Mathematika 63 (2017) 292–350 © 2016 University College London
doi:10.1112/S0025579316000279

APPROXIMATING THE MAIN CONJECTURE IN VINOGRADOV'S MEAN VALUE THEOREM

TREVOR D. WOOLEY

Abstract. We apply multigrade efficient congruencing to estimate Vinogradov's integral of degree k for moments of order $2s$, establishing strongly diagonal behaviour for $1 \leqslant s \leqslant \frac{1}{2}k(k+1)-\frac{1}{3}k+o(k)$. In particular, as $k \to \infty$, we confirm the main conjecture in Vinogradov's mean value theorem for a proportion asymptotically approaching 100% of the critical interval $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$.

§1. *Introduction.* Our focus in this paper is the Vinogradov system of Diophantine equations. When k and s are natural numbers, and X is a large real number, denote by $J_{s,k}(X)$ the number of integral solutions of the system

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j \quad (1 \leqslant j \leqslant k), \tag{1.1}$$

with $1 \leqslant x_i, y_i \leqslant X$ $(1 \leqslant i \leqslant s)$. Bounds for $J_{s,k}(X)$ are linked via orthogonality to mean value estimates for exponential sums and hence feature prominently in the analysis of problems spanning the analytic theory of numbers. Thus, for example, the strongest available conclusions concerning the validity of the asymptotic formula in Waring's problem, the zero-free region for the Riemann zeta function and the distribution modulo 1 of polynomial sequences all depend on bounds for $J_{s,k}(X)$. We refer the reader to the comprehensive sources due to Arkhipov *et al* [**1**] and Vinogradov [**11**] for discussion of the many applications of such estimates, collectively described as instances of *Vinogradov's mean value theorem*. A more recent tour of the subject is described in [**18**]. By considering mean values of an associated exponential sum, it follows that the validity of the *strongly diagonal* estimate

$$J_{s,k}(X) \ll X^{s+\varepsilon}, \tag{1.2}$$

for $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$, would imply the *main conjecture* in Vinogradov's mean value theorem, which asserts that for each $\varepsilon > 0$, one has

$$J_{s,k}(X) \ll X^{\varepsilon}(X^s + X^{2s-k(k+1)/2}). \tag{1.3}$$

Here and throughout this paper, the implicit constants associated with Vinogradov's notation $\ll$ and $\gg$ may depend on s, k and ε.

For almost all of the eighty year history of the subject, an estimate of the strength of (1.3) has seemed a very remote prospect indeed, for until only a

Received 10 March 2016, published online 21 December 2016.
MSC (2010): 11L15, 11L07, 11P55 (primary).

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

year before this paper was written, the bound (1.2) was known to hold only for $s \leqslant k+1$ (see [**8**, Lemma 5.4]). By enhancing the *efficient congruencing* method introduced in [**15**], recent work of the author joint with Ford [**4**] has established the estimate (1.2) for $s \leqslant \frac{1}{4}(k+1)^2$, amounting to half of the range $s \leqslant \frac{1}{2}k(k+1)$ in which diagonal behaviour dominates (1.3). Our goal in this paper is to adapt the *multigrade efficient congruencing method* detailed in our very recent work [**19**] so as to obtain strongly diagonal estimates of the shape (1.2). It transpires that when k is large, we are able to establish the validity of the conjectured estimate (1.2) for almost all s in the critical interval $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$ or, as one might say, a proportion asymptotically approaching 100% of the critical interval. We consequently find ourselves within a whisker of the proof of the main conjecture (1.3), a situation hitherto unprecedented in the analysis of mean value estimates for exponential sums of large degree.

The most precise form of our new estimate may be found in Theorem 2.1 below. For the present, we restrict ourselves to a conclusion relatively simple to state that is indicative of what may now be achieved.

THEOREM 1.1. *Let k be a natural number with $k \geqslant 7$, put $r = k - \lceil 2\sqrt{k} \rceil + 2$ and suppose that s is an integer satisfying*

$$1 \leqslant s \leqslant kr - \frac{1}{2}r(r-1) - \sum_{m=1}^{r-1} \frac{m(r-m)}{s-r-m}.$$

Then, for each $\varepsilon > 0$, one has $J_{s,k}(X) \ll X^{s+\varepsilon}$.

A modicum of computation reveals that when k is large, this estimate confirms the main conjecture (1.3) for almost all of the critical interval of exponents $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$.

COROLLARY 1.2. *When s and k are natural numbers with $k \geqslant 7$ and*

$$1 \leqslant s \leqslant \tfrac{1}{2}k(k+1) - \tfrac{7}{3}k,$$

then, for each $\varepsilon > 0$, one has $J_{s,k}(X) \ll X^{s+\varepsilon}$.

As we have already noted, a conclusion analogous to Theorem 1.1 is made available in [**4**, Theorem 1.1] in the more limited range $1 \leqslant s \leqslant \frac{1}{4}(k+1)^2$. Earlier conclusions were limited to the much shorter interval $1 \leqslant s \leqslant k+1$ (see [**10**] for a particularly precise statement in this situation). In view of the lower bound

$$J_{s,k}(X) \gg X^s + X^{2s-k(k+1)/2}, \tag{1.4}$$

that arises by considering the diagonal solutions of (1.1) with $\mathbf{x} = \mathbf{y}$, together with a lower bound for the product of local densities (see [**9**, equation (7.4)]), one sees that the conclusion of Theorem 1.1 cannot hold when $s > \frac{1}{2}k(k+1)$.

The gap between our new result and a complete proof of the main conjecture (1.3) stands at $\frac{7}{3}k$ variables, amounting to a proportion $O(1/k)$ of

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Table 1: Values for $D(k)$ described in Theorem 1.4.

k	4	5	6	7	8	9	10	11	12
$D(k)$	8	10	17	20	29	38	44	55	68
$\frac{1}{2}k(k+1)$	10	15	21	28	36	45	55	66	78
k	13	14	15	16	17	18	19	20	
$D(k)$	75	90	105	122	132	151	170	191	
$\frac{1}{2}k(k+1)$	91	105	120	136	153	171	190	210	

the length of the critical interval $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$. In a certain sense, therefore, our conclusion establishes the main conjecture in 100% of the critical interval as $k \to \infty$, justifying the assertion concluding our opening paragraph. In §11, we describe some modifications to our basic strategy which offer some improvement in the conclusion of Corollary 1.2 towards the main conjecture (1.3). We have opted for a relatively concise account of this improvement, since the details of the associated argument are of sufficient complexity that the key elements of our basic strategy would be obscured were we to make this account the main focus of our exposition.

THEOREM 1.3. *When k is a sufficiently large natural number and s is an integer satisfying*

$$1 \leqslant s \leqslant \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3},$$

then, for each $\varepsilon > 0$, one has $J_{s,k}(X) \ll X^{s+\varepsilon}$.

Our methods are applicable not only for large values of k. By taking $r = k - \lceil 2\sqrt{k} \rceil + 2$ in Theorem 2.1 below, one may establish an improvement on the conclusion of [**4**, Theorem 1.1]. We note here that the latter delivers the bound $J_{s,k}(X) \ll X^{s+\varepsilon}$ for $1 \leqslant s \leqslant \frac{1}{4}(k+1)^2$.

THEOREM 1.4. *Define the number $D(k)$ as in Table 1. Then, whenever $k \geqslant 4$ and $1 \leqslant s \leqslant D(k)$, one has $J_{s,k}(X) \ll X^{s+\varepsilon}$.*

One may enquire concerning the impact of our methods in the case $k = 3$. Here, although the methods of this paper do not apply directly, a careful variant of our ideas proves surprisingly successful. This is a matter which we address elsewhere (see [**20**]).

A trivial consequence of the estimate supplied by Theorems 1.1 and 1.3 provides a new upper bound for $J_{s,k}(X)$ at the critical value $s = \frac{1}{2}k(k+1)$.

THEOREM 1.5. *Suppose that k is a large natural number. Then*

$$J_{(1/2)k(k+1),k}(X) \ll X^{k(k+1)/2+\Delta},$$

where $\Delta = (\frac{1}{3} + o(1))k$.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

As remarked in the discussion following the statement of [4, Theorem 1.2], the work of that paper shows that a conclusion analogous to Theorem 1.5 holds with $\Delta = (\frac{3}{2} - \sqrt{2})k^2 + O(k)$. Our new result for the first time in the subject obtains a conclusion in which $\Delta = o(k^2)$. Indeed, one now has a good asymptotic approximation to the main conjecture (1.3) for all s, since we have

$$J_{s,k}(X) \ll X^{\Delta_{s,k}}(X^s + X^{2s-k(k+1)/2}),$$

with $\Delta_{s,k} = O(k)$ for all s.

We are also able to obtain a very slight improvement in our previous bound for the the number of variables required to establish the anticipated asymptotic formula in Waring's problem, at least, when k is sufficiently large. We refer the reader to Theorem 12.2 for an account of this new bound, and to Theorem 12.1 for some consequences of Theorem 1.3 in the context of Tarry's problem. The latter is worth highlighting already. When h, k and s are positive integers with $h \geqslant 2$, consider the Diophantine system

$$\sum_{i=1}^{s} x_{i1}^j = \sum_{i=1}^{s} x_{i2}^j = \cdots = \sum_{i=1}^{s} x_{ih}^j \quad (1 \leqslant j \leqslant k). \tag{1.5}$$

Let $W(k,h)$ denote the least natural number s having the property that the simultaneous equations (1.5) possess an integral solution $\mathbf{x}$ with

$$\sum_{i=1}^{s} x_{iu}^{k+1} \neq \sum_{i=1}^{s} x_{iv}^{k+1} \quad (1 \leqslant u < v \leqslant h).$$

Also, let $P(k,h)$ denote the least natural number s having the property that the simultaneous equations (1.5) possess an integral solution $\mathbf{x}$ with

$$\{x_{1u}, \dots, x_{su}\} \neq \{x_{1v}, \dots, x_{sv}\} \quad (1 \leqslant u < v \leqslant h).$$

It is trivial that $P(k,h) \leqslant W(k,h)$, and relatively straightforward to establish that when h and k are natural numbers with $h \geqslant 2$, then $P(k,h) \leqslant \frac{1}{2}k(k+1)+1$ (see Hardy and Wright [5, Theorem 409]). The corresponding bound for the more difficult quantity $W(k,h)$ has, however, hitherto remained far beyond reach. By applying Theorem 1.5, we are now able to show in Theorem 12.1 that when h and k are natural numbers with $h \geqslant 2$ and k sufficiently large, then one has $W(k,h) \leqslant \frac{1}{2}k(k+1)+1$. As noted earlier, other applications of Vinogradov's mean value theorem can be found in the classical literature on the subject, such as [1, 11, 12].

We have written elsewhere concerning the basic strategy underlying efficient congruencing; a sketch of the basic ideas can be found in [15, §2]. The multigrade efficient congruencing method seeks to more fully extract the information available from congruences of different levels. We direct the reader to [19] for an introduction to such ideas. Perhaps it is worth noting that the main challenge in the present adaptation of multigrade efficient congruencing is that

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

no loss of more than a constant factor can be tolerated in the basic congruencing steps. This task is complicated as we progress through the iteration, stepping from congruences modulo p^a to congruences modulo p^b, since the ratio b/a can vary widely according to which of the several possible moduli dominate proceedings at each stage of the iteration. Finally, we remark that although one can envision further improvement in the range of s accommodated by Theorem 1.3, it would seem that a new idea is required to replace the defect $\frac{1}{3}k$ by a quantity ck with $c < \frac{1}{3}$. The term $\frac{1}{3}k$ seems to be an unavoidable consequence of the application of Hölder's inequality underlying Lemmas 7.1 and 11.3 that teases apart the information available from congruences of different levels.

Recent developments (added 29th May 2016). The area of research focusing on Vinogradov's mean value theorem and its hinterland has recently undergone a burst of activity, with rapid progress from several quarters. On the one hand, the author [**20**] has applied the methods of this paper to establish the cubic case of the main conjecture in full. On the other hand, very recent work of Bourgain *et al* [**2**] extended the range

$$1 \leqslant s \leqslant \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3},$$

in which our Theorem 1.3 applies, to the full critical range $1 \leqslant s \leqslant \frac{1}{2}k(k+1)$, thereby confirming the main conjecture in full. The latter work [**2**] was submitted to the arXiv on 14th December 2015, the most recent (third) revision having been submitted on 1st April 2016. This paper is in all essential mathematical respects identical with a version predating the work of Bourgain *et al*, and was submitted to the arXiv on 13th January 2014. However, its appearance in print has been delayed by forces beyond the author's control.

The methods of this paper may be seen as a p-adic version of the method underlying [**2**], the latter being more akin to Vinogradov's use of real short intervals dating from the 1930s. Two comments are in order here. First, the p-adic methods of the present work continue to represent a useful alternative to those of [**2**], since they are easily adapted to other number-theoretic situations, such as those relevant to number fields and function fields. Second, it seems now very likely that the methods of the present paper, in combination with subsequent developments, will also establish the main conjecture in full, in all the settings just outlined as well as in the real setting explored in [**2**]. It seems reasonable to speculate that methods of the widest applicability will incorporate elements of both approaches.

§2. *The basic infrastructure.* We begin our discussion of the proof of Theorem 1.1 by describing the components and basic notation that we subsequently assemble into the apparatus required for the multigrade efficient congruencing method. This is very similar to that introduced in our recent work [**19**], and resembles the infrastructure of our earliest work on efficient congruencing [**15**]. The reader might wonder whether some kind of universal account could be given that would encompass all possibilities. For the present

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

such a goal seems premature, since innovations are the rule for such a rapidly evolving circle of ideas. Instead, novel consequences of the method seem to require careful arrangement of parameters together with a significant measure of artistry.

We establish Theorem 1.1 as a consequence of a theorem that in many circumstances is somewhat sharper, though more complicated to state.

THEOREM 2.1. *Suppose that s, k and r are natural numbers with $k \geqslant 4$,*

$$2 \leqslant r \leqslant k - \lceil 2\sqrt{k} \rceil + 2 \quad \textit{and} \quad \max\{2r-1, \tfrac{1}{2}r(r-1) + \Delta\} \leqslant s < s_1,$$

where

$$s_1 = \frac{1}{2}\Big(kr - \frac{1}{2}r(r-1) - \Delta\Big)\Big(1 + \sqrt{1 - \frac{4r(r(r-1)/2 + \Delta)}{(kr - r(r-1)/2 - \Delta)^2}}\Big)$$

and

$$\Delta = \sum_{m=1}^{r-1} \frac{m(r-m)}{s-m}.$$

Then, for each $\varepsilon > 0$, one has $J_{s+r}(X) \ll X^{s+r+\varepsilon}$.

We consider k to be fixed, and abbreviate $J_{s,k}(X)$ to $J_s(X)$ without further comment. Let $s \in \mathbb{N}$ be arbitrary, and define $\lambda_s^* \in \mathbb{R}$ by means of the relation

$$\lambda_s^* = \limsup_{X \to \infty} \frac{\log J_s(X)}{\log X}.$$

Thus, for each $\varepsilon > 0$, and any $X \in \mathbb{R}$ sufficiently large in terms of s, k and ε, one has $J_s(X) \ll X^{\lambda_s^* + \varepsilon}$. Note that the lower bound (1.4) combines with a trivial estimate for $J_s(X)$ to show that $s \leqslant \lambda_s^* \leqslant 2s$, whilst the conjectured upper bound (1.2) implies that $\lambda_s^* = s$ for $s \leqslant \frac{1}{2}k(k+1)$.

