/\mathbb{Q}}(\lambda(\boldsymbol{\theta}))\big).$$

Next, we recall the inverse different $\mathfrak{d}^{-1}$, so that

$$\mathfrak{d}^{-1} = \{\eta \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\eta\xi) \in \mathbb{Z} \text{ for all } \xi \in \mathfrak{O}_K\}.$$

There is a basis $\mathrm{P} = \{\rho_1, \dots, \rho_n\}$ of $\mathfrak{d}^{-1}$ dual to Ω having the property that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\rho_i\omega_j) = \begin{cases} 1, & \text{when } i = j, \\ 0, & \text{when } i \neq j. \end{cases}$$

We next introduce a special case of the linear form $\lambda(\boldsymbol{\theta})$ introduced above, defining $\alpha = \alpha(\boldsymbol{\theta})$ by putting

$$\alpha(\boldsymbol{\theta}) = \theta_1\rho_1 + \ldots + \theta_n\rho_n.$$

When this and allied forms appear in an n-fold integral, we abbreviate the n-fold differential $\mathrm{d}\theta_1 \cdots \mathrm{d}\theta_n$ to $\mathrm{d}\alpha$. We also write $\mathbb{T}$ for $[0,1)^n$. In this notation, we have the orthogonality relation

$$\int_{\mathbb{T}} \mathcal{E}(\alpha\gamma)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } \gamma = 0, \\ 0, & \text{when } \gamma \in \mathfrak{O}_K \setminus \{0\}. \end{cases}$$

The introduction of all of this notation enables us to reformulate Theorem 11.1 in the form of a mean-value estimate. Define the exponential sum

$$F_k(\boldsymbol{\alpha}, \boldsymbol{\beta}; X) = \sum_{u \in \mathcal{B}(X)} \sum_{v \in \mathcal{B}(X)} \mathcal{E}(\psi_k(u, v; \boldsymbol{\alpha}, \boldsymbol{\beta})),$$

in which $\psi_k(u, v; \boldsymbol{\alpha}, \boldsymbol{\beta})$ is defined precisely as in the preamble to equation (1.6). Then, as a consequence of the analogue in number fields of Corollary 1.2, one has the following conclusion.

Corollary 11.3. *Suppose that $\varphi_j \in \mathfrak{O}_K[u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u; \boldsymbol{\varphi}) \neq 0$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$,*

$$\int_{\mathbb{T}^k} \int_{\mathbb{T}^k} |F_k(\boldsymbol{\alpha}, \boldsymbol{\beta}; X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta} \ll X^{2s+\varepsilon}.$$

We provide a proof of Theorem 11.1 in outline only, since the interested reader will have no difficulty in following the plan laid out in [11, §15] in order to modify our treatment in §§2–10 so as to substitute a number field setting in place of $\mathbb{Z}$.

Our methods involve congruences, and this requires some rapid discussion. We again consider an integer $k \geqslant 1$, and polynomials $\varphi_1, \dots, \varphi_k \in \mathfrak{O}_K[t, u]$. Throughout the argument, the ring $\mathfrak{O}_K$ replaces $\mathbb{Z}$. Let $\mathfrak{p} = (\pi)$ be a prime ideal of $\mathfrak{O}_K$, and write $p = N_{K/\mathbb{Q}}(\pi)$. We work implicitly in the $\mathfrak{p}$-adic field completing K at the place $\mathfrak{p}$, and we assume throughout that $p > (k!)^n$ (for safety). Congruences modulo p^h are now replaced throughout by congruences modulo $\mathfrak{p}^h$, and the function $e(z)$ is replaced by $\mathcal{E}(z)$. When $F : \mathbb{T}^k \to \mathbb{C}$ is integrable, we write

$$\oint F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = \int_{\mathbb{T}^k} F(\boldsymbol{\alpha})\,\mathrm{d}\alpha.$$

Next, when B is a positive integer, we define

$$\oint_{\mathfrak{p}^B} F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = p^{-kB} \sum_{u_1 \pmod{\mathfrak{p}^B}} \cdots \sum_{u_k \pmod{\mathfrak{p}^B}} F(\mathbf{u}\pi^{-B}). \tag{11.1}$$