Next, we recall some standard notational conventions. The letters s and k denote natural numbers with $k \geqslant 3$, and ε denotes a sufficiently small positive number. Our basic parameter is X, a large real number depending at most on k, s and ε, unless otherwise indicated. Whenever ε appears in a statement, we assert that the statement holds for each $\varepsilon > 0$. As usual, we write $\lfloor \psi \rfloor$ to denote the largest integer no larger than ψ, and $\lceil \psi \rceil$ to denote the least integer no smaller than ψ. We make sweeping use of vector notation. Thus, with t implied from the environment at hand, we write $\mathbf{z} \equiv \mathbf{w} \pmod{p}$ to denote that $z_i \equiv w_i \pmod{p}$ $(1 \leqslant i \leqslant t)$, or $\mathbf{z} \equiv \xi \pmod{p}$ to denote that $z_i \equiv \xi \pmod{p}$ $(1 \leqslant i \leqslant t)$, or $[\mathbf{z} \pmod{q}]$ to denote the t-tuple $(\zeta_1, \dots, \zeta_t)$, where for $1 \leqslant i \leqslant t$ one has $1 \leqslant \zeta_i \leqslant q$ and $z_i \equiv \zeta_i \pmod{q}$. Finally, we employ the convention that whenever $G : [0,1)^k \to \mathbb{C}$ is integrable, then

$$\oint G(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} = \int_{[0,1)^k} G(\boldsymbol{\alpha})\, d\boldsymbol{\alpha}.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Thus, on writing

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1 \leqslant x \leqslant X} e(\alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_k x^k),$$

where as usual $e(z)$ denotes $\mathrm{e}^{2\pi \mathrm{i} z}$, it follows from orthogonality that

$$J_t(X) = \oint |f_k(\boldsymbol{\alpha}; X)|^{2t}\, d\boldsymbol{\alpha} \quad (t \in \mathbb{N}). \tag{2.1}$$

We next introduce the parameters which define the iterative method that is the central concern of this paper. We suppose throughout that $k \geqslant 4$, and put

$$r_0 = k - \lceil 2\sqrt{k} \rceil + 2. \tag{2.2}$$

We take r to be an integral parameter satisfying $1 \leqslant r \leqslant r_0$, and we consider a natural number s with $k + 1 \leqslant s \leqslant \frac{1}{2}k(k+1)$. We then define $\Delta = \Delta(r, s)$ by taking

$$\Delta = \sum_{m=1}^{r-1} \frac{m(r-m)}{s-m} \tag{2.3}$$

and suppose in what follows that

$$s \geqslant \max\{2r - 1, \tfrac{1}{2}r(r-1) + \Delta\}. \tag{2.4}$$

Next, we put

$$\mathfrak{a} = kr - \tfrac{1}{2}r(r-1) - \Delta \quad \text{and} \quad \mathfrak{b} = r(\tfrac{1}{2}r(r-1) + \Delta), \tag{2.5}$$

and then define

$$\theta_+ = \tfrac{1}{2}(\mathfrak{a} + \sqrt{\mathfrak{a}^2 - 4\mathfrak{b}}) \quad \text{and} \quad \theta_- = \tfrac{1}{2}(\mathfrak{a} - \sqrt{\mathfrak{a}^2 - 4\mathfrak{b}}). \tag{2.6}$$

We will suppose throughout that $s < \theta_+$. Here, some explanation may defuse confusion that may arise from the implicit dependence of θ_+ on s. In practice, the definition (2.3) ensures that Δ is no larger than about $\frac{1}{3}k$, and hence one finds from (2.6) that θ_+ is roughly

$$kr - \tfrac{1}{2}r(r+1) - \Delta > \tfrac{1}{2}r(r-1) + \Delta.$$

The condition $s < \theta_+$ is consequently easily verified, since there are relatively few values of s to check, and in particular none exceeding $\frac{1}{2}k(k+1)$. Likewise, the condition (2.4) is also easily verified for the values of s open to discussion.

Our goal is to establish that $\lambda^*_{s+r} = s + r$. Having established the latter, one finds by applying Hölder's inequality to the right-hand side of (2.1) that whenever $1 \leqslant t \leqslant s + r$, one has

$$J_t(X) \leqslant \left(\oint |f_k(\boldsymbol{\alpha}; X)|^{2s+2r}\, d\boldsymbol{\alpha} \right)^{t/(s+r)} \ll X^{t+\varepsilon},$$

whence $\lambda^*_t = t$. Thus, it is clear that the main conclusions of this paper follow by focusing on λ^*_{s+r}. Henceforth, for brevity we write $\lambda = \lambda^*_{s+r}$.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Let R be a natural number sufficiently large in terms of s and k. Specifically, we choose R as follows. From (2.5) and (2.6), one finds that $\theta_+\theta_- = \mathfrak{b}$, and so the hypothesis $s < \theta_+$ ensures that

$$\theta_- = \mathfrak{b}/\theta_+ < \mathfrak{b}/s \leqslant \mathfrak{b}/(\tfrac{1}{2}r(r-1)+\Delta) = r.$$

Observe next that $\theta_+ > \theta_-$, so that on writing $\tau = \theta_+/\theta_-$, one finds that

$$\begin{aligned}\frac{1}{\theta_-^R}\biggl(\frac{\theta_+^{R+1}-\theta_-^{R+1}}{\theta_+-\theta_-} - \frac{\theta_+\theta_-}{r\sqrt{k}}\biggl(\frac{\theta_+^R-\theta_-^R}{\theta_+-\theta_-}\biggr)\biggr) &= \frac{\tau^{R+1}-1}{\tau-1} - \frac{\tau\theta_-}{r\sqrt{k}}\biggl(\frac{\tau^R-1}{\tau-1}\biggr)\\ &> \biggl(1-\frac{1}{\sqrt{k}}\biggr)\biggl(\frac{\tau^{R+1}-1}{\tau-1}\biggr)\\ &> (1-1/\sqrt{k})\tau^R.\end{aligned}$$

Hence, we obtain the upper bound

$$(1-1/\sqrt{k})\theta_+^R < \frac{\theta_+^{R+1}-\theta_-^{R+1}}{\theta_+-\theta_-} - \frac{\theta_+\theta_-}{r\sqrt{k}}\biggl(\frac{\theta_+^R-\theta_-^R}{\theta_+-\theta_-}\biggr).$$

Recall again our assumption that $s < \theta_+$, and put $\nu = \theta_+ - s > 0$. Then we have

$$s^n = \theta_+^n(1-\nu/\theta_+)^n \leqslant \theta_+^n \mathrm{e}^{-\nu n/\theta_+}.$$

Consequently, if we take $R = \lceil W\theta_+/\nu\rceil$, with W a large enough integer, then we ensure that

$$s^R \leqslant \mathrm{e}^{-W}\theta_+^R < (1-1/\sqrt{k})\theta_+^R,$$

whence

$$s^R < \frac{\theta_+^{R+1}-\theta_-^{R+1}}{\theta_+-\theta_-} - \frac{\theta_+\theta_-}{r\sqrt{k}}\biggl(\frac{\theta_+^R-\theta_-^R}{\theta_+-\theta_-}\biggr). \tag{2.7}$$

The significance of this condition will become apparent in due course (see equation (8.1) below, and the ensuing discussion).

Having fixed R satisfying these conditions, we take N to be a natural number sufficiently large in terms of s, k and R, and then put

$$B = Nk^N, \qquad \theta = (17N^2(s+k))^{-3RN}, \qquad \delta = (1000N^4(s+k))^{-3RN}\theta. \tag{2.8}$$

In view of the definition of λ, there exists a sequence of natural numbers $(X_l)_{l=1}^{\infty}$, tending to infinity, with the property that $J_{s+r}(X_l) > X_l^{\lambda-\delta}$ ($l \in \mathbb{N}$). Also, provided that X_l is sufficiently large, one has the corresponding upper bound $J_{s+r}(Y) < Y^{\lambda+\delta}$ for $Y \geqslant X_l^{1/2}$. We consider a fixed element $X = X_l$ of the sequence $(X_l)_{l=1}^{\infty}$, which we may assume to be sufficiently large in terms of s, k and N. We put $M = X^{\theta}$, and note from (2.8) that $X^{\delta} < M^{1/N}$. Throughout, implicit constants may depend on s, k, N, and also on ε in view of our earlier convention, but not on any other variable.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We next introduce the cast of exponential sums and mean values appearing in our arguments. Let p be a prime number with $M < p \leqslant 2M$ to be fixed in due course. When c and ξ are non-negative integers, and $\boldsymbol{\alpha} \in [0,1)^k$, we define

$$\mathfrak{f}_c(\boldsymbol{\alpha};\xi) = \sum_{\substack{1 \leqslant x \leqslant X \\ x \equiv \xi \pmod{p^c}}} e(\alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_k x^k). \tag{2.9}$$

When $1 \leqslant m \leqslant k-1$, denote by $\Xi_c^m(\xi)$ the set of integral m-tuples $(\xi_1, \dots, \xi_m)$, with $1 \leqslant \boldsymbol{\xi} \leqslant p^{c+1}$ and $\boldsymbol{\xi} \equiv \xi \pmod{p^c}$, and satisfying the property that $\xi_i \not\equiv \xi_j \pmod{p^{c+1}}$ for $i \neq j$. We then put

$$\mathfrak{F}_c^m(\boldsymbol{\alpha};\xi) = \sum_{\boldsymbol{\xi} \in \Xi_c^m(\xi)} \prod_{i=1}^{m} \mathfrak{f}_{c+1}(\boldsymbol{\alpha};\xi_i). \tag{2.10}$$

When a and b are positive integers, we define

$$I_{a,b}^{m,r}(X;\xi,\eta) = \oint |\mathfrak{F}_a^m(\boldsymbol{\alpha};\xi)^2 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s+2r-2m}| \, d\boldsymbol{\alpha}, \tag{2.11}$$

$$K_{a,b}^{m,r}(X;\xi,\eta) = \oint |\mathfrak{F}_a^m(\boldsymbol{\alpha};\xi)^2 \mathfrak{F}_b^r(\boldsymbol{\alpha};\eta)^2 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2m}| \, d\boldsymbol{\alpha}. \tag{2.12}$$

This notation extends to the case $m = 0$, of course, by simply interpreting the exponential sum $\mathfrak{F}_c^0(\boldsymbol{\alpha};\xi)$ to be 1.

Note that, by orthogonality, the mean value $I_{a,b}^{m,r}(X;\xi,\eta)$ counts the number of integral solutions of the system

$$\sum_{i=1}^{m}(x_i^j - y_i^j) = \sum_{l=1}^{s+r-m}(v_l^j - w_l^j) \quad (1 \leqslant j \leqslant k), \tag{2.13}$$

with $1 \leqslant \mathbf{x}, \mathbf{y}, \mathbf{v}, \mathbf{w} \leqslant X$, $\mathbf{v} \equiv \mathbf{w} \equiv \eta \pmod{p^b}$ and $\mathbf{x}, \mathbf{y} \in \Xi_a^m(\xi) \pmod{p^{a+1}}$. Similarly, the mean value $K_{a,b}^{m,r}(X;\xi,\eta)$ counts the number of solutions of

$$\sum_{i=1}^{m}(x_i^j - y_i^j) = \sum_{l=1}^{r}(u_l^j - v_l^j) + \sum_{n=1}^{s-m}(w_n^j - z_n^j) \quad (1 \leqslant j \leqslant k), \tag{2.14}$$

with $1 \leqslant \mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{z} \leqslant X$, and satisfying $\mathbf{w} \equiv \mathbf{z} \equiv \eta \pmod{p^b}$,

$$\mathbf{x}, \mathbf{y} \in \Xi_a^m(\xi) \pmod{p^{a+1}} \quad \text{and} \quad \mathbf{u}, \mathbf{v} \in \Xi_b^r(\eta) \pmod{p^{b+1}}.$$

Given any one such solution of the system (2.14), an application of the binomial theorem shows that $\mathbf{x} - \eta, \mathbf{y} - \eta, \mathbf{u} - \eta, \mathbf{v} - \eta, \mathbf{w} - \eta, \mathbf{z} - \eta$ is also a solution. Since in any solution counted by $K_{a,b}^{m,r}(X;\xi,\eta)$, one has $\mathbf{u} \equiv \mathbf{v} \equiv \eta \pmod{p^b}$ and $\mathbf{w} \equiv \mathbf{z} \equiv \eta \pmod{p^b}$, we deduce that

$$\sum_{i=1}^{m}(x_i - \eta)^j \equiv \sum_{i=1}^{m}(y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leqslant j \leqslant k). \tag{2.15}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We put

$$I_{a,b}^{m,r}(X) = \max_{1\leqslant \xi\leqslant p^a} \max_{\substack{1\leqslant \eta\leqslant p^b \\ \eta\not\equiv \xi \pmod p}} I_{a,b}^{m,r}(X;\xi,\eta), \tag{2.16}$$

$$K_{a,b}^{m,r}(X) = \max_{1\leqslant \xi\leqslant p^a} \max_{\substack{1\leqslant \eta\leqslant p^b \\ \eta\not\equiv \xi \pmod p}} K_{a,b}^{m,r}(X;\xi,\eta). \tag{2.17}$$

The implicit dependence on p in the above notation will be rendered irrelevant in §5, since we fix the choice of this prime following the proof of Lemma 5.1.

We must align the definition of $K_{0,b}^{m,r}(X)$ with the conditioning idea. When $\boldsymbol{\zeta}$ is a tuple of integers, we denote by $\Xi^m(\boldsymbol{\zeta})$ the set of m-tuples $(\xi_1,\dots,\xi_m) \in \Xi_0^m(0)$ such that $\xi_i \not\equiv \zeta_j \pmod p$ for all i and j. Recalling (2.9), we put

$$\mathfrak{F}^m(\boldsymbol{\alpha};\boldsymbol{\zeta}) = \sum_{\boldsymbol{\xi}\in\Xi^m(\boldsymbol{\zeta})} \prod_{i=1}^{m} \mathfrak{f}_1(\boldsymbol{\alpha};\xi_i)$$

and then define

$$\widetilde{I}_c^{m,r}(X;\eta) = \oint |\mathfrak{F}^m(\boldsymbol{\alpha};\eta)^2 \mathfrak{f}_c(\boldsymbol{\alpha};\eta)^{2s+2r-2m}|\,d\boldsymbol{\alpha}, \tag{2.18}$$

$$\widetilde{K}_c^{m,r}(X;\eta) = \oint |\mathfrak{F}^m(\boldsymbol{\alpha};\eta)^2 \mathfrak{F}_c^r(\boldsymbol{\alpha};\eta)^2 \mathfrak{f}_c(\boldsymbol{\alpha};\eta)^{2s-2m}|\,d\boldsymbol{\alpha}, \tag{2.19}$$

$$K_{0,c}^{m,r}(X) = \max_{1\leqslant\eta\leqslant p^c} \widetilde{K}_c^{m,r}(X;\eta). \tag{2.20}$$

As in our earlier work, we make use of an operator that makes transparent the relationship between mean values and their anticipated magnitudes. For the purposes at hand, it is useful to reconfigure this normalization so as to make visible the deviation in a mean value from strongly diagonal behaviour. Thus, in the present circumstances, we adopt the convention that

$$[[J_{s+r}(X)]] = J_{s+r}(X)/X^{s+r}, \tag{2.21}$$

$$[[I_{a,b}^{m,r}(X)]] = \frac{I_{a,b}^{m,r}(X)}{(X/M^a)^m (X/M^b)^{s+r-m}}, \tag{2.22}$$

$$[[K_{a,b}^{m,r}(X)]] = \frac{K_{a,b}^{m,r}(X)}{(X/M^a)^m (X/M^b)^{s+r-m}}. \tag{2.23}$$

Using this notation, our earlier bounds for $J_{s+r}(X)$ may be rewritten in the form

$$[[J_{s+r}(X)]] > X^{\Lambda-\delta} \quad \text{and} \quad [[J_{s+r}(Y)]] < Y^{\Lambda+\delta} \quad (Y \geqslant X^{1/2}), \tag{2.24}$$

where Λ is defined by $\Lambda = \lambda - (s+r)$.

Finally, we recall two simple estimates associated with the system (1.1).