Here, the summations on the right hand side of (11.1) are taken over complete sets of residues modulo $\mathfrak{p}^B$, with the argument $\mathbf{u}\pi^{-B}$ interpreted as follows. We interpret each coordinate $u_i\pi^{-B}$ in the argument on the right hand side of (11.1) in the shape

$$u_i\pi^{-B} = \beta_{i1}\rho_1 + \dots + \beta_{in}\rho_n,$$

with $\beta_{ij} \in \mathbb{R}$, and then reduce each coefficient β_{ij} modulo 1. With this convention, the expression $\mathbf{u}\pi^{-B}$ may be identified as belonging to $\mathbb{T}^k$. Integrals with subscripts p^B in §§2–10 are now replaced by this newly defined integral with subscript $\mathfrak{p}^B$, in obvious fashion. Now, for $\nu \in \mathfrak{O}_K[t]$, one has the orthogonality relation

$$\oint_{\mathfrak{p}^B} E(\nu\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } \nu \equiv 0 \pmod{(\mathfrak{p}^B, t^2)}, \\ 0, & \text{when } \nu \not\equiv 0 \pmod{(\mathfrak{p}^B, t^2)}. \end{cases}$$

Modified versions of Theorem 3.3 and its corollary may now be stated in the number field setting. We recall the definitions (3.6) and (3.8), though of course now in their modified apparitions.

Theorem 11.4. *Let K be an algebraic extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$. Suppose that $k \in \mathbb{N}$, and that $\mathfrak{p} = (\pi)$ is a prime ideal of $\mathfrak{O}_K$ with $p = N_{K/\mathbb{Q}}(\pi) > (k!)^n$. Then one has $\lambda(k(k+1)/2, k) = 0$.*

Corollary 11.5. *Let K be an algebraic extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$. Suppose that $k \in \mathbb{N}$, and that $\mathfrak{p} = (\pi)$ is a prime ideal of $\mathfrak{O}_K$ with $p = N_{K/\mathbb{Q}}(\pi) > (k!)^n$. Suppose that $\tau > 0$ and $\varepsilon > 0$. Let B be sufficiently large in terms of n, k, τ and ε. Put $s = k(k+1)/2$ and $H = \lceil B/k \rceil$. Then, for every $\boldsymbol{\varphi} \in \Phi_\tau(B)$, and every sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, one has*

$$U_{s,k}^B(\mathfrak{a}) \ll p^{B\varepsilon} U_{s,k}^{B,H}(\mathfrak{a}).$$

With Corollary 11.5 in hand, the proofs of Theorem 11.1 and its corollaries follow just as in the discussion of §10, as modified in the proof of [11, Theorem 15.1] described in [11, §15]. The reader should experience no difficulty in following this pedestrian pathway.

12. A function field variant

The conclusions of §1 also have their natural analogues in function fields, and again proofs are supplied relatively easily owing to the flexibility of efficient congruencing methods. We illustrate our ideas by considering the function field $\mathbb{F}_q(T)$. We once again begin by describing the infrastructure necessary to describe our function field variants.

Consider a finite field $\mathbb{F}_q$ having characteristic $p > k$, and with $q = p^l$. Associated with the polynomial ring $\mathbb{O} = \mathbb{F}_q[T]$ is the field of fractions $\mathbb{K} = \mathbb{F}_q(T)$. We now take as our basic parameter the integer X, a sufficiently large natural number, and we put

$$\mathbb{O}_X = \{\nu \in \mathbb{F}_q[T] : \deg(\nu) \leqslant X\}.$$

In the present setting, we consider the system of congruences (1.1) with

$$x_i = u_i + v_i t \quad (1 \leqslant i \leqslant 2s),$$

and denote by $\Upsilon_{s,k}(X; \boldsymbol{\varphi}; \mathbb{K})$ the number of solutions of (1.1) with $\mathbf{u}, \mathbf{v} \in \mathbb{O}_X$. The analogue of Theorem 1.1 for the class of function fields $\mathbb{F}_q(T)$ at hand may now be recorded.