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

LEMMA 2.2. *Suppose that c is a non-negative integer with $c\theta \leqslant 1$. Then, for each natural number u, one has*

$$\max_{1\leqslant \xi \leqslant p^c} \oint |\mathfrak{f}_c(\boldsymbol{\alpha}; \xi)|^{2u}\, d\boldsymbol{\alpha} \ll_u J_u(X/M^c).$$

Proof. This is [15, Lemma 3.1]. □

LEMMA 2.3. *Suppose that c and d are non-negative integers with $c \leqslant \theta^{-1}$ and $d \leqslant \theta^{-1}$. Then, whenever $u, v \in \mathbb{N}$ and $\xi, \zeta \in \mathbb{Z}$, one has*

$$\oint |\mathfrak{f}_c(\boldsymbol{\alpha}; \xi)^{2u} \mathfrak{f}_d(\boldsymbol{\alpha}; \zeta)^{2v}|\, d\boldsymbol{\alpha} \ll_{u,v} (J_{u+v}(X/M^c))^{u/(u+v)} (J_{u+v}(X/M^d))^{v/(u+v)}.$$

Proof. This is [4, Corollary 2.2]. □

§3. *Auxiliary systems of congruences.* Our goal of establishing strongly diagonal behaviour dictates that we must establish essentially diagonal behaviour for the solutions of auxiliary congruences central to our methods. Complicating our discussion in present circumstances is the potential for the ratio b/a to be small, for in earlier work [4, 17] this was assumed to be at least $\frac{1}{2}(k-1)$ or thereabouts. We begin by adjusting our notation to accommodate the demands of this paper. When a and b are integers with $1 \leqslant a < b$, we write $\mathcal{B}^n_{a,b}(\mathbf{m}; \xi, \eta)$ for the set of solutions of the system of congruences

$$\sum_{i=1}^{n} (z_i - \eta)^j \equiv m_j \pmod{p^{jb}} \quad (1 \leqslant j \leqslant k), \tag{3.1}$$

with $1 \leqslant \mathbf{z} \leqslant p^{kb}$ and $\mathbf{z} \equiv \boldsymbol{\xi} \pmod{p^{a+1}}$ for some $\boldsymbol{\xi} \in \Xi^n_a(\xi)$. We define an equivalence relation $\mathcal{R}(\lambda)$ on integral n-tuples by declaring $\mathbf{x}$ and $\mathbf{y}$ to be $\mathcal{R}(\lambda)$-equivalent when $\mathbf{x} \equiv \mathbf{y} \pmod{p^\lambda}$. When $hb \in \mathbb{N}$, we then write $\mathcal{C}^{n,h}_{a,b}(\mathbf{m}; \xi, \eta)$ for the set of $\mathcal{R}(hb)$-equivalence classes of $\mathcal{B}^n_{a,b}(\mathbf{m}; \xi, \eta)$, and we define $B^{n,h}_{a,b}(p)$ by putting

$$B^{n,h}_{a,b}(p) = \max_{1\leqslant \xi \leqslant p^a} \max_{\substack{1\leqslant \eta \leqslant p^b \\ \eta \not\equiv \xi \pmod p}} \max_{1\leqslant \mathbf{m} \leqslant p^{kb}} \operatorname{card}(\mathcal{C}^{n,h}_{a,b}(\mathbf{m}; \xi, \eta)). \tag{3.2}$$

When $a = 0$ we modify these definitions, so that $\mathcal{B}^n_{0,b}(\mathbf{m}; \xi, \eta)$ denotes the set of solutions of the system of congruences (3.1) with $1 \leqslant \mathbf{z} \leqslant p^{kb}$ and $\mathbf{z} \equiv \boldsymbol{\xi} \pmod p$ for some $\boldsymbol{\xi} \in \Xi^n_0(\xi)$, and for which in addition $\mathbf{z} \not\equiv \eta \pmod p$. As in the situation in which one has $a \geqslant 1$, when $hb \in \mathbb{N}$, we write $\mathcal{C}^{n,h}_{0,b}(\mathbf{m}; \xi, \eta)$ for the set of $\mathcal{R}(hb)$-equivalence classes of $\mathcal{B}^n_{0,b}(\mathbf{m}; \xi, \eta)$, but we define $B^{n,h}_{0,b}(p)$ by putting

$$B^{n,h}_{0,b}(p) = \max_{1\leqslant \eta \leqslant p^b} \max_{1\leqslant \mathbf{m} \leqslant p^{kb}} \operatorname{card}(\mathcal{C}^{n,h}_{0,b}(\mathbf{m}; 0, \eta)). \tag{3.3}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We observe that the definition of $B_{a,b}^{n,h}(p)$ ensures that whenever $0 < h' \leqslant h$ and both hb and $h'b$ are natural numbers, one has

$$B_{a,b}^{n,h'}(p) \leqslant B_{a,b}^{n,h}(p). \tag{3.4}$$

Readers might wonder concerning the wisdom of permitting in $B_{a,b}^{n,h}(p)$ the parameter h to be a rational number with $hb \in \mathbb{N}$. We remark that this somewhat strange notational device is designed to facilitate ease of comparison with the earlier work [**4**, **17**, **19**]. Since the role of the parameter h is simply that of indicating certain congruence relations modulo p^{hb}, the reader may take comfort from our imposition of the condition $hb \in \mathbb{N}$.

LEMMA 3.1. *Let m be an integer with $0 \leqslant m \leqslant k-1$, and suppose that a and b are integers with $0 \leqslant a < b$ and $(k-m)b \geqslant (m+1)a$. Suppose in addition that h is a natural number with $a \leqslant h \leqslant (k-m)b - ma$. Then one has*

$$B_{a,b}^{m+1,h/b}(p) \leqslant k!.$$

Proof. We are able to follow the arguments of the proofs of [**17**, Lemma 3.5] and [**4**, Lemma 3.3], with some modifications. For the sake of transparency of exposition, we provide an essentially complete account. We begin by considering the situation with $a \geqslant 1$, the alterations required when $a = 0$ being easily accommodated within our basic argument. Consider fixed natural numbers a and b with $1 \leqslant a < b$ and $(k-m)b \geqslant (m+1)a$, and fixed integers ξ and η with $1 \leqslant \xi \leqslant p^a$, $1 \leqslant \eta \leqslant p^b$ and $\eta \not\equiv \xi \pmod p$. Note that in view of the relation (3.4), the conclusion of the lemma follows in general if we can establish it when $h = (k-m)b - ma$. We henceforth assume that the latter is the case. We then denote by $\mathcal{D}_1(\mathbf{n})$ the set of $\mathcal{R}(h)$-equivalence classes of solutions of the system of congruences

$$\sum_{i=1}^{m+1} (z_i - \eta)^j \equiv n_j \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k), \tag{3.5}$$

with $1 \leqslant \mathbf{z} \leqslant p^{kb}$ and $\mathbf{z} \equiv \boldsymbol{\xi} \pmod{p^{a+1}}$ for some $\boldsymbol{\xi} \in \Xi_a^{m+1}(\xi)$. To any solution $\mathbf{z}$ of (3.1) there corresponds a unique $(m+1)$-tuple $(n_{k-m}, \dots, n_k)$, satisfying $1 \leqslant \mathbf{n} \leqslant p^{(k-m)b}$, for which (3.5) holds and

$$n_j \equiv m_j \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k).$$

Since $h/b \leqslant k-m$, we therefore infer that

$$\operatorname{card}(\mathcal{C}_{a,b}^{m+1,h/b}(\mathbf{m}; \xi, \eta)) \leqslant \max_{1 \leqslant \mathbf{n} \leqslant p^{(k-m)b}} \operatorname{card}(\mathcal{D}_1(\mathbf{n})). \tag{3.6}$$

We fix any choice of $\mathbf{n}$ for which the maximum is achieved in (3.6). There is plainly no loss of generality in supposing that $\mathcal{D}_1(\mathbf{n})$ is non-empty. Observe that

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

for any solution $\mathbf{z}'$ of (3.5) there is an $\mathcal{R}(k-m)$-equivalent solution $\mathbf{z}$ satisfying $1 \leqslant \mathbf{z} \leqslant p^{(k-m)b}$. Rewriting each variable z_i in (3.5) in the shape $z_i = p^a y_i + \xi$, we infer from the hypothesis that $\mathbf{z} \equiv \boldsymbol{\xi} \pmod{p^{a+1}}$ for some $\boldsymbol{\xi} \in \Xi_a^{m+1}(\xi)$ that the $(m+1)$-tuple $\mathbf{y}$ necessarily satisfies

$$y_i \not\equiv y_l \pmod{p} \quad (1 \leqslant i < l \leqslant m+1). \tag{3.7}$$

Write $\zeta = \xi - \eta$, and note that the constraint $\eta \not\equiv \xi \pmod{p}$ ensures that $p \nmid \zeta$. We denote the multiplicative inverse of ζ modulo $p^{(k-m)b}$ by ζ^{-1}. Then we deduce from (3.5) that $\operatorname{card}(\mathcal{D}_1(\mathbf{n}))$ is bounded above by the number of $\mathcal{R}(h-a)$-equivalence classes of solutions of the system of congruences

$$\sum_{i=1}^{m+1} (p^a y_i \zeta^{-1} + 1)^j \equiv n_j (\zeta^{-1})^j \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k), \tag{3.8}$$

with $1 \leqslant \mathbf{y} \leqslant p^{(k-m)b-a}$ satisfying (3.7). Let $\mathbf{y} = \mathbf{w}$ be any solution of the system (3.8). Then we find that all other solutions $\mathbf{y}$ satisfy the system

$$\sum_{i=1}^{m+1} ((p^a y_i \zeta^{-1} + 1)^j - (p^a w_i \zeta^{-1} + 1)^j) \equiv 0 \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k). \tag{3.9}$$

We next apply [**17**, Lemma 3.2], just as in the arguments of the proofs of [**17**, Lemmas 3.3 to 3.6]. Consider an index j with $k-m \leqslant j \leqslant k$, and apply the latter lemma with $\alpha = k-m-1$ and $\beta = j-k+m+1$. We find that there exist integers $c_{j,l}$ $(k-m-1 \leqslant l \leqslant j)$ and $d_{j,u}$ $(j-k+m+1 \leqslant u \leqslant j)$, bounded in terms of k, and with $d_{j,j-k+m+1} \neq 0$, for which one has the polynomial identity

$$c_{j,k-m-1} + \sum_{l=k-m}^{j} c_{j,l}(x+1)^l = \sum_{u=j-k+m+1}^{j} d_{j,u} x^u. \tag{3.10}$$

Since we may assume p to be large, we may suppose that $p \nmid d_{j,j-k+m+1}$. Thus, multiplying (3.10) through by the multiplicative inverse of $d_{j,j-k+m+1}$ modulo $p^{(k-m)b}$, we see that there is no loss in supposing that

$$d_{j,j-k+m+1} \equiv 1 \pmod{p^{(k-m)b}}.$$

Consequently, by taking suitable linear combinations of the congruences comprising (3.9), we discern that any solution of this system satisfies

$$(\zeta^{-1} p^a)^{j-k+m+1} \sum_{i=1}^{m+1} (\psi_j(y_i) - \psi_j(w_i)) \equiv 0 \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k),$$

in which

$$\psi_j(z) = z^{j-k+m+1} + \sum_{u=j-k+m+2}^{j} d_{j,u} (\zeta^{-1} p^a)^{u-j+k-m-1} z^u.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Note here that

$$\psi_j(z) \equiv z^{j-k+m+1} \pmod{p}. \tag{3.11}$$

Denote by $\mathcal{D}_2(\mathbf{u})$ the set of $\mathcal{R}(h-a)$-equivalence classes of solutions of the system of congruences

$$\sum_{i=1}^{m+1} \psi_j(y_i) \equiv u_j \pmod{p^{(k-m)b-(j-k+m+1)a}} \quad (k-m \leqslant j \leqslant k),$$

with $1 \leqslant \mathbf{y} \leqslant p^{(k-m)b-a}$ satisfying (3.7). Then we have shown thus far that

$$\operatorname{card}(\mathcal{D}_1(\mathbf{n})) \leqslant \max_{1 \leqslant \mathbf{u} \leqslant p^{(k-m)b}} \operatorname{card}(\mathcal{D}_2(\mathbf{u})). \tag{3.12}$$

Let $\mathcal{D}_3(\mathbf{v})$ denote the set of solutions of the congruence

$$\sum_{i=1}^{m+1} \psi_j(y_i) \equiv v_j \pmod{p^{h-a}} \quad (k-m \leqslant j \leqslant k),$$

with $1 \leqslant \mathbf{y} \leqslant p^{h-a}$ satisfying (3.7). For $k-m \leqslant j \leqslant k$, we have

$$(k-m)b - (j-k+m+1)a \geqslant (k-m)b - (m+1)a = h-a.$$

Then we arrive at the upper bound

$$\operatorname{card}(\mathcal{D}_2(\mathbf{u})) \leqslant \max_{1 \leqslant \mathbf{v} \leqslant p^{h-a}} \operatorname{card}(\mathcal{D}_3(\mathbf{v})). \tag{3.13}$$

By combining (3.6), (3.12) and (3.13), we discern at this point that

$$\operatorname{card}(\mathcal{C}_{a,b}^{m+1,h/b}(\mathbf{m}; \xi, \eta)) \leqslant \max_{1 \leqslant \mathbf{v} \leqslant p^{h-a}} \operatorname{card}(\mathcal{D}_3(\mathbf{v})). \tag{3.14}$$

Define the determinant

$$J(\boldsymbol{\psi}; \mathbf{x}) = \det(\psi'_{k-m+l-1}(x_i))_{1 \leqslant i,l \leqslant m+1}.$$

In view of (3.11), one has $\psi'_{k-m+l-1}(y_i) \equiv l y_i^{l-1} \pmod{p}$. It follows from (3.7) that

$$\det(y_i^{l-1})_{1 \leqslant i,l \leqslant m+1} = \prod_{1 \leqslant i < u \leqslant m+1} (y_i - y_u) \not\equiv 0 \pmod{p},$$

so that, since $p > k$, we have $(J(\boldsymbol{\psi}; \mathbf{y}), p) = 1$. We therefore deduce from [**13**, Theorem 1], just as in the corresponding argument of the proof of [**17**, Lemma 3.3] following [**17**, equation (3.17)], that

$$\operatorname{card}(\mathcal{D}_3(\mathbf{v})) \leqslant (k-m)(k-m+1)\cdots k \leqslant k!$$

and thus the conclusion of the lemma when $a \geqslant 1$ follows at once from (3.2) and (3.14).

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

When $a = 0$, we must apply some minor modifications to the above argument. In this case, we denote by $\mathcal{D}_1(\mathbf{n}; \eta)$ the set of $\mathcal{R}(h)$-equivalence classes of solutions of the system of congruences (3.5) with $1 \leqslant \mathbf{z} \leqslant p^{kb}$ and $\mathbf{z} \equiv \boldsymbol{\xi} \pmod{p}$ for some $\boldsymbol{\xi} \in \Xi_0^{m+1}(0)$, and for which in addition $z_i \not\equiv \eta \pmod{p}$ for $1 \leqslant i \leqslant m+1$. Then, as in the opening paragraph of our proof, it follows from (3.1) that

$$\operatorname{card}(\mathcal{C}_{0,b}^{m+1,h/b}(\mathbf{m}; 0, \eta)) \leqslant \max_{1 \leqslant \mathbf{n} \leqslant p^{(k-m)b}} \operatorname{card}(\mathcal{D}_1(\mathbf{n}; \eta)). \tag{3.15}$$

But $\operatorname{card}(\mathcal{D}_1(\mathbf{n}; \eta)) = \operatorname{card}(\mathcal{D}_1(\mathbf{n}; 0))$, and $\operatorname{card}(\mathcal{D}_1(\mathbf{n}; 0))$ counts the solutions of the system of congruences

$$\sum_{i=1}^{m+1} y_i^j \equiv n_j \pmod{p^{(k-m)b}} \quad (k-m \leqslant j \leqslant k),$$

with $1 \leqslant \mathbf{y} \leqslant p^{(k-m)b}$ satisfying (3.7), and in addition $p \nmid y_i$ $(1 \leqslant i \leqslant m+1)$. Write

$$J(\mathbf{y}) = \det((k-m+j-1)y_i^{k-m+j-2})_{1 \leqslant i,j \leqslant m+1}.$$

Then, since $p > k$, we have

$$J(\mathbf{y}) = \frac{k!}{(k-m-1)!}(y_1 \cdots y_{m+1})^{k-m-1} \prod_{1 \leqslant i < j \leqslant m+1} (y_i - y_j) \not\equiv 0 \pmod{p}.$$

We therefore conclude from [**13**, Theorem 1] that

$$\operatorname{card}(\mathcal{D}_1(\mathbf{n}; 0)) \leqslant (k-m)(k-m+1) \cdots k \leqslant k!.$$

In view of (3.3), the conclusion of the lemma therefore follows from (3.15) when $a = 0$. This completes our account of the proof of the lemma. □

§4. *The conditioning process.* The mean value $K_{a,b}^{m,r}(X; \xi, \eta)$ differs only slightly from the special case $K_{a,b}^{k-1,k-1}(X; \xi, \eta)$ considered in [**19**], and thus our treatment of the conditioning process may be swiftly executed.

LEMMA 4.1. *Let a and b be integers with $b > a \geqslant 1$. Then, whenever $s \geqslant 2r-1$, one has*

$$I_{a,b}^{r,r}(X) \ll K_{a,b}^{r,r}(X) + M^{2s/3} I_{a,b+1}^{r,r}(X).$$

Proof. Our argument follows the proof of [**19**, Lemma 4.1] with minor adjustments. Consider fixed integers ξ and η with $\eta \not\equiv \xi \pmod{p}$. Let T_1 denote the number of integral solutions $\mathbf{x}$, $\mathbf{y}$, $\mathbf{v}$, $\mathbf{w}$ of the system (2.13) counted by $I_{a,b}^{r,r}(X; \xi, \eta)$ in which $v_1, \dots, v_s$ together occupy at least r distinct residue classes modulo p^{b+1}, and let T_2 denote the corresponding number of solutions in which these integers together occupy at most $r-1$ distinct residue classes modulo p^{b+1}. Then

$$I_{a,b}^{r,r}(X; \xi, \eta) = T_1 + T_2. \tag{4.1}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

From (2.10) to (2.12), orthogonality and Schwarz's inequality, one has

$$\begin{aligned} T_1 &\leqslant \binom{s}{r} \oint |\mathfrak{F}_a^r(\boldsymbol{\alpha};\xi)|^2 \mathfrak{F}_b^r(\boldsymbol{\alpha};\eta) \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{s-r} \mathfrak{f}_b(-\boldsymbol{\alpha};\eta)^s \, d\boldsymbol{\alpha} \\ &\ll (K_{a,b}^{r,r}(X;\xi,\eta))^{1/2} (I_{a,b}^{r,r}(X;\xi,\eta))^{1/2}. \end{aligned} \tag{4.2}$$

In order to treat T_2, we observe first that the hypothesis $s \geqslant 2r-1$ ensures that there is an integer $\zeta \equiv \eta \pmod{p^b}$ having the property that three at least of the variables $v_1, \dots, v_s$ are congruent to ζ modulo p^{b+1}. Hence, recalling the definitions (2.10) and (2.11), one finds from orthogonality and Hölder's inequality that

$$\begin{aligned} T_2 &\leqslant \binom{s}{3} \sum_{\substack{1 \leqslant \zeta \leqslant p^{b+1} \\ \zeta \equiv \eta \pmod{p^b}}} \oint |\mathfrak{F}_a^r(\boldsymbol{\alpha};\xi)|^2 \mathfrak{f}_{b+1}(\boldsymbol{\alpha};\zeta)^3 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{s-3} \mathfrak{f}_b(-\boldsymbol{\alpha};\eta)^s \, d\boldsymbol{\alpha} \\ &\ll M \max_{\substack{1 \leqslant \zeta \leqslant p^{b+1} \\ \zeta \equiv \eta \pmod{p^b}}} (I_{a,b}^{r,r}(X;\xi,\eta))^{1-3/(2s)} (I_{a,b+1}^{r,r}(X;\xi,\zeta))^{3/(2s)}. \end{aligned} \tag{4.3}$$

By substituting (4.2) and (4.3) into (4.1), and recalling (2.16) and (2.17), we therefore conclude that

$$I_{a,b}^{r,r}(X) \ll (K_{a,b}^{r,r}(X))^{1/2} (I_{a,b}^{r,r}(X))^{1/2} + M (I_{a,b}^{r,r}(X))^{1-3/(2s)} (I_{a,b+1}^{r,r}(X))^{3/(2s)},$$

whence

$$I_{a,b}^{r,r}(X) \ll K_{a,b}^{r,r}(X) + M^{2s/3} I_{a,b+1}^{r,r}(X).$$

This completes the proof of the lemma. □

Repeated application of Lemma 4.1 combines with a trivial bound for the mean value $K_{a,b+H}^{r,r}(X)$ to deliver the basic conditioning lemma of this section.

LEMMA 4.2. *Let a and b be integers with $1 \leqslant a < b$, and let H be any integer with $H \geqslant 15$. Suppose that $b + H \leqslant (2\theta)^{-1}$. Then there exists an integer h with $0 \leqslant h < H$ having the property that*

$$I_{a,b}^{r,r}(X) \ll (M^h)^{2s/3} K_{a,b+h}^{r,r}(X) + (M^H)^{-s/4} (X/M^b)^s (X/M^a)^{\lambda - s}.$$

Proof. Repeated application of Lemma 4.1 yields the upper bound

$$I_{a,b}^{r,r}(X) \ll \sum_{h=0}^{H-1} (M^h)^{2s/3} K_{a,b+h}^{r,r}(X) + (M^H)^{2s/3} I_{a,b+H}^{r,r}(X). \tag{4.4}$$

On considering the underlying Diophantine systems, it follows from Lemma 2.3 that for each ξ and η, one has

$$\begin{aligned} I_{a,b+H}^{r,r}(X;\xi,\eta) &\leqslant \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2r} \mathfrak{f}_{b+H}(\boldsymbol{\alpha};\eta)^{2s}| \, d\boldsymbol{\alpha} \\ &\ll (J_{s+r}(X/M^a))^{r/(s+r)} (J_{s+r}(X/M^{b+H}))^{s/(s+r)}. \end{aligned}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Since $M^{b+H} = (X^\theta)^{b+H} \leqslant X^{1/2}$, we deduce from (2.16) and (2.24) that

$$\begin{aligned}(M^H)^{2s/3} I^{r,r}_{a,b+H}(X) &\ll X^\delta((X/M^a)^{r/(s+r)}(X/M^{b+H})^{s/(s+r)})^\lambda (M^H)^{2s/3}\\ &= X^\delta (X/M^b)^s (X/M^a)^{\lambda - s} M^\Omega,\end{aligned}$$

where

$$\Omega = \lambda\left(a - \frac{ar}{s+r} - \frac{bs}{s+r}\right) + s(b-a) + Hs\left(\frac{2}{3} - \frac{\lambda}{s+r}\right).$$

Since $\lambda \geqslant s + r$, the lower bound $b > a$ leads to the estimate

$$\Omega \leqslant -s(b-a)\frac{\lambda}{s+r} + s(b-a) - \frac{1}{3}Hs \leqslant -\frac{1}{3}Hs.$$

This completes the proof of the lemma, since with $H \geqslant 15$ one has

$$X^\delta M^{-Hs/3} \ll M^{-Hs/4}. \qquad \square$$

§5. *The precongruencing step.* The alteration of the definition of $K^{m,r}_{a,b}(X)$ relative to our earlier treatments does not prevent previous precongruencing arguments from applying, *mutatis mutandis*. However, we seek to ensure that our initial value of b is very large, so that subsequent iterations work efficiently. For this reason, the argument of the proof of [**4**, Lemma 6.1] must be modified in several ways that demand a fairly complete account of the proof. We recall the definition (2.8) of B.

LEMMA 5.1. *There exist a prime number p, with $M < p \leqslant 2M$, and an integer h, with $0 \leqslant h \leqslant 4B$, for which one has*

$$J_{s+r}(X) \ll M^{2sB+2sh/3} K^{r,r}_{0,B+h}(X).$$

Proof. The mean value $J_{s+r}(X)$ counts the number of integral solutions of the system

$$\sum_{i=1}^{s+r}(x_i^j - y_i^j) = 0 \quad (1 \leqslant j \leqslant k), \tag{5.1}$$

with $1 \leqslant \mathbf{x}, \mathbf{y} \leqslant X$. Let $\mathcal{P}$ denote a set of $\lceil (s+r)^2\theta^{-1}\rceil$ prime numbers lying in $(M, 2M]$. That such a set exists is a consequence of the prime number theorem. The argument of the proof of [**4**, Lemma 6.1] leading to equation (6.2) of that paper shows that for some $p \in \mathcal{P}$, one has $J_{s+r}(X) \ll T(p)$, where $T(p)$ denotes the number of solutions of the system (5.1) counted by $J_{s+r}(X)$ in which $x_1, \dots, x_{s+r}$ are distinct modulo p, and likewise $y_1, \dots, y_{s+r}$ are distinct modulo p.

We now examine the residue classes modulo p^B of a given solution $\mathbf{x}, \mathbf{y}$ counted by $T(p)$. Let $\boldsymbol{\eta}$ and $\boldsymbol{\zeta}$ be s-tuples with $1 \leqslant \boldsymbol{\eta}, \boldsymbol{\zeta} \leqslant p^B$ satisfying the condition that for $1 \leqslant i \leqslant s$, one has $x_i \equiv \eta_i \pmod{p^B}$ and $y_i \equiv \zeta_i \pmod{p^B}$. Recall the notation introduced prior to (2.18). Then, since $x_1, \dots, x_{s+r}$ are

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

distinct modulo p, it follows that $(x_{s+1}, \dots, x_{s+r}) \in \Xi^r(\boldsymbol{\eta})$, and likewise one finds that $(y_{s+1}, \dots, y_{s+r}) \in \Xi^r(\boldsymbol{\zeta})$. Then, on considering the underlying Diophantine systems, one finds that

$$T(p) \leqslant \sum_{1 \leqslant \boldsymbol{\eta}, \boldsymbol{\zeta} \leqslant p^B} \oint \Big(\prod_{i=1}^{s} \mathfrak{f}_B(\boldsymbol{\alpha}; \eta_i) \mathfrak{f}_B(-\boldsymbol{\alpha}; \zeta_i) \Big) \mathfrak{F}^r(\boldsymbol{\alpha}; \boldsymbol{\eta}) \mathfrak{F}^r(-\boldsymbol{\alpha}; \boldsymbol{\zeta})\, d\boldsymbol{\alpha}.$$

Write

$$\mathcal{J}(\boldsymbol{\theta}, \psi) = \oint |\mathfrak{F}^r(\boldsymbol{\alpha}; \boldsymbol{\theta})^2 \mathfrak{f}_B(\boldsymbol{\alpha}; \psi)^{2s}|\, d\boldsymbol{\alpha}.$$

Then, by applying Hölder's inequality, and again considering the underlying Diophantine systems, we discern that

$$\begin{aligned} T(p) &\leqslant \sum_{1 \leqslant \boldsymbol{\eta}, \boldsymbol{\zeta} \leqslant p^B} \prod_{i=1}^{s} (\mathcal{J}(\boldsymbol{\eta}, \eta_i) \mathcal{J}(\boldsymbol{\zeta}, \zeta_i))^{1/(2s)} \\ &\leqslant \sum_{1 \leqslant \boldsymbol{\eta}, \boldsymbol{\zeta} \leqslant p^B} \prod_{i=1}^{s} (\mathcal{J}(\eta_i, \eta_i) \mathcal{J}(\zeta_i, \zeta_i))^{1/(2s)}. \end{aligned}$$

Hence, on recalling the definition (2.18), we obtain the upper bound

$$\begin{aligned} T(p) &\leqslant p^{2sB} \max_{1 \leqslant \eta \leqslant p^B} \oint |\mathfrak{F}^r(\boldsymbol{\alpha}; \eta)^2 \mathfrak{f}_B(\boldsymbol{\alpha}; \eta)^{2s}|\, d\boldsymbol{\alpha} \\ &= p^{2sB} \max_{1 \leqslant \eta \leqslant p^B} \widetilde{I}_B^{r,r}(X; \eta). \end{aligned} \tag{5.2}$$

By modifying the argument of the proof of [**4**, Lemma 6.1] leading from equation (6.3) to equation (6.6) of that paper, along the lines easily surmised from our proof of Lemma 4.1 above, one finds that

$$\widetilde{I}_c^{r,r}(X; \eta) \ll \widetilde{K}_c^{r,r}(X; \eta) + M^{2s/3} \max_{1 \leqslant \zeta \leqslant p^{c+1}} \widetilde{I}_{c+1}^{r,r}(X; \zeta). \tag{5.3}$$

Iterating (5.3) in order to bound $\widetilde{I}_B^{r,r}(X; \eta)$, just as in the argument concluding the proof of [**4**, Lemma 6.1] (and see also (4.4) above), we discern from (5.2) that

$$\begin{aligned} J_{s+r}(X) \ll M^{2sB} &\max_{0 \leqslant h \leqslant 4B} (M^h)^{2s/3} K_{0,B+h}^{r,r}(X) \\ &+ M^{2sB+8sB/3} \max_{1 \leqslant \zeta \leqslant p^{5B+1}} \widetilde{I}_{5B+1}^{r,r}(X; \zeta). \end{aligned} \tag{5.4}$$

By considering the underlying Diophantine systems, we deduce from Lemma 2.3 that

$$\widetilde{I}_{5B+1}^{r,r}(X; \zeta) \ll (J_{s+r}(X))^{r/(s+r)} (J_{s+r}(X/M^{5B+1}))^{s/(s+r)}.$$

In this way, we find from (5.4) either that

$$J_{s+r}(X) \ll M^{2sB+2sh/3} K_{0,B+h}^{r,r}(X) \tag{5.5}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

for some index h with $0 \leqslant h \leqslant 4B$, so that the conclusion of the lemma holds, or else that

$$J_{s+r}(X) \ll M^{14sB/3}(J_{s+r}(X))^{r/(s+r)}(J_{s+r}(X/M^{5B+1}))^{s/(s+r)}.$$

In the latter case, since $\lambda \geqslant s+r$, we obtain the upper bound

$$\begin{aligned} J_{s+r}(X) &\ll M^{14(s+r)B/3} J_{s+r}(X/M^{5B+1}) \\ &\ll M^{14(s+r)B/3}(X/M^{5B+1})^{\lambda+\delta} \\ &\ll X^{\lambda+\delta} M^{-(s+r)B/3}. \end{aligned}$$

Invoking the definition (2.8) of δ, we find that $J_{s+r}(X) \ll X^{\lambda-2\delta}$, contradicting the lower bound (2.24) if $X = X_l$ is large enough. We are therefore forced to accept the former upper bound (5.5), and hence the proof of the lemma is completed by reference to (2.20). □

At this point, we fix the prime number p, once and for all, in accordance with Lemma 5.1.