Theorem 12.1. *Suppose that $\varphi_j(u) \in \mathbb{O}[t,u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u;\boldsymbol{\varphi}) \not\equiv 0 \pmod t$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then, whenever $p > k$ and $\varepsilon > 0$, one has*

$$\Upsilon_{s,k}(X;\boldsymbol{\varphi};\mathbb{K}) \ll (q^X)^{2s+\varepsilon}.$$

As in the corresponding situation in §11, analogues of Corollaries 1.2 and 1.3 appropriate for function fields follow directly from Theorem 12.1. We again record an analogue of Vinogradov's mean value theorem, though now in function fields. In this context, we denote by $J^*_{s,k}(X;\mathbb{K})$ the number of solutions of the system (1.8) with $\mathbf{u},\mathbf{v} \in \mathbb{O}_X$.

Corollary 12.2. *Let s be a positive integer. Then, whenever $p > k$ and $\varepsilon > 0$, one has*

$$J^*_{s,k}(X;\mathbb{K}) \ll (q^X)^{\varepsilon}\big((q^X)^{2s} + (q^X)^{4s-k(k+1)}\big).$$

The conclusion of Theorem 12.1 follows by applying an analogue of Theorem 3.3. In order to describe this analogue, we require some additional infrastructure. We denote by $\mathbb{K}_\infty = \mathbb{F}_q((1/T))$ the completion of $\mathbb{F}_q(T)$ at ∞. One may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i \leqslant n} a_i T^i$ for some $n \in \mathbb{Z}$ and coefficients $a_i = a_i(\alpha)$ in $\mathbb{F}_q$ for $-\infty < i \leqslant n$. We define $\operatorname{ord}\alpha$ to the largest integer i for which $a_i(\alpha) \neq 0$. We then write $\langle\alpha\rangle$ for $q^{\operatorname{ord}\alpha}$. Here, we adopt the convention that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$.

Consider the compact additive subgroup $\mathbb{T}$ of $\mathbb{K}_\infty$ defined by $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle\alpha\rangle < 1\}$. Every element α of $\mathbb{K}_\infty$ can be written uniquely in the shape $\alpha = \lfloor\alpha\rfloor + \|\alpha\|$, where $\lfloor\alpha\rfloor \in \mathbb{F}_q[T]$ and $\|\alpha\| \in \mathbb{T}$, and we may normalise any Haar measure $\mathrm{d}\alpha$ on $\mathbb{K}_\infty$ in such a manner that $\int_{\mathbb{T}} \mathrm{d}\alpha = 1$.

In order to define the analogue of the exponential function, we begin by observing that there is a non-trivial character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\mathrm{tr}(a)/p)$, where $\mathrm{tr}(a) = a + a^p + \ldots + a^{p^{l-1}}$ denotes the familiar trace map. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(\mathrm{res}(\alpha))$. One then has

$$\int_{\mathbb{T}} e(h\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } h = 0, \\ 0, & \text{when } h \in \mathbb{F}_q[T] \setminus \{0\}. \end{cases}$$

Just as in the corresponding situation in §11, the introduction of this notation allows us to reformulate Theorem 12.1 in the form of a mean value estimate. Define now

$$F_k(\boldsymbol{\alpha},\boldsymbol{\beta};X) = \sum_{u \in \mathbb{O}_X} \sum_{v \in \mathbb{O}_X} e(\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta})),$$

in which $\psi_k(u,v;\boldsymbol{\alpha},\boldsymbol{\beta})$ is again defined as in the preamble to equation (1.6). Then, as a consequence of the analogue in function fields of Corollary 1.2, one has the following conclusion.