§6. *The efficient congruencing step.* Our strategy for executing the efficient congruencing process is based on that in our recent work [**19**, §6], though in present circumstances only one phase is required, relating $K_{a,b}^{m+1,r}(X)$ to $K_{a,b}^{m,r}(X)$ and $I_{b,b'}^{r,r}(X)$, for a suitable value of b'. We begin our discussion of the efficient congruencing process with some additional notation. We define the generating function

$$\mathfrak{H}_{c,d}^{m}(\boldsymbol{\alpha}; \xi) = \sum_{\boldsymbol{\xi} \in \Xi_c^m(\xi)} \sum_{\substack{1 \leqslant \boldsymbol{\zeta} \leqslant p^d \\ \boldsymbol{\zeta} \equiv \boldsymbol{\xi} \pmod{p^{c+1}}}} \prod_{i=1}^{m} |\mathfrak{f}_d(\boldsymbol{\alpha}; \zeta_i)|^2, \tag{6.1}$$

in which we adopt the natural convention that $\mathfrak{H}_{c,d}^{0}(\boldsymbol{\alpha}; \xi) = 1$. It is useful for future reference to record the consequence of Hölder's inequality given in [**19**, equation (6.2)], namely that whenever ω is a real number with $m\omega \geqslant 1$, then

$$\mathfrak{H}_{c,d}^{m}(\boldsymbol{\alpha}; \xi)^{\omega} \leqslant (p^{d-c})^{m\omega-1} \sum_{\substack{1 \leqslant \zeta \leqslant p^d \\ \zeta \equiv \xi \pmod{p^c}}} |\mathfrak{f}_d(\boldsymbol{\alpha}; \zeta)|^{2m\omega}. \tag{6.2}$$

LEMMA 6.1. *Let m be an integer with $0 \leqslant m \leqslant r-1$. Suppose that a and b are integers with $0 \leqslant a < b \leqslant \theta^{-1}$ and $(k-m)b \geqslant (m+1)a$, and suppose further that $a \leqslant b/\sqrt{k}$. Then, whenever b' is an integer with $a \leqslant b' \leqslant (k-m)b - ma$, one has*

$$K_{a,b}^{m+1,r}(X) \ll ((M^{b'-a})^s I_{b,b'}^{r,r}(X))^{1/(s-m)}(K_{a,b}^{m,r}(X))^{(s-m-1)/(s-m)}.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Proof. We first consider the situation in which $a \geqslant 1$. The argument associated with the case $a = 0$ is very similar, and so we are able to appeal later to a highly abbreviated argument for this case in order to complete the proof of the lemma. Consider fixed integers ξ and η with

$$1 \leqslant \xi \leqslant p^a, \quad 1 \leqslant \eta \leqslant p^b \quad \text{and} \quad \eta \not\equiv \xi \pmod{p}. \tag{6.3}$$

The quantity $K_{a,b}^{m+1,r}(X; \xi, \eta)$ counts the number of integral solutions of the system (2.14) with m replaced by $m + 1$, subject to the attendant conditions on $\mathbf{x}$, $\mathbf{y}$, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$, $\mathbf{z}$. Given such a solution of the system (2.14), the discussion leading to (2.15) shows that

$$\sum_{i=1}^{m+1} (x_i - \eta)^j \equiv \sum_{i=1}^{m+1} (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leqslant j \leqslant k). \tag{6.4}$$

In the notation introduced in §3, it follows that for some k-tuple of integers $\mathbf{m}$, both $[\mathbf{x} \pmod{p^{kb}}]$ and $[\mathbf{y} \pmod{p^{kb}}]$ lie in $\mathcal{B}_{a,b}^{m+1}(\mathbf{m}; \xi, \eta)$. Write

$$\mathfrak{G}_{a,b}(\boldsymbol{\alpha}; \mathbf{m}) = \sum_{\boldsymbol{\theta} \in \mathcal{B}_{a,b}^{m+1}(\mathbf{m}; \xi, \eta)} \prod_{i=1}^{m+1} \mathfrak{f}_{kb}(\boldsymbol{\alpha}; \theta_i).$$

Then, on considering the underlying Diophantine systems, we see from (2.12) and (6.4) that

$$K_{a,b}^{m+1,r}(X; \xi, \eta) = \sum_{m_1=1}^{p^b} \cdots \sum_{m_k=1}^{p^{kb}} \oint |\mathfrak{G}_{a,b}(\boldsymbol{\alpha}; \mathbf{m})^2 \mathfrak{F}_m^*(\boldsymbol{\alpha})^2| \, d\boldsymbol{\alpha},$$

where we write

$$\mathfrak{F}_m^*(\boldsymbol{\alpha}) = \mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta) \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{s-m-1}. \tag{6.5}$$

We now partition the vectors in each set $\mathcal{B}_{a,b}^{m+1}(\mathbf{m}; \xi, \eta)$ into equivalence classes modulo $p^{b'}$ as in §3. Write $\mathcal{C}(\mathbf{m}) = \mathcal{C}_{a,b}^{m+1,b'/b}(\mathbf{m}; \xi, \eta)$. An application of Cauchy's inequality leads via (3.2) and Lemma 3.1 to the bound

$$\begin{aligned} |\mathfrak{G}_{a,b}(\boldsymbol{\alpha}; \mathbf{m})|^2 &= \Big| \sum_{\mathfrak{C} \in \mathcal{C}(\mathbf{m})} \sum_{\boldsymbol{\theta} \in \mathfrak{C}} \prod_{i=1}^{m+1} \mathfrak{f}_{kb}(\boldsymbol{\alpha}; \theta_i) \Big|^2 \\ &\leqslant \operatorname{card}(\mathcal{C}(\mathbf{m})) \sum_{\mathfrak{C} \in \mathcal{C}(\mathbf{m})} \Big| \sum_{\boldsymbol{\theta} \in \mathfrak{C}} \prod_{i=1}^{m+1} \mathfrak{f}_{kb}(\boldsymbol{\alpha}; \theta_i) \Big|^2 \\ &\leqslant k! \sum_{\mathfrak{C} \in \mathcal{C}(\mathbf{m})} \Big| \sum_{\boldsymbol{\theta} \in \mathfrak{C}} \prod_{i=1}^{m+1} \mathfrak{f}_{kb}(\boldsymbol{\alpha}; \theta_i) \Big|^2. \end{aligned}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

It may be helpful to note here that since $b'/b \leqslant k-m-ma/b$, then in view of the relation (3.2), it follows from Lemma 3.1 that

$$\mathrm{card}(\mathcal{C}(\mathbf{m})) = B_{a,b}^{m+1,b'/b}(p) \leqslant k!.$$

Hence,

$$K_{a,b}^{m+1,r}(X;\xi,\eta) \ll \sum_{\mathbf{m}} \sum_{\mathfrak{C}\in\mathcal{C}(\mathbf{m})} \oint \Big| \mathfrak{F}_m^*(\alpha) \sum_{\boldsymbol{\theta}\in\mathfrak{C}} \prod_{i=1}^{m+1} \mathfrak{f}_{kb}(\boldsymbol{\alpha};\theta_i) \Big|^2 d\boldsymbol{\alpha}.$$

For each k-tuple $\mathbf{m}$ and equivalence class $\mathfrak{C}$, the integral above counts solutions of (2.14) with the additional constraint that both $[\mathbf{x} \pmod{p^{kb}}]$ and $[\mathbf{y} \pmod{p^{kb}}]$ lie in $\mathfrak{C}$. In particular, one has $\mathbf{x} \equiv \mathbf{y} \pmod{p^{b'}}$. Moreover, the sets $\mathcal{B}_{a,b}^{m+1}(\mathbf{m};\xi,\eta)$ are disjoint for distinct k-tuples $\mathbf{m}$ with $1 \leqslant m_j \leqslant p^{jb}$ $(1 \leqslant j \leqslant k)$, so to each pair $(\mathbf{x},\mathbf{y})$ there corresponds at most one pair $(\mathbf{m},\mathfrak{C})$. Thus, we deduce that

$$K_{a,b}^{m+1,r}(X;\xi,\eta) \ll H^{\dagger}(X;\xi,\eta),$$

where $H^{\dagger}(X;\xi,\eta)$ denotes the number of solutions of (2.14) subject to the additional condition $\mathbf{x} \equiv \mathbf{y} \pmod{p^{b'}}$. Hence, on considering the underlying Diophantine systems and recalling (6.1), we discern that

$$K_{a,b}^{m+1,r}(X;\xi,\eta) \ll \oint \mathfrak{H}_{a,b'}^{m+1}(\boldsymbol{\alpha};\xi)|\mathfrak{F}_m^*(\boldsymbol{\alpha})|^2\, d\boldsymbol{\alpha}. \tag{6.6}$$

An inspection of the definition of $\Xi_a^m(\xi)$ in the preamble to (2.10) reveals on this occasion that when $\boldsymbol{\xi} \in \Xi_a^{m+1}(\xi)$, then

$$(\xi_1,\dots,\xi_m) \in \Xi_a^m(\xi) \quad \text{and} \quad (\xi_{m+1}) \in \Xi_a^1(\xi).$$

Then a further consideration of the underlying Diophantine systems leads from (6.6) via (6.1) to the upper bound

$$K_{a,b}^{m+1,r}(X;\xi,\eta) \ll \oint \mathfrak{H}_{a,b'}^{m}(\boldsymbol{\alpha};\xi)\mathfrak{H}_{a,b'}^{1}(\boldsymbol{\alpha};\xi)|\mathfrak{F}_m^*(\boldsymbol{\alpha})|^2\, d\boldsymbol{\alpha}.$$

By applying Hölder's inequality to the integral on the right-hand side of this relation, bearing in mind the definition (6.5), we obtain the bound

$$K_{a,b}^{m+1,r}(X;\xi,\eta) \ll U_1^{\omega_1}U_2^{\omega_2}U_3^{\omega_3}, \tag{6.7}$$

where

$$\omega_1 = \frac{s-m-1}{s-m}, \qquad \omega_2 = \frac{1}{s}, \qquad \omega_3 = \frac{m}{s(s-m)} \tag{6.8}$$

and

$$U_1 = \oint \mathfrak{H}_{a,b'}^{m}(\boldsymbol{\alpha};\xi)|\mathfrak{F}_b^r(\boldsymbol{\alpha};\eta)^2\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2m}|\, d\boldsymbol{\alpha}, \tag{6.9}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

$$U_2 = \oint |\mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta)|^2 \mathfrak{H}_{a,b'}^1(\boldsymbol{\alpha}; \xi)^s \, d\boldsymbol{\alpha}, \tag{6.10}$$

$$U_3 = \oint |\mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta)|^2 \mathfrak{H}_{a,b'}^m(\boldsymbol{\alpha}; \xi)^{s/m} \, d\boldsymbol{\alpha}. \tag{6.11}$$

We now relate the mean values U_i to those introduced in §2. Observe first that a consideration of the underlying Diophantine systems leads from (6.9) via (6.1) and (2.10) to the upper bound

$$U_1 \leqslant \oint |\mathfrak{F}_a^m(\boldsymbol{\alpha}; \xi)^2 \mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta)^2 \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{2s-2m}| \, d\boldsymbol{\alpha}.$$

On recalling (2.12) and (2.17), we thus deduce that

$$U_1 \leqslant K_{a,b}^{m,r}(X). \tag{6.12}$$

Next, by employing (6.2) within (6.10) and (6.11), we find that

$$U_2 + U_3 \ll (M^{b'-a})^s \max_{\substack{1 \leqslant \zeta \leqslant p^{b'} \\ \zeta \equiv \xi \pmod{p^a}}} \oint |\mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta)^2 \mathfrak{f}_{b'}(\boldsymbol{\alpha}; \zeta)^{2s}| \, d\boldsymbol{\alpha}.$$

Notice here that since the condition (6.3) implies that $\eta \not\equiv \xi \pmod{p}$, and we have $\zeta \equiv \xi \pmod{p^a}$ with $a \geqslant 1$, then once more one has $\zeta \not\equiv \eta \pmod{p}$. In this way we deduce from (2.11) and (2.16) that

$$U_2 + U_3 \ll (M^{b'-a})^s I_{b,b'}^{r,r}(X). \tag{6.13}$$

By substituting (6.12) and (6.13) into the relation

$$K_{a,b}^{m+1,r}(X; \xi, \eta) \ll U_1^{\omega_1} (U_2 + U_3)^{1-\omega_1},$$

that is immediate from (6.7), and then recalling (6.8) and (2.17), the conclusion of the lemma follows when $a \geqslant 1$. When $a = 0$, we must modify this argument slightly. In this case, from (2.19) and (2.20), we find that

$$K_{0,b}^{m+1,r}(X) = \max_{1 \leqslant \eta \leqslant p^b} \oint |\mathfrak{F}^{m+1}(\boldsymbol{\alpha}; \eta)^2 \mathfrak{F}_b^r(\boldsymbol{\alpha}; \eta)^2 \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{2s-2m-2}| \, d\boldsymbol{\alpha}.$$

The desired conclusion follows in this instance by pursuing the proof given above in the case $a \geqslant 1$, noting that the definition of $\mathfrak{F}^{m+1}(\boldsymbol{\alpha}; \eta)$ ensures that the variables resulting from the congruencing argument avoid the congruence class η modulo p. This completes our account of the proof of the lemma. □

We note that in our application of Lemma 6.1, we restrict to situations with $0 \leqslant m \leqslant r - 1$. Thus, since $r \leqslant r_0$, it follows from (2.2) that the hypothesis $a \leqslant b/\sqrt{k}$ ensures that

$$k - m - ma/b \geqslant k - (k - 2\sqrt{k} + 1) - (k - 2\sqrt{k} + 1)/\sqrt{k} > \sqrt{k}.$$

Since b is large, we are therefore at liberty to apply Lemma 6.1 with a choice for b' satisfying the condition $b/b' < 1/\sqrt{k}$, thereby preparing appropriately for subsequent applications of Lemma 6.1.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

§7. *The multigrade combination.* We next combine the estimates supplied by Lemma 6.1 so as to bound $K_{a,b}^{r,r}(X)$ in terms of the mean values $I_{b,k_m b}^{r,r}(X)$ $(0 \leqslant m \leqslant r-1)$, in which the integers k_m satisfy $k_m \leqslant k - m - \lceil m/\sqrt{k} \rceil$. Before announcing our basic asymptotic estimate, we define the exponents

$$s_m = s - m \quad \text{and} \quad \phi_m = (s-r)/(s_m s_{m+1}) \quad (0 \leqslant m \leqslant r-1). \tag{7.1}$$

In addition, we write

$$\phi^* = (s-r)/s, \tag{7.2}$$

so that

$$\begin{aligned} \phi^* + \sum_{m=0}^{r-1} \phi_m &= \frac{s-r}{s} + (s-r) \sum_{m=0}^{r-1} (s_{m+1}^{-1} - s_m^{-1}) \\ &= \frac{s-r}{s} + (s-r)\left(\frac{1}{s-r} - \frac{1}{s} \right) = 1. \end{aligned} \tag{7.3}$$

LEMMA 7.1. *Suppose that a and b are integers with $0 \leqslant a < b \leqslant \theta^{-1}$ and $(k-r+1)b \geqslant ra$, and suppose further that $a \leqslant b/\sqrt{k}$. Then, whenever a' is an integer with $a' \geqslant a$ for which $(k-r+1)b \geqslant ra'$, one has*

$$K_{a,b}^{r,r}(X) \ll (J_{s+r}(X/M^b))^{\phi^*} \prod_{m=0}^{r-1} ((M^{b_m - a})^s I_{b,b_m}^{r,r}(X))^{\phi_m},$$

where we write $b_m = (k-m)b - ma'$.

Proof. We prove by backwards induction that for $0 \leqslant l \leqslant r-1$, one has

$$K_{a,b}^{r,r}(X) \ll (K_{a,b}^{l,r}(X))^{\phi_l^*} \prod_{m=l}^{r-1} ((M^{b_m - a})^s I_{b,b_m}^{r,r}(X))^{\phi_m}, \tag{7.4}$$

where

$$\phi_l^* = (s-r)/(s-l).$$

The conclusion of the lemma follows from the case $l = 0$ of (7.4), on noting that Lemma 2.2 delivers the estimate $K_{a,b}^{0,r}(X) \ll J_{s+r}(X/M^b)$.

We observe first that the inductive hypothesis (7.4) holds when $l = r-1$, as a consequence of the case $m = r-1$ of Lemma 6.1 and the definitions (7.1) and (7.2). Suppose then that J is a non-negative integer not exceeding $r-2$, and that the inductive hypothesis (7.4) holds for $J < l \leqslant r-1$. An application of Lemma 6.1 yields the estimate

$$K_{a,b}^{J+1,r}(X) \ll ((M^{b_J - a})^s I_{b,b_J}^{r,r}(X))^{1/(s-J)} (K_{a,b}^{J,r}(X))^{(s-J-1)/(s-J)}.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

On substituting this bound into the estimate (7.4) with $l = J+1$, one obtains the new upper bound

$$K_{a,b}^{r,r}(X) \ll (K_{a,b}^{J,r}(X))^{\phi_J^*} \prod_{m=J}^{r-1} ((M^{b_m-a})^s I_{b,b_m}^{r,r}(X))^{\phi_m}$$

and thus the inductive hypothesis holds with $l = J$. This completes the inductive step, so in view of our earlier remarks, the conclusion of the lemma now follows. □

We next convert Lemma 7.1 into a more portable form by making use of the anticipated magnitude operator $[[\,\cdot\,]]$ introduced in (2.21) to (2.23).

LEMMA 7.2. *Suppose that a and b are integers with $0 \leqslant a < b \leqslant \theta^{-1}$ and $(k-r+1)b \geqslant ra$, and suppose further that $a \leqslant b/\sqrt{k}$. Then, whenever a' is an integer with $a' \geqslant a$ for which $(k-r+1)b \geqslant ra'$, one has*

$$[[K_{a,b}^{r,r}(X)]] \ll ((X/M^b)^{\Lambda+\delta})^{\phi^*} \prod_{m=0}^{r-1} [[I_{b,b_m}^{r,r}(X)]]^{\phi_m},$$

where $b_m = (k-m)b - ma'$.

Proof. We find from Lemma 7.1 in combination with (2.23) that

$$[[K_{a,b}^{r,r}(X)]] \ll M^{\mu^* b + \nu^* a} ((X/M^b)^{\Lambda+\delta})^{\phi^*} \prod_{m=0}^{r} [[I_{b,b_m}^{r,r}(X)]]^{\phi_m}, \tag{7.5}$$

where

$$\mu^* = s - \phi^*(s+r) - r\sum_{m=0}^{r-1} \phi_m \quad \text{and} \quad \nu^* = r - s\sum_{m=0}^{r-1} \phi_m.$$

On recalling (7.2) and (7.3), a modicum of computation confirms that

$$\mu^* = s - \phi^*(s+r) - r(1-\phi^*) = 0 \quad \text{and} \quad \nu^* = r - s(1-\phi^*) = 0.$$

The conclusion of the lemma is therefore immediate from (7.5). □

We next turn to the task of establishing a multistep multigrade combination. Here, in order to keep complications under control, we discard some information not essential to our ultimate iterative process. We begin by introducing some additional notation. We recall that R is a positive integer sufficiently large in terms of s and k. We consider R-tuples of integers $(m_1, \dots, m_R) \in [0, r-1]^R$, to each of which we associate an R-tuple of integers $\mathbf{h}(\mathbf{m}) = (h_1(\mathbf{m}), \dots, h_R(\mathbf{m})) \in [0, \infty)^R$. The integral tuples $\mathbf{h}(\mathbf{m})$ will be fixed as the iteration

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

proceeds, with $h_n(\mathbf{m})$ depending at most on the first n coordinates of $(m_1, \dots, m_R)$. We may abuse notation in some circumstances by writing $h_n(\mathbf{m}, m_n)$ or $h_n(m_1, \dots, m_{n-1}, m_n)$ in place of $h_n(m_1, \dots, m_R)$, reflecting the latter implicit dependence. We suppose that a (large) positive integer b has already been fixed. We then define the sequences $(a_n) = (a_n(\mathbf{m}; \mathbf{h}))$ and $(b_n) = (b_n(\mathbf{m}; \mathbf{h}))$ by putting

$$a_0 = \lfloor b/\sqrt{k} \rfloor \quad \text{and} \quad b_0 = b, \tag{7.6}$$

and then applying the iterative relations

$$a_n = b_{n-1} \quad \text{and} \quad b_n = (k-m_n)b_{n-1} - m_n a_{n-1} + h_n(\mathbf{m}) \quad (1 \leqslant n \leqslant R). \tag{7.7}$$

Finally, we define the quantity $\Theta_n(\mathbf{m}; \mathbf{h})$ for $0 \leqslant n \leqslant R$ by putting

$$\Theta_n(\mathbf{m}; \mathbf{h}) = (X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a_n,b_n}(X)]] + M^{-3sk^R b}. \tag{7.8}$$

LEMMA 7.3. *Suppose that a and b are integers with $0 \leqslant a < b \leqslant (16Rk^{2R}\theta)^{-1}$ and $(k-r+1)b \geqslant ra$, and suppose further that $a \leqslant b/\sqrt{k}$. Then there exists a choice for $\mathbf{h}(\mathbf{m}) \in [0, \infty)^R$, satisfying the condition that $0 \leqslant h_n(\mathbf{m}) \leqslant 15k^R b$ $(1 \leqslant n \leqslant R)$, and for which one has*

$$(X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a,b}(X)]] \ll \prod_{\mathbf{m}\in[0,r-1]^R} \Theta_R(\mathbf{m}; \mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}}.$$

Proof. We prove by induction on l that when $1 \leqslant l \leqslant R$, one has the upper bound

$$(X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a,b}(X)]] \ll \prod_{\mathbf{m}\in[0,r-1]^l} \Theta_l(\mathbf{m}; \mathbf{h})^{\phi_{m_1}\cdots\phi_{m_l}}. \tag{7.9}$$

We observe first that, as a consequence of (7.3) and Lemma 7.2, one has

$$(X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a,b}(X)]] \ll \prod_{m=0}^{r-1} ((X/M^b)^{-\Lambda-\delta}[[I^{r,r}_{b,b^*_m}(X)]])^{\phi_m}, \tag{7.10}$$

where

$$b^*_m = (k-m)b - m\lfloor b/\sqrt{k} \rfloor.$$

Moreover, it follows from Lemma 4.2 that for each m with $0 \leqslant m \leqslant r-1$, there exists an integer $h = h(m)$, with $0 \leqslant h \leqslant 15k^R b$, having the property that

$$I^{r,r}_{b,b^*_m}(X) \ll (M^h)^{2s/3} K^{r,r}_{b,b^*_m+h}(X) + (M^{15k^R b})^{-s/4}(X/M^{b^*_m})^s (X/M^b)^{\lambda-s},$$

whence from (2.22) and (2.23) we discern that

$$[[I^{r,r}_{b,b^*_m}(X)]] \ll M^{-hs/3}[[K^{r,r}_{b,b_1}(X)]] + M^{-3sk^R b}(X/M^b)^{\Lambda+\delta}, \tag{7.11}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

where

$$b_1 = (k-m)b_0 - ma_0 + h(m).$$

The inductive hypothesis (7.9) therefore follows in the case $R = 1$ by substituting (7.11) into (7.10). Notice here that we have discarded the factor $M^{-hs/3}$ from (7.11), since at this stage of our argument it serves only as an unwelcome complication.

Suppose next that the inductive hypothesis (7.9) holds for $1 \leqslant l < L$, with some integer L satisfying $L \leqslant R$. Consider the quantity $\Theta_{L-1}(\mathbf{m};\mathbf{h})$ for a given tuple $\mathbf{m} \in [0, r-1]^{L-1}$ and a fixed tuple $\mathbf{h} = \mathbf{h}(\mathbf{m})$. We distinguish two possibilities. If it is the case that

$$\Theta_{L-1}(\mathbf{m};\mathbf{h}) \ll M^{-3sk^Rb},$$

then from (7.3) one finds that

$$\Theta_{L-1}(\mathbf{m};\mathbf{h}) \ll \Big(\prod_{m_L=0}^{r-1} (M^{-3sk^Rb})^{\phi_{m_L}} \Big)^{s/r},$$

so that

$$\Theta_{L-1}(\mathbf{m};\mathbf{h}) \ll \prod_{m_L=0}^{r-1} (M^{-3sk^Rb})^{\phi_{m_L}} \ll \prod_{m_L=0}^{r-1} \Theta_L(\mathbf{m}, m_L; \mathbf{h}, 0)^{\phi_{m_L}}. \tag{7.12}$$

When

$$\Theta_{L-1}(\mathbf{m};\mathbf{h}) \ll (X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a_{L-1},b_{L-1}}(X)]],$$

meanwhile, we apply Lemma 7.2 to obtain the bound

$$\Theta_{L-1}(\mathbf{m};\mathbf{h}) \ll \Big(\frac{X}{M^b}\Big)^{-\Lambda-\delta} \Big(\frac{X}{M^{b_{L-1}}}\Big)^{(\Lambda+\delta)(1-r/s)} \prod_{m_L=0}^{r-1} [[I^{r,r}_{b_{L-1},b^*_{m_L}}(X)]]^{\phi_{m_L}}, \tag{7.13}$$

where

$$b^*_{m_L} = (k-m_L)b_{L-1} - ma_{L-1}.$$

Two observations here serve to confirm that Lemma 7.2 is applicable. First, the hypothesis $b \leqslant (16Rk^{2R}\theta)^{-1}$ ensures that $b_{L-1} \leqslant \theta^{-1}$. Second, just as in the discussion concluding §6, an inductive argument shows that $a_n \leqslant b_n/\sqrt{k}$ for each n, for the hypothesis $1 \leqslant r \leqslant r_0 = k - \lceil 2\sqrt{k}\rceil + 2$ ensures that whenever $a_{n-1} \leqslant b_{n-1}/\sqrt{k}$, then

$$k - m_n - m_n a_{n-1}/b_{n-1} \geqslant k - (k - 2\sqrt{k}+1) - (k-2\sqrt{k}+1)/\sqrt{k} > \sqrt{k},$$

whence $b_n > \sqrt{k}b_{n-1} = \sqrt{k}a_n$. The claimed relation therefore follows by induction from (7.6), and in particular one obtains

$$(k-r+1)b_{L-1} - ra_{L-1} \geqslant b_{L-1}(k - (k-2\sqrt{k}+1) - (k-2\sqrt{k}+1)/\sqrt{k}) > 0.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

The applicability of Lemma 7.2 now confirmed, we again invoke Lemma 4.2, finding that for each integer m_L with $0 \leqslant m_L \leqslant r-1$, there exists an integer $h_L = h_L(\mathbf{m}, m_L)$, with $0 \leqslant h_L \leqslant 15k^R b$, having the property that

$$[[I^{r,r}_{b_{L-1},b^*_{m_L}}(X)]] \ll M^{-h_L s/3}[[K^{r,r}_{b_{L-1},b_L}(X)]] + M^{-3sk^R b}(X/M^{b_{L-1}})^{\Lambda+\delta}.$$

Thus, we deduce that

$$\begin{aligned}(X/M^b)^{-\Lambda-\delta}[[I^{r,r}_{b_{L-1},b^*_{m_L}}(X)]] &\ll (X/M^b)^{-\Lambda-\delta}[[K^{r,r}_{a_L,b_L}(X)]] + M^{-3sk^R b}\\ &\ll \Theta_L(\mathbf{m}, m_L; \mathbf{h}, h_L).\end{aligned}$$

On substituting this estimate into (7.13), we deduce from (7.3) that

$$\begin{aligned}\Theta_{L-1}(\mathbf{m}; \mathbf{h}) &\ll (M^{b-b_{L-1}})^{(1-r/s)(\Lambda+\delta)} \prod_{m_L=0}^{r-1} \Theta_L(\mathbf{m}, m_L; \mathbf{h}, h_L)^{\phi_{m_L}}\\ &\ll \prod_{m_L=0}^{r-1} \Theta_L(\mathbf{m}, m_L; \mathbf{h}, h_L)^{\phi_{m_L}}. \qquad (7.14)\end{aligned}$$

Applying this estimate in combination with (7.12) within the case $l = L-1$ of the inductive hypothesis (7.9), we conclude that for some choice of the integer $h_L = h_L(\mathbf{m})$, one has the upper bound

$$(X/M^b)^{-\Lambda-\delta}[[K_{a,b}(X)]] \ll \prod_{\mathbf{m}\in[0,r-1]^{L-1}} \prod_{m_L=0}^{r-1} \Theta_L(\mathbf{m}, m_L; \mathbf{h}, h_L)^{\phi_{m_1}\cdots\phi_{m_L}}.$$

This confirms the inductive hypothesis (7.9) for $l = L$, and thus the conclusion of the lemma follows by induction. □

We remark that in obtaining the estimate (7.14), we made use of the trivial lower bound $b_{L-1} \geqslant b$. By discarding the power $M^{b-b_{L-1}}$ at this point, we are throwing away potentially useful information. However, it transpires that the weak information made available by the factor M^b in the conclusion of Lemma 7.3 already suffices for our purposes in the main iteration.

§8. *The latent monograde process.* Our objective in this section is to convert the block estimate encoded in Lemma 7.3 into a single monograde estimate that can be incorporated into our iterative method. We begin by recalling an elementary lemma from our previous work [**19**].

LEMMA 8.1. *Suppose that $z_0, \dots, z_l \in \mathbb{C}$, and that β_i and γ_i are positive real numbers for $0 \leqslant i \leqslant l$. Put $\Omega = \beta_0\gamma_0 + \cdots + \beta_l\gamma_l$. Then one has*

$$|z_0^{\beta_0} \cdots z_l^{\beta_l}| \leqslant \sum_{i=0}^{l} |z_i|^{\Omega/\gamma_i}.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Proof. This is [19, Lemma 8.1]. □

Before proceeding further, we introduce some additional notation. Define the positive number s_0 by means of the relation

$$s_0^R = \frac{\theta_+^{R+1} - \theta_-^{R+1}}{\theta_+ - \theta_-} - \frac{\theta_+\theta_-}{r\sqrt{k}}\left(\frac{\theta_+^R - \theta_-^R}{\theta_+ - \theta_-}\right), \tag{8.1}$$

in which $\theta_\pm$ are defined as in (2.6). We recall that, in view of (2.7), one has $s < s_0$. Next, casting an eye towards the iterative relations (7.6) and (7.7), we define new sequences $(\tilde{a}_n) = (\tilde{a}_n(\mathbf{m}))$ and $(\tilde{b}_n) = (\tilde{b}_n(\mathbf{m}))$ by means of the relations

$$\tilde{a}_0 = 1/\sqrt{k} \quad \text{and} \quad \tilde{b}_0 = 1, \tag{8.2}$$

and

$$\tilde{a}_n = \tilde{b}_{n-1} \quad \text{and} \quad \tilde{b}_n = (k - m_n)\tilde{b}_{n-1} - m_n\tilde{a}_{n-1} \quad (1 \leqslant n \leqslant R). \tag{8.3}$$

We then define

$$k_{\mathbf{m}} = \tilde{b}_R(\mathbf{m}) \quad \text{and} \quad \rho_{\mathbf{m}} = \tilde{b}_R(\mathbf{m})(s/s_0)^R \quad \text{for } \mathbf{m} \in [0, r-1]^R. \tag{8.4}$$

The motivation for defining the sequences $(\tilde{a}_n)$ and $(\tilde{b}_n)$ is to provide a base pair of sequences corresponding to the simplified situation in which $h_n(\mathbf{m}) = 0$ for all n and $\mathbf{m}$. It transpires that the corresponding sequences (a_n) and (b_n), equipped with potentially positive values of $h_n(\mathbf{m})$, may be bounded below by the sequences $(\tilde{a}_n)$ and $(\tilde{b}_n)$, although this turns out to be less simple to establish than might be supposed.