Corollary 12.3. *Suppose that $\varphi_j \in \mathbb{O}[u]$ $(1 \leqslant j \leqslant k)$ is a system of polynomials with $W(u;\boldsymbol{\varphi}) \neq 0$. Let s be a positive integer with $s \leqslant k(k+1)/2$. Then for each $\varepsilon > 0$, one has*

$$\int_{\mathbb{T}^k} \int_{\mathbb{T}^k} |F_k(\boldsymbol{\alpha},\boldsymbol{\beta};X)|^{2s}\,\mathrm{d}\boldsymbol{\alpha}\,\mathrm{d}\boldsymbol{\beta} \ll (q^X)^{2s+\varepsilon}.$$

We again provide a proof of Theorem 12.1 in brief only. The reader will experience no difficulty in following the plan laid out in [11, §17] in order to modify our treatment in §§2–10 so as to replace the ring of integers $\mathbb{Z}$ in the former setting by its function field analogue $\mathbb{O} = \mathbb{F}_q[T]$ presently the focus of attention.

We again consider an integer $k \geqslant 1$, and polynomials $\varphi_1(u), \dots, \varphi_k(u) \in \mathbb{O}[t,u]$. Throughout the argument, the ring $\mathbb{O}$ replaces $\mathbb{Z}$. Let $\pi \in \mathbb{O}$ be a monic irreducible polynomial, having positive degree of course. We assume throughout, as previously noted, that $\mathrm{char}(\mathbb{F}_q) = p > k$. Congruences modulo p^h are now replaced throughout by congruences modulo π^h, and the function $e(z)$ of §§2–10 is replaced by its surrogate from this section. When $F : \mathbb{T}^k \to \mathbb{C}$ is integrable, we write

$$\oint F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = \int_{\mathbb{T}^k} F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha}.$$

Also, when B is a positive integer, we define

$$\oint_{\pi^B} F(\boldsymbol{\alpha})\,\mathrm{d}\boldsymbol{\alpha} = \langle \pi \rangle^{-kB} \sum_{u_1 \pmod{\pi^B}} \cdots \sum_{u_k \pmod{\pi^B}} F(\mathbf{u}\pi^{-B}),$$

where the summations are taken over complete sets of residues modulo π^B. Integrals with subscripts p^B in §§2–10 are now replaced by this newly defined integral with subscript π^B, in obvious fashion. Now, for $\nu \in \mathbb{O}[t]$, one has the orthogonality relation

$$\oint_{\pi^B} E(\alpha\nu)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{when } \nu \equiv 0 \pmod{(\pi^B, t^2)}, \\ 0, & \text{when } \nu \not\equiv 0 \pmod{(\pi^B, t^2)}. \end{cases}$$

Modified versions of Theorem 3.3 and its corollary may now be stated in the function field setting. We recall the definitions (3.6) and (3.8), now in their modified attire.

Theorem 12.4. *Let $\mathbb{O} = \mathbb{F}_q[T]$. Suppose that $k \in \mathbb{N}$, and that $\pi \in \mathbb{O}$ is a monic irreducible polynomial. Then, under the assumption that $\mathrm{ch}(\mathbb{F}_q) > k$, one has*

$$\lambda(k(k+1)/2, k) = 0.$$

Corollary 12.5. *Let $\mathbb{O} = \mathbb{F}_q[T]$. Suppose that $k \in \mathbb{N}$, and that $\pi \in \mathbb{O}$ is a monic irreducible polynomial. Suppose also that $\tau > 0$ and $\varepsilon > 0$. Let B be sufficiently large in terms of k, τ and ε. Put $s = k(k+1)/2$ and $H = \lceil B/k \rceil$. Finally, suppose that $\mathrm{ch}(\mathbb{F}_q) > k$. Then for every $\boldsymbol{\varphi} \in \Phi_\tau(B)$, and every sequence $(\mathfrak{a}) \in \mathbb{D}_0(B)$, one has*

$$U_{s,k}^B(\mathfrak{a}) \ll \langle \pi \rangle^{B\varepsilon} U_{s,k}^{B,H}(\mathfrak{a}).$$

Granted Corollary 12.5, the proofs of Theorem 12.1 and its corollaries follow just as in the discussion of §10, as modified in the proof of [11, Theorem 17.1] described in §17 of the latter source. The well-travelled reader will experience no discomfort in pursuing this pedestrian route.

13. Appendix: minimal TDI systems in dimension 2

Our goal in this section is to provide an informal classification of translation-dilation invariant (TDI) systems in two dimensions having the minimal number of equations.

Such systems as concern us are generated by polynomials $\varphi_j(x,y), \psi_j(x,y) \in \mathbb{C}[x,y]$ $(1 \leqslant j \leqslant k)$, with $k \geqslant 2$ and

$$\deg \varphi_j = \deg \psi_j \quad (1 \leqslant j \leqslant k),$$

with

$$1 \leqslant \deg \varphi_1 < \ldots < \deg \varphi_k.$$

We shall suppose that these polynomials satisfy the condition that whenever $s \in \mathbb{N}$, then the system of equations

$$\left.\begin{aligned} \sum_{i=1}^{s} \big(\varphi_j(x_i,y_i) - \varphi_j(x_{s+i},y_{s+i})\big) = 0 \\ \sum_{i=1}^{s} \big(\psi_j(x_i,y_i) - \psi_j(x_{s+i},y_{s+i})\big) = 0 \end{aligned}\right\} \quad (1 \leqslant j \leqslant k) \tag{13.1}$$

is translation-dilation invariant. By this we mean that whenever $\mathbf{x}, \mathbf{y}$ is a solution of the system (13.1), then for any $q \in \mathbb{C}^\times$ and $a, b \in \mathbb{C}$, the tuple $q\mathbf{x} + a, q\mathbf{y} + b$ is also a solution of the system (13.1). We show that, up to reasonable notions of equivalence and non-degeneracy of systems, all systems of the shape (13.1) fall into one of three families simple to describe.

We observe first that, by taking appropriate linear combinations of the polynomials $\varphi_j(x,y)$ and $\psi_j(x,y)$, for $1 \leqslant j \leqslant k$, we may suppose without loss of generality that these polynomials are both homogeneous. This is an immediate consequence of the dilation invariance condition associated with the system (13.1), specifically that $q\mathbf{x}, q\mathbf{y}$ should be a solution of (13.1) whenever $\mathbf{x}, \mathbf{y}$ is a solution.

The TDI property also ensures that for $1 \leqslant j \leqslant k$, the polynomials

$$\frac{\partial \varphi_j}{\partial x}(x,y), \quad \frac{\partial \varphi_j}{\partial y}(x,y), \quad \frac{\partial \psi_j}{\partial x}(x,y), \quad \frac{\partial \psi_j}{\partial y}(x,y),$$

must all lie in the set

$$\big\{\lambda \varphi_{j-1}(x,y) + \mu \psi_{j-1}(x,y) : \lambda, \mu \in \mathbb{C}\big\}.$$

In order to confirm this observation, one has merely to observe that a Taylor series expansion of $\varphi_j(x+a, y+b)$ takes the shape

$$\varphi_j(x,y) + \Big(a\frac{\partial \varphi_j}{\partial x}(x,y) + b\frac{\partial \varphi_j}{\partial y}(x,y)\Big) + \ldots,$$

with a similar expansion holding for $\psi_j(x+a, y+b)$. Then, on substituting this expansion into the system (13.1), we see that the TDI property of this system requires that

$$\sum_{i=1}^{s} \Big(\frac{\partial \varphi_j}{\partial x}(x_i,y_i) - \frac{\partial \varphi_j}{\partial x}(x_{s+i},y_{s+i})\Big) = 0$$

and

$$\sum_{i=1}^{s} \Big(\frac{\partial \varphi_j}{\partial y}(x_i,y_i) - \frac{\partial \varphi_j}{\partial y}(x_{s+i},y_{s+i})\Big) = 0,$$

with a similar property associated to $\psi_j(x,y)$. It follows that

$$\operatorname{span}_{\mathbb{C}}\left\{\frac{\partial\varphi_j}{\partial x},\frac{\partial\varphi_j}{\partial y},\frac{\partial\psi_j}{\partial x},\frac{\partial\psi_j}{\partial y}\right\}\subseteq\operatorname{span}_{\mathbb{C}}\{\varphi_{j-1},\psi_{j-1}\}\quad(2\leqslant j\leqslant k),\tag{13.2}$$

whence, in particular,

$$\dim\operatorname{span}_{\mathbb{C}}\left\{\frac{\partial\varphi_j}{\partial x},\frac{\partial\varphi_j}{\partial y},\frac{\partial\psi_j}{\partial x},\frac{\partial\psi_j}{\partial y}\right\}\leqslant 2\quad(2\leqslant j\leqslant k).\tag{13.3}$$