LEMMA 8.2. *Suppose that $\Lambda \geqslant 0$, let a and b be integers with*

$$0 \leqslant a < b \leqslant (20Rk^{2R}\theta)^{-1} \quad \textit{and} \quad (k - r + 1)b \geqslant ra,$$

and suppose further that $a \leqslant b/\sqrt{k}$. Suppose in addition that there are real numbers ψ, c and γ, with

$$0 \leqslant c \leqslant (2\delta)^{-1}\theta, \qquad \gamma \geqslant -sb \quad \textit{and} \quad \psi \geqslant 0,$$

such that

$$X^\Lambda M^{\Lambda\psi} \ll X^{c\delta} M^{-\gamma}[[K_{a,b}^{r,r}(X)]]. \tag{8.5}$$

Then, for some $\mathbf{m} \in [0, r-1]^R$, there are a real number h with $0 \leqslant h \leqslant 16k^{2R}b$, and positive integers a' and b' with $a' \leqslant b'/\sqrt{k}$, such that

$$X^\Lambda M^{\Lambda\psi'} \ll X^{c'\delta} M^{-\gamma'}[[K_{a',b'}^{r,r}(X)]], \tag{8.6}$$

where ψ', c', γ' and b' are real numbers satisfying the conditions

$$\psi' = \rho_{\mathbf{m}}(\psi + (1 - r/s)b), \qquad c' = \rho_{\mathbf{m}}(c + 1),$$
$$\gamma' = \rho_{\mathbf{m}}\gamma, \qquad b' = k_{\mathbf{m}}b + h.$$

Moreover, the real number $k_{\mathbf{m}}$ satisfies $2^R \leqslant k_{\mathbf{m}} \leqslant k^R$.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Proof. We deduce from the postulated bound (8.5) and Lemma 7.3 that there exists a choice of the tuple $\mathbf{h} = \mathbf{h}(\mathbf{m})$, with $0 \leqslant h_n(\mathbf{m}) \leqslant 15k^R b$ $(1 \leqslant n \leqslant R)$, such that

$$X^{\Lambda} M^{\Lambda\psi} \ll X^{(c+1)\delta} M^{-\gamma} (X/M^b)^{\Lambda} \prod_{\mathbf{m}\in[0,r-1]^R} \Theta_R(\mathbf{m};\mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}}.$$

Consequently, one has

$$\prod_{\mathbf{m}\in[0,r-1]^R} \Theta_R(\mathbf{m};\mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}} \gg X^{-(c+1)\delta} M^{\Lambda(\psi+b)+\gamma}.$$

Note that, in view of (7.3), one has

$$\sum_{m=0}^{r-1} \phi_m = r/s, \tag{8.7}$$

so that

$$\sum_{\mathbf{m}\in[0,r-1]^R} \phi_{m_1}\cdots\phi_{m_R} = (r/s)^R \leqslant r/s.$$

Then we deduce from the definition (7.8) of $\Theta_n(\mathbf{m};\mathbf{h})$ that

$$\begin{aligned} \prod_{\mathbf{m}\in[0,r-1]^R} &(X^{-\Lambda}[[K^{r,r}_{a_R,b_R}(X)]] + M^{-3sk^R b})^{\phi_{m_1}\cdots\phi_{m_R}} \\ &\gg X^{-(c+1)\delta} M^{\Lambda(\psi+(1-r/s)b)+\gamma}. \end{aligned} \tag{8.8}$$

In preparation for our application of Lemma 8.1, we examine the exponents $\phi_{m_1}\cdots\phi_{m_R}$ occurring in the lower bound (8.8). Our plan is to apply Lemma 8.1 with exponents given by

$$\beta^{(n)}_{\mathbf{m}} = \phi_{m_1}\cdots\phi_{m_n} \quad \text{and} \quad \gamma^{(n)}_{\mathbf{m}} = \tilde{b}_n(\mathbf{m}) \quad (\mathbf{m} \in [0, r-1]^n),$$

in the natural sense. In order to analyze the quantity Ω that will emerge from the application of this lemma, we define

$$B_n = \sum_{\mathbf{m}\in[0,r-1]^n} \beta^{(n)}_{\mathbf{m}} \tilde{b}_n(\mathbf{m}) \quad \text{and} \quad A_n = \sum_{\mathbf{m}\in[0,r-1]^n} \beta^{(n)}_{\mathbf{m}} \tilde{a}_n(\mathbf{m}),$$

and then put $\Omega = B_R$. From the iterative formulae (8.2) and (8.3), we obtain for $n \geqslant 1$ the relations

$$\begin{aligned} B_{n+1} &= \sum_{m_{n+1}=0}^{r-1} \sum_{\mathbf{m}\in[0,r-1]^n} ((k-m_{n+1})\tilde{b}_n(\mathbf{m}) - m_{n+1}\tilde{a}_n(\mathbf{m}))\phi_{m_1}\cdots\phi_{m_{n+1}} \\ &= B_n \sum_{m=0}^{r-1} (k-m)\phi_m - A_n \sum_{m=0}^{r-1} m\phi_m \end{aligned} \tag{8.9}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

and

$$A_{n+1} = \sum_{m_{n+1}=0}^{r-1} \sum_{\mathbf{m}\in[0,r-1]^n} \tilde{b}_n(\mathbf{m})\phi_{m_1}\cdots\phi_{m_{n+1}} = B_n \sum_{m=0}^{r-1} \phi_m. \tag{8.10}$$

We observe that from (7.1), one has

$$\sum_{m=0}^{r-1}(k-m)\phi_m = \sum_{m=0}^{r-1} \frac{(k-m)(s-r)}{(s-m)(s-m-1)}.$$

The summands on the right-hand side here may be rewritten in the shape

$$\frac{(r-m)(k-m)}{s-m} - \frac{(r-m-1)(k-m-1)}{s-m-1} - \frac{r-m-1}{s-m-1}.$$

Hence, we obtain

$$s\sum_{m=0}^{r-1}(k-m)\phi_m = kr - s\sum_{l=1}^{r}\frac{r-l}{s-l} = kr - \frac{1}{2}r(r-1) - \Delta,$$

in which Δ is defined via (2.3). In addition, one has

$$\begin{aligned} s\sum_{m=0}^{r-1} m\phi_m &= sk\sum_{m=0}^{r-1}\phi_m - s\sum_{m=0}^{r-1}(k-m)\phi_m \\ &= kr - \left(kr - \frac{1}{2}r(r-1) - \Delta\right) \\ &= \frac{1}{2}r(r-1) + \Delta. \end{aligned}$$

Utilizing the formulae just obtained, we conclude from (8.9) that for $n \geqslant 1$, one has

$$sB_{n+1} = (kr - \tfrac{1}{2}r(r-1) - \Delta)B_n - (\tfrac{1}{2}r(r-1) + \Delta)A_n,$$

while from (8.7) and (8.10), one sees that

$$sA_{n+1} = rB_n.$$

Then, on recalling (2.5), we arrive at the iterative relation

$$s^2B_{n+2} - s\mathfrak{a}B_{n+1} + \mathfrak{b}B_n = 0 \quad (n \geqslant 1). \tag{8.11}$$

In addition, also from (2.5) and (8.2), one has the initial data

$$sB_1 = s\sum_{m=0}^{r-1}((k-m)\tilde{b}_0 - m\tilde{a}_0)\phi_m = \mathfrak{a} - \mathfrak{b}/(r\sqrt{k}) \tag{8.12}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

and, from (8.2) and (8.7), one finds that

$$sA_1 = s\sum_{m=0}^{r-1} \tilde{b}_0\phi_m = r.$$

Thus, we see also that

$$\begin{aligned} s^2B_2 &= s^2\sum_{m=0}^{r-1}((k-m)B_1 - mA_1)\phi_m = s(\mathfrak{a}B_1 - \mathfrak{b}A_1/r) \\ &= \mathfrak{a}(\mathfrak{a} - \mathfrak{b}/(r\sqrt{k})) - \mathfrak{b}. \end{aligned} \tag{8.13}$$

On recalling (2.6), one finds that the recurrence formula (8.11) has a solution of the shape

$$s^nB_n = \sigma_+\theta_+^n + \sigma_-\theta_-^n \quad (n \geqslant 1),$$

where, in view of (8.12) and (8.13), one has

$$\sigma_+\theta_+ + \sigma_-\theta_- = sB_1 = \mathfrak{a} - \mathfrak{b}/(r\sqrt{k})$$

and

$$\sigma_+\theta_+^2 + \sigma_-\theta_-^2 = s^2B_2 = \mathfrak{a}(\mathfrak{a} - \mathfrak{b}/(r\sqrt{k})) - \mathfrak{b}.$$

Since $\mathfrak{a} = \theta_+ + \theta_-$ and $\mathfrak{b} = \theta_+\theta_-$, we therefore deduce that

$$s^nB_n = \frac{\theta_+^{n+1} - \theta_-^{n+1}}{\theta_+ - \theta_-} - \frac{\theta_+\theta_-}{r\sqrt{k}}\left(\frac{\theta_+^n - \theta_-^n}{\theta_+ - \theta_-}\right).$$

In particular, on recalling (8.1), we find that $s^RB_R = s_0^R$, so that

$$B_R = (s_0/s)^R. \tag{8.14}$$

Also, therefore, it follows from (2.7) that $s < s_0$ and hence also that $B_R > 1$.

Returning now to the application of Lemma 8.1, we note first that $\Omega = B_R$ and hence (8.8) yields the relation

$$\begin{aligned} &\sum_{\mathbf{m}\in[0,r-1]^R} (X^{-\Lambda}[[K_{a_R,b_R}^{r,r}(X)]] + M^{-3sk^Rb})^{B_R/\tilde{b}_R(\mathbf{m})} \\ &\quad \gg X^{-(c+1)\delta}M^{\Lambda(\psi+(1-r/s)b)+\gamma}. \end{aligned}$$

But, in view of (8.4) and (8.14), one has $\tilde{b}_R(\mathbf{m})/B_R = \rho_{\mathbf{m}}$, and thus we find that for some tuple $\mathbf{m} \in [0, r-1]^R$, one has

$$X^{-\Lambda}[[K_{a_R,b_R}^{r,r}(X)]] + M^{-3sk^Rb} \gg X^{-\rho_{\mathbf{m}}(c+1)\delta}M^{\Lambda\rho_{\mathbf{m}}(\psi+(1-r/s)b)+\rho_{\mathbf{m}}\gamma},$$

whence

$$X^{-\Lambda}[[K_{a_R,b_R}^{r,r}(X)]] + M^{-3sk^Rb} \gg X^{-c'\delta}M^{\Lambda\psi'+\gamma'}. \tag{8.15}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Two further issues remain to be resolved, the first being the removal of the term M^{-3sk^Rb} on the left-hand side of (8.15). We observe that the relations (8.3) ensure that $\tilde{b}_R(\mathbf{m}) \leqslant k^R$, and hence (8.4) reveals that $\rho_{\mathbf{m}} < \tilde{b}_R(\mathbf{m}) \leqslant k^R$. Our hypothesis on c therefore ensures that

$$c'\delta \leqslant k^R(c+1)\delta \leqslant k^R(\tfrac{1}{2}\theta + \delta) \leqslant k^R\theta,$$

so that

$$X^{-c'\delta}M^{\Lambda\psi'+\gamma'} \geqslant M^{-k^R+\rho_{\mathbf{m}}\gamma} > M^{-k^R-sk^Rb}.$$

Since

$$M^{-3sk^Rb} \leqslant M^{-2sk^R-sk^Rb},$$

it follows from (8.15) that

$$X^{-\Lambda}[[K^{r,r}_{a_R,b_R}(X)]] \gg X^{-c'\delta}M^{\Lambda\psi'+\gamma'}. \tag{8.16}$$

Our final task consists of extracting appropriate constraints on the parameters a_R and b_R. We note first that from (7.6), one has $a_0 = \lfloor b/\sqrt{k} \rfloor \leqslant b/\sqrt{k}$, so that on writing

$$h_1^*(\mathbf{m}) = h_1(\mathbf{m}) + m_1(b/\sqrt{k} - a_0)$$

and

$$h_n^*(\mathbf{m}) = h_n(\mathbf{m}) \quad (n > 1),$$

we have

$$h_1^*(\mathbf{m}) \leqslant h_1(\mathbf{m}) + m_1 \leqslant h_1(\mathbf{m}) + k < 16k^Rb$$

and

$$h_n^*(\mathbf{m}) = h_n(\mathbf{m}) \leqslant 16k^Rb \quad (n > 1).$$

Define the sequences $(a_n^*) = (a_n^*(\mathbf{m};\mathbf{h}))$ and $(b_n^*) = (b_n^*(\mathbf{m};\mathbf{h}))$ by means of the relations

$$a_n^* = b_{n-1}^* \quad \text{and} \quad b_n^* = (k-m_n)b_{n-1}^* - m_na_{n-1}^* + h_n^*(\mathbf{m}) \quad (1 \leqslant n \leqslant R),$$

where

$$a_0^* = b/\sqrt{k} \quad \text{and} \quad b_0^* = b.$$

Then a comparison with (7.6) and (7.7) reveals that $a_n^* = a_n$ and $b_n^* = b_n$ for $n \geqslant 1$. Moreover, it is apparent from (8.2) and (8.3) that $\tilde{a}_nb = a_n^*(\mathbf{m};\mathbf{0})$ and $\tilde{b}_nb = b_n^*(\mathbf{m};\mathbf{0})$ for $n \geqslant 0$. We claim that for $n \geqslant 0$, one has

$$b_n^*(\mathbf{m};\mathbf{0}) \leqslant b_n^*(\mathbf{m};\mathbf{h}) \leqslant b_n^*(\mathbf{m};\mathbf{0}) + 16k^{R+n}b. \tag{8.17}$$

The validity of these inequalities for $n = 0$ is immediate from the definition of $b_n^*(\mathbf{m};\mathbf{h})$. We use an inductive argument to establish (8.17) for $n \geqslant 1$, though this requires some discussion.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Observe first that, by linearity, the recurrence sequence $b_n^*(\mathbf{m};\mathbf{h})$ is given by the formula

$$b_n^*(\mathbf{m};\mathbf{h}) = b_n^*(\mathbf{m};\mathbf{0}) + \sum_{l=1}^{R} c_{n,l}(\mathbf{m};\mathbf{h}) \quad (0 \leqslant n \leqslant R), \tag{8.18}$$

in which $c_{n,l}(\mathbf{m};\mathbf{h})$ is determined by the relations

$$c_{l,l}(\mathbf{m};\mathbf{h}) = h_l^*(\mathbf{m}) \quad \text{and} \quad c_{n,l}(\mathbf{m};\mathbf{h}) = 0 \quad (n < l),$$

with

$$c_{n+1,l}(\mathbf{m};\mathbf{h}) = (k - m_{n+1})c_{n,l}(\mathbf{m};\mathbf{h}) - m_{n+1}c_{n-1,l}(\mathbf{m};\mathbf{h}) \quad (n \geqslant l). \tag{8.19}$$

We recall our assumption that $r \leqslant k - \lceil 2\sqrt{k} \rceil + 2$, which ensures that

$$m_{n+1} \leqslant r - 1 \leqslant k - \lceil 2\sqrt{k} \rceil + 1.$$

In view of this upper bound, we are able to prove by induction that

$$c_{n+1,l}(\mathbf{m};\mathbf{h}) > \sqrt{k}c_{n,l}(\mathbf{m};\mathbf{h}) \tag{8.20}$$

for each integer n with $n \geqslant l - 1$. In order to confirm this assertion, note first that such is the case when $n = l - 1$. Granted that $c_{n,l}(\mathbf{m};\mathbf{h}) > \sqrt{k}c_{n-1,l}(\mathbf{m};\mathbf{h})$, meanwhile, one deduces from (8.19) that when $n \geqslant l - 1$, one has

$$\begin{aligned} c_{n+1,l}(\mathbf{m};\mathbf{h}) &\geqslant (\lceil 2\sqrt{k} \rceil - 1)c_{n,l}(\mathbf{m};\mathbf{h}) - (k - \lceil 2\sqrt{k} \rceil + 1)c_{n,l}(\mathbf{m};\mathbf{h})/\sqrt{k} \\ &\geqslant ((2\sqrt{k} - 1) - (\sqrt{k} - 2 + 1/\sqrt{k}))c_{n,l}(\mathbf{m};\mathbf{h}) \\ &> \sqrt{k}c_{n,l}(\mathbf{m};\mathbf{h}), \end{aligned} \tag{8.21}$$

establishing this inductive hypothesis. Thus, in particular, one arrives at the lower bound $c_{n,l}(\mathbf{m};\mathbf{h}) \geqslant 0$ for all n. On substituting this conclusion into (8.18), we deduce that $b_n^*(\mathbf{m};\mathbf{h}) \geqslant b_n^*(\mathbf{m};\mathbf{0})$ for every n, confirming the first of the inequalities in (8.17).