We concentrate initially on the consequences of the relations (13.2) and (13.3) relating to the polynomials φ_j. By a second application of (13.2), we find that

$$\dim\operatorname{span}_{\mathbb{C}}\left\{\frac{\partial^2\varphi_k}{\partial x^2},\frac{\partial^2\varphi_k}{\partial x\,\partial y},\frac{\partial^2\varphi_k}{\partial y^2}\right\}\leqslant 2.$$

Thus, there exist $a,b,c\in\mathbb{C}$, not all zero, such that

$$a\frac{\partial^2\varphi_k}{\partial x^2}+b\frac{\partial^2\varphi_k}{\partial x\,\partial y}+c\frac{\partial^2\varphi_k}{\partial y^2}=0.\tag{13.4}$$

For ease of exposition, write

$$\varphi_k^{(r)}=\frac{\partial^k\varphi_k}{\partial x^r\,\partial y^{k-r}}\quad(0\leqslant r\leqslant k),$$

and note that each quantity $\varphi_k^{(r)}$ is a constant. Then we deduce from (13.4) that

$$a\varphi_k^{(r+2)}+b\varphi_k^{(r+1)}+c\varphi_k^{(r)}=0\quad(0\leqslant r\leqslant k-2).\tag{13.5}$$

We divide our further discussion into three cases:

(a) Suppose first that the relation (13.4) holds with $a\neq 0$. In this case we examine the characteristic equation

$$a\lambda^2+b\lambda+c=0\tag{13.6}$$

of the recurrence relation (13.5). Let λ_1 and λ_2 be the roots of the equation (13.6). Then, for some $A,B\in\mathbb{C}$, one has

$$\varphi_k^{(r)}=\begin{cases}A\lambda_1^r+B\lambda_2^r, & \text{when } \lambda_1\neq\lambda_2,\\ (Ar+B)\lambda_1^r, & \text{when } \lambda_1=\lambda_2.\end{cases}$$

When $\lambda_1\neq\lambda_2$, this observation reveals that the coefficient c_r of x^ry^{k-r} in $\varphi_k(x,y)$ satisfies

$$r!(k-r)!c_r=\varphi_k^{(r)}=A\lambda_1^r+B\lambda_2^r,$$

and hence

$$k!\varphi_k(x,y)=\sum_{r=0}^{k}\binom{k}{r}\varphi_k^{(r)}x^ry^{k-r}=A(\lambda_1x+y)^k+B(\lambda_2x+y)^k.\tag{13.7}$$

When $\lambda_1=\lambda_2$, meanwhile, the recurrence relation has a singular solution. One finds in this scenario that the coefficient c_r of x^ry^{k-r} in $\varphi_k(x,y)$ satisfies

$$r!(k-r)!c_r=\varphi_k^{(r)}=(Ar+B)\lambda_1^r,$$

whence

$$k!\varphi_k(x,y)=\sum_{r=0}^{k}\binom{k}{r}\varphi_k^{(r)}x^ry^{k-r}=Ak\lambda_1x(\lambda_1x+y)^{k-1}+B(\lambda_1x+y)^k. \tag{13.8}$$

(b) Next we suppose that the relation (13.4) holds with $a=c=0$, whence $b\neq 0$. Then we have

$$\frac{\partial^2\varphi_k}{\partial x\,\partial y}=0,$$

so that for some $A,B\in\mathbb{C}$, one has $\varphi_k(x,y)=Ax^k+By^k$.

(c) Finally, we suppose that the relation (13.4) holds with $a=0$ and $c\neq 0$. In this situation we may interchange the roles of x and y to obtain formulae of the shapes (13.7) and (13.8), save that x and y have been interchanged.

A similar argument applies for the polynomial $\psi_k(x,y)$. Thus, we see that for suitable complex numbers A' and B', and for certain characteristic equation roots λ_1' and λ_2', the polynomial $\psi_k(x,y)$ takes one of the forms

$$A'x^k+B'y^k,\quad A'(\lambda_1'x+y)^k+B'(\lambda_2'x+y)^k,\quad A'k\lambda_1'x(\lambda_1'x+y)^{k-1}+B'(\lambda_1'x+y)^k,$$

or similar expressions with the roles of x and y interchanged.

We now return to examine the consequences of our classification for the relation

$$\dim\operatorname{span}_{\mathbb{C}}\left\{\frac{\partial\varphi_k}{\partial x},\frac{\partial\varphi_k}{\partial y},\frac{\partial\psi_k}{\partial x},\frac{\partial\psi_k}{\partial y}\right\}\leqslant 2$$

implied by (13.3). Note that we also require that

$$\dim\operatorname{span}_{\mathbb{C}}\{\varphi_k,\psi_k\}=2.$$

There is no loss of generality in replacing (φ_k,ψ_k) by the pair (Φ_k,Ψ_k), where

$$\Phi_k=\alpha\varphi_k+\beta\psi_k\quad\text{and}\quad\Psi_k=\gamma\varphi_k+\delta\psi_k,$$

for any

$$\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in\mathrm{GL}_2(\mathbb{C}).$$

Likewise, we may replace $\varphi_k(x,y)$ and $\psi_k(x,y)$ by

$$\varphi_k(\mu x+\nu y,\rho x+\sigma y)\quad\text{and}\quad\psi_k(\mu x+\nu y,\rho x+\sigma y)$$

for any

$$\begin{pmatrix}\mu&\nu\\ \rho&\sigma\end{pmatrix}\in\mathrm{GL}_2(\mathbb{C}).$$

With such transformations in mind, a modicum of contemplation reveals that our classification discussed thus far implies that, up to the equivalence implicit in these $\mathrm{GL}_2(\mathbb{C})$ transformations just considered, the polynomial pairs $(\varphi_k(x,y),\psi_k(x,y))$ must take one of the forms

$$(x^k,y^k)\quad\text{and}\quad(x^k,x^{k-1}y).$$

It then follows that the systems of polynomials defining the equations (13.1) are equivalent to ones taking the form

$$(\varphi_j(x,y),\psi_j(x,y))=(x^j,y^j)\quad(1\leqslant j\leqslant k),$$

or

$$(\varphi_j(x,y),\psi_j(x,y)) = (x^j, x^{j-1}y) \quad (1 \leqslant j \leqslant k).$$

One additional detail now briefly detains us, for we have considered polynomials defined over $\mathbb{C}[x,y]$, and ones equivalent via $\mathrm{GL}_2(\mathbb{C})$ transformations. If we seek to restrict attention to polynomials defined over $\mathbb{Z}[x,y]$, then similar arguments apply, although our transformations must apply in such a manner that the resulting polynomials remain defined over $\mathbb{Z}[x,y]$. Since the characteristic roots λ_1, λ_2 introduced above must lie in a quadratic extension of $\mathbb{Q}$, when $\lambda_1 \neq \lambda_2$, and must lie in $\mathbb{Q}$, when $\lambda_1 = \lambda_2$, we arrive at the following conclusion. Thus, the polynomials $(\varphi_j(x,y),\psi_j(x,y))$ must be equivalent via $\mathrm{GL}_2(\mathbb{Q})$ transformations to pairs taking one of the following forms, for $1 \leqslant j \leqslant k$:

(a) When λ_1 and λ_2 are distinct rational numbers, then

$$\varphi_j(x,y) = x^j \quad \text{and} \quad \psi_j(x,y) = y^j.$$

(b) When $\lambda_1 = \lambda_2$, a rational number, then

$$\varphi_j(x,y) = x^j \quad \text{and} \quad \psi_j(x,y) = x^{j-1}y.$$

(c) When λ_1 and λ_2 are distinct, but neither are rational, then necessarily λ_1 and λ_2 are conjugate quadratic irrational numbers in a number field of the shape $\mathbb{Q}(\sqrt{d})$, for some non-square integer d. One then has

$$\varphi_j(x,y) = (x+y\sqrt{d})^j + (x-y\sqrt{d})^j$$

and

$$\psi_j(x,y) = \frac{1}{\sqrt{d}}\big((x+y\sqrt{d})^j - (x-y\sqrt{d})^j\big),$$

so that

$$\varphi_j(x,y) + \sqrt{d}\psi_j(x,y) = (x+y\sqrt{d})^j.$$

So far as mean values of the corresponding exponential sums are concerned, the scenario (a) is accommodated via the classical theory resolved in work of the author [10] and [11], and also [2]. Meanwhile, the scenario (c) is handled via the extension of Vinogradov's mean value theorem to quadratic number fields, a matter handled for quite general number fields in the author's work [11, §15]. Finally, the scenario (b) is the subject of this memoir.

We finish by observing that the system (13.1), in the scenarios (a), (b) and (c), correspond to systems of Vinogradov type over $\mathbb{Z}[t]$ modulo $\omega(t)$, in the following sense. Thus, scenario (a) corresponds to the Vinogradov system of congruences

$$\sum_{i=1}^{s}\big((x_i+y_it)^j - (x_{s+i}+y_{s+i}t)^j\big) \equiv 0 \pmod{\omega(t)} \quad (1 \leqslant j \leqslant k), \tag{13.9}$$

wherein $\omega(t)$ is a quadratic polynomial in $\mathbb{Z}[t]$ having two distinct rational roots. Meanwhile, scenario (b) corresponds to the Vinogradov system of congruences (13.9) in which $\omega(t)$ is a quadratic polynomial in $\mathbb{Z}[t]$ having repeated (rational) roots. Finally, scenario (c) corresponds to the Vinogradov system of congruences (13.9) in which $\omega(t)$ is a quadratic polynomial in $\mathbb{Z}[t]$ irreducible over $\mathbb{Q}$, but splitting in $\mathbb{Q}(\sqrt{d})$.

References

[1] J. Bourgain, C. Demeter and S. Guo, *Sharp bounds for the cubic Parsell-Vinogradov system in two dimensions*, Adv. Math. **320** (2017), 827–875.

[2] J. Bourgain, C. Demeter and L. Guth, *Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three*, Ann. of Math. (2) **184** (2016), no. 2, 633–682.

[3] J. Brandes and T. D. Wooley, *Vinogradov systems with a slice off*, Mathematika **63** (2017), no. 3, 797–817.

[4] S. Guo and R. Zhang, *On integer solutions of Parsell-Vinogradov systems*, Invent. Math. **218** (2019), no. 1, 1–81.

[5] S. Guo and P. Zorin-Kranich, *Decoupling for moment manifolds associated to Arkhipov-Chubarikov-Karatsuba systems*, Adv. Math. **360** (2020), article no. 106889, 56pp.

[6] S. T. Parsell, S. M. Prendiville and T. D. Wooley, *Near-optimal mean value estimates for multidimensional Weyl sums*, Geom. Funct. Anal. **23** (2013), 1962–2024.

[7] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Ann. of Math. (2) **175** (2012), no. 3, 1575–1627.

[8] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, Duke Math. J. **162** (2013), 673–730.

[9] T. D. Wooley, *Multigrade efficient congruencing and Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **111** (2015), no. 3, 519–560.

[10] T. D. Wooley, *The cubic case of the main conjecture in Vinogradov's mean value theorem*, Adv. Math. **294** (2016), 532–561.

[11] T. D. Wooley, *Nested efficient congruencing and relatives of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **118** (2019), no. 4, 942–1016.

[12] T. D. Wooley, *The main conjecture for a Vinogradov subsystem*, submitted, preprint, 11pp.; arXiv:2610.05515.

[13] T. D. Wooley, *Sharp mean value estimates in the absence of translation-dilation invariance*, submitted, preprint, 13pp.; arXiv:2610.05525.

Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907-2067, USA

Email address: twooley@purdue.edu