Next, making use of the lower bound $c_{n,l}(\mathbf{m};\mathbf{h}) \geqslant 0$, just obtained, within (8.19), we find that

$$c_{n+1,l}(\mathbf{m};\mathbf{h}) \leqslant kc_{n,l}(\mathbf{m};\mathbf{h}) \quad (n \geqslant l),$$

so that

$$c_{n,l}(\mathbf{m};\mathbf{h}) \leqslant k^{n-l}h_l^*(\mathbf{m}) \quad (n \geqslant l).$$

We therefore deduce from (8.18) and the bound $h_n^*(\mathbf{m}) \leqslant 16k^R b$ that

$$b_n^*(\mathbf{m};\mathbf{h}) \leqslant b_n^*(\mathbf{m};\mathbf{0}) + 16k^R b \sum_{l=1}^{n} k^{n-l} \leqslant b_n^*(\mathbf{m};\mathbf{0}) + 16k^{R+n}b.$$

This confirms the second of the inequalities in (8.17).

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We now make use of the inequalities (8.17). Observe first that in view of (8.4), one has

$$b_R = b_R^*(\mathbf{m};\mathbf{h}) \leqslant b_R^*(\mathbf{m};\mathbf{0}) + 16k^{2R}b = \tilde{b}_R(\mathbf{m})b + 16k^{2R}b = k_{\mathbf{m}}b + 16k^{2R}b.$$

In addition, one has

$$b_R = b_R^*(\mathbf{m};\mathbf{h}) \geqslant b_R^*(\mathbf{m};\mathbf{0}) = \tilde{b}_R(\mathbf{m})b = k_{\mathbf{m}}b.$$

Thus, there exists an integer $h_{\mathbf{m}}$, with $0 \leqslant h_{\mathbf{m}} \leqslant 16k^{2R}b$, for which one has $b_R = k_{\mathbf{m}}b + h_{\mathbf{m}}$.

The argument confirming (8.21) shows also that for each $n \geqslant 0$, one has

$$b_{n+1}^*(\mathbf{m};\mathbf{0}) > \sqrt{k}b_n^*(\mathbf{m};\mathbf{0}). \tag{8.22}$$

Then it follows from (8.18) and (8.20) that

$$b_R^*(\mathbf{m};\mathbf{h}) > \sqrt{k}b_{R-1}^*(\mathbf{m};\mathbf{h}),$$

whence

$$a_R = b_{R-1} = b_{R-1}^*(\mathbf{m};\mathbf{h}) < b_R^*(\mathbf{m};\mathbf{h})/\sqrt{k} = b_R/\sqrt{k}.$$

Then we deduce from (8.16) that there exist integers $b' = b_R$, $a' = a_R$ and $h = h_{\mathbf{m}}$ satisfying the conditions

$$0 \leqslant h_{\mathbf{m}} \leqslant 16k^{2R}b, \qquad b' = k_{\mathbf{m}}b + h \qquad \text{and} \qquad a' \leqslant b'/\sqrt{k},$$

and for which

$$X^{-\Lambda}[[K_{a',b'}^{r,r}(X)]] \gg X^{-c'\delta}M^{\Lambda\psi'+\gamma'}.$$

The desired conclusion (8.6) now follows, with all the associated conditions.

It now remains only to confirm the bounds on $k_{\mathbf{m}}$ asserted in the final line of the statement of the lemma. For this, we note that by applying (8.22) in an inductive argument, one obtains from (8.4) the lower bound

$$k_{\mathbf{m}} = \tilde{b}_R(\mathbf{m}) = b_R^*(\mathbf{m};\mathbf{0})/b \geqslant (\sqrt{k})^R b_0^*(\mathbf{m};\mathbf{0})/b \geqslant 2^R.$$

Likewise, though more directly, one has

$$k_{\mathbf{m}} = \tilde{b}_R(\mathbf{m}) = b_R^*(\mathbf{m};\mathbf{0})/b \leqslant k^R b_0^*(\mathbf{m};\mathbf{0})/b = k^R.$$

Thus, $2^R \leqslant k_{\mathbf{m}} \leqslant k^R$, and the proof of the lemma is complete. □

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

§9. *The iterative process.* We begin with a crude estimate of use at the conclusion of our argument.

LEMMA 9.1. *Suppose that a and b are integers with $0 \leqslant a < b \leqslant (2\theta)^{-1}$. Then, provided that $\Lambda \geqslant 0$, one has*

$$[[K_{a,b}^{r,r}(X)]] \ll X^{\Lambda+\delta}.$$

Proof. On considering the underlying Diophantine equations, we deduce from Lemma 2.3 that

$$K_{a,b}^{r,r}(X) \ll (J_{s+r}(X/M^a))^{r/(s+r)}(J_{s+r}(X/M^b))^{s/(s+r)},$$

whence

$$[[K_{a,b}^{r,r}(X)]] \ll \frac{X^{\delta}((X/M^a)^{r/(s+r)}(X/M^b)^{s/(s+r)})^{s+r+\Lambda}}{(X/M^a)^r(X/M^b)^s} \leqslant X^{\Lambda+\delta}.$$

This completes the proof of the lemma. □

We now come to the main event.

The Proof of Theorem 2.1. We prove that when s is the largest integer smaller than s_1, then one has $\Lambda \leqslant 0$, for in such circumstances the conclusion of the lemma follows at once from (2.24). By reference to (2.5) and (2.6), we find that $s < s_1 = \theta_+$. Thus, since R has been chosen sufficiently large in terms of s, k and θ_+, the hypothesis $s < s_1$ ensures that $s < s_0$, where s_0 is defined by means of (8.1). Assume then that $\Lambda \geqslant 0$, for otherwise there is nothing to prove. We begin by noting that as a consequence of Lemma 5.1, one finds from (2.21) and (2.23) that there exists an integer h_{-1} with $0 \leqslant h_{-1} \leqslant 4B$ such that

$$[[J_{s+r}(X)]] \ll M^{Bs-sh_{-1}/3}[[K_{0,B+h_{-1}}^{r,r}(X)]].$$

We therefore deduce from (2.24) that

$$X^{\Lambda} \ll X^{\delta}[[J_{s+r}(X)]] \ll X^{\delta}M^{Bs-sh_{-1}/3}[[K_{0,B+h_{-1}}^{r,r}(X)]]. \tag{9.1}$$

Next, we define sequences (κ_n), (h_n), (a_n), (b_n), (c_n), (ψ_n) and (γ_n), for $0 \leqslant n \leqslant N$, in such a way that

$$2^R \leqslant \kappa_{n-1} \leqslant k^R, \qquad 0 \leqslant h_{n-1} \leqslant \max\{16k^{2R}b_{n-1}, 4B\} \tag{9.2}$$

and

$$X^{\Lambda}M^{\Lambda\psi_n} \ll X^{c_n\delta}M^{-\gamma_n}[[K_{a_n,b_n}^{r,r}(X)]]. \tag{9.3}$$

We note here that the sequences (a_n) and (b_n) are not directly related to our earlier use of these letters. Given a fixed choice for the sequences (a_n), (κ_n) and (h_n), the remaining sequences are defined by means of the relations

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

$$b_{n+1} = \kappa_n b_n + h_n, \tag{9.4}$$
$$c_{n+1} = (s/s_0)^R \kappa_n (c_n + 1), \tag{9.5}$$
$$\psi_{n+1} = (s/s_0)^R \kappa_n (\psi_n + (1 - r/s) b_n), \tag{9.6}$$
$$\gamma_{n+1} = (s/s_0)^R \kappa_n \gamma_n. \tag{9.7}$$

We put

$$\kappa_{-1} = k^R, \qquad b_{-1} = 0, \qquad a_0 = 0, \qquad b_0 = B + h_{-1},$$
$$\psi_0 = 0, \qquad c_0 = 1, \qquad \gamma_0 = \tfrac{1}{3} s h_{-1} - Bs,$$

so that both (9.2) and (9.3) hold with $n = 0$ as a consequence of our initial choice of κ_{-1} and b_{-1}, together with (9.1). We prove by induction that for each non-negative integer n with $n < N$, the sequences $(a_m)_{m=0}^n$, $(\kappa_m)_{m=0}^n$ and $(h_m)_{m=-1}^n$ may be chosen in such a way that

$$1 \leqslant b_n \leqslant (20Rk^{2R}\theta)^{-1}, \quad \psi_n \geqslant 0, \quad \gamma_n \geqslant -sb_n, \quad 0 \leqslant c_n \leqslant (2\delta)^{-1}\theta, \tag{9.8}$$
$$0 \leqslant a_n \leqslant b_n/\sqrt{k}, \qquad (k - r + 1)b_n \geqslant r a_n, \tag{9.9}$$

and so that (9.2) and (9.3) both hold with n replaced by $n + 1$.

Let $0 \leqslant n < N$, and suppose that (9.2) and (9.3) both hold for the index n. We have already shown such to be the case for $n = 0$. From (9.2) and (9.4), we find that $b_n \leqslant 5(17k^{2R})^n B$, whence, by invoking (2.8), we find that for $0 \leqslant n \leqslant N$, one has

$$b_n \leqslant (20Rk^{2R}\theta)^{-1}.$$

It is apparent from (9.5) and (9.6) that c_n and ψ_n are non-negative for all n. Observe also that since $s \leqslant s_0$ and $\kappa_m \leqslant k^R$, then by iterating (9.5) we obtain the bound

$$c_n \leqslant k^{Rn} + k^R \left(\frac{k^{Rn} - 1}{k^R - 1} \right) \leqslant 3k^{Rn} \quad (n \geqslant 0), \tag{9.10}$$

and by reference to (2.8) we see that $c_n \leqslant (2\delta)^{-1}\theta$ for $0 \leqslant n < N$.

In order to bound γ_n, we recall that $s \leqslant s_0$ and iterate the relation (9.7) to deduce that

$$\gamma_m = (s/s_0)^{Rm} \kappa_0 \cdots \kappa_{m-1} \gamma_0 \geqslant -(s/s_0)^{Rm} \kappa_0 \cdots \kappa_{m-1} Bs. \tag{9.11}$$

In addition, we find from (9.4) that for $m \geqslant 0$ one has $b_{m+1} \geqslant \kappa_m b_m$, so that an inductive argument yields the lower bound

$$b_m \geqslant \kappa_0 \cdots \kappa_{m-1} b_0 \geqslant \kappa_0 \cdots \kappa_{m-1} B.$$

Hence, we deduce from (9.11) that

$$\gamma_m \geqslant -(s/s_0)^{Rm} s b_m > -sb_m.$$

Assembling this conclusion together with those of the previous paragraph, we have shown that (9.8) holds for $0 \leqslant n \leqslant N$.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

At this point in the argument, we may suppose that (9.3), (9.8) and (9.9) hold for the index n. An application of Lemma 8.2 therefore reveals that there exist real numbers κ_n and h_n satisfying the constraints implied by (9.2) with n replaced by $n+1$, for which the upper bound (9.3) holds for some a_n with $0 \leqslant a_n \leqslant b_n/\sqrt{k}$, also with n replaced by $n+1$. Our hypothesis on r, moreover, ensures that $(k-r+1)b_{n+1} \geqslant ra_{n+1}$. Hence (9.9) holds also with n replaced by $n+1$. This completes the inductive step, so that in particular the upper bound (9.3) holds for $0 \leqslant n \leqslant N$.

We now exploit the bound just established. Since we have the upper bound $b_N \leqslant 5(17k^{2R})^N B \leqslant (2\theta)^{-1}$, it is a consequence of Lemma 9.1 that

$$[[K^{r,r}_{a_N,b_N}(X)]] \ll X^{\Lambda+\delta}.$$

By combining this with (9.3) and (9.11), we obtain the bound

$$X^{\Lambda} M^{\Lambda\psi_N} \ll X^{\Lambda+(c_N+1)\delta} M^{\kappa_0\cdots\kappa_{N-1}Bs(s/s_0)^{RN}}. \tag{9.12}$$

Meanwhile, an application of (9.10) in combination with (2.8) shows that $X^{(c_N+1)\delta} < M$. We therefore deduce from (9.12) that

$$\Lambda\psi_N \leqslant (s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}Bs + 1.$$

Notice here that $\kappa_n \geqslant 2^R$ and

$$s/s_0 \geqslant (s_1-1)/s_0 \geqslant 1 - 2/s_0 > \tfrac{1}{2}.$$

Hence,

$$1 < (s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}Bs,$$

so that

$$\Lambda\psi_N \leqslant 2(s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}Bs. \tag{9.13}$$

A further application of the lower bound $b_n \geqslant \kappa_0\cdots\kappa_{n-1}B$ leads from (9.6) and the bound $s \leqslant s_0$ to the relation

$$\begin{aligned}\psi_{n+1} &= (s/s_0)^R(\kappa_n\psi_n + \kappa_n(1-r/s)b_n)\\ &\geqslant (s/s_0)^R\kappa_n\psi_n + (s/s_0)^R\kappa_n(1-r/s)\kappa_0\cdots\kappa_{n-1}B\\ &\geqslant (s/s_0)^R\kappa_n\psi_n + (s/s_0)^{R(n+1)}(1-r/s)\kappa_0\cdots\kappa_nB.\end{aligned}$$

An inductive argument therefore delivers the lower bound

$$\psi_N \geqslant N(1-r/s)(s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}B.$$

Thus, we deduce from (9.13) that

$$\Lambda \leqslant \frac{2(s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}Bs}{N(1-r/s)(s/s_0)^{RN}\kappa_0\cdots\kappa_{N-1}B} = \frac{2s(1-r/s)^{-1}}{N}.$$

Since we are at liberty to take N as large as we please in terms of s and k, we are forced to conclude that $\Lambda \leqslant 0$. In view of our opening discussion, this completes the proof of the theorem. □

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

§10. *Strongly diagonal behaviour.* We are now equipped to establish Theorem 1.1 and its corollary. Let k be an integer with $k \geqslant 7$, put $r = k - \lceil 2\sqrt{k} \rceil + 2$ and suppose that s is a natural number with $s \geqslant \frac{1}{4}(k+1)^2$. We note that [**4**, Theorem 1.1] demonstrates that whenever $1 \leqslant s \leqslant \frac{1}{4}(k+1)^2$, then one has $J_{s,k}(X) \ll X^{s+\varepsilon}$, and so we are certainly at liberty to assume that $s > \frac{1}{4}(k+1)^2$. Write

$$\Delta = \sum_{m=1}^{r-1} \frac{m(r-m)}{s-m-r}, \tag{10.1}$$

and define s_1 as in the statement of Theorem 2.1. We aim to show that the real number

$$t_0 = kr - \tfrac{1}{2}r(r+1) - \Delta$$

satisfies the bounds

$$\max\{2r-1, \lceil \tfrac{1}{2}r(r-1) + \Delta \rceil\} \leqslant t_0 \leqslant s_1.$$

If these bounds be confirmed, then it follows from Theorem 2.1 that whenever

$$1 \leqslant s \leqslant t_0 + r = kr - \tfrac{1}{2}r(r-1) - \Delta,$$

then $J_{s,k}(X) \ll X^{s+\varepsilon}$, and the conclusion of Theorem 1.1 follows.

We observe in our first step that, in view of the lower bound $s > \frac{1}{4}(k+1)^2$ and our hypothesis $k \geqslant 7$, one has

$$\begin{aligned} \Delta &\leqslant \sum_{m=1}^{k-5} \frac{m(k-4-m)}{s-k+4-m} \leqslant \sum_{m=1}^{k-5} \frac{m(k-4-m)}{(k^2-6k+37)/4} \\ &= \frac{2(k-3)(k-4)(k-5)}{3(k^2-6k+37)} < \frac{2}{3}(k-6). \end{aligned}$$

Next, one finds that $t_0 \leqslant s_1$ provided only that

$$(kr - \tfrac{1}{2}r(r-1) - \Delta - 2r)^2 \leqslant (kr - \tfrac{1}{2}r(r-1) - \Delta)^2 - 4r(\tfrac{1}{2}r(r-1) + \Delta),$$

an inequality that is satisfied provided that

$$4r(kr - \tfrac{1}{2}r(r-1) - \Delta) - 4r^2 \geqslant 4r(\tfrac{1}{2}r(r-1) + \Delta).$$

This last inequality amounts to the constraint $kr - r(r-1) - r \geqslant 2\Delta$. We therefore conclude that $t_0 \leqslant s_1$ whenever $r(k-r) \geqslant \frac{4}{3}(k-6)$. But when $k \geqslant 7$, it is easily verified that

$$r(k-r) \geqslant (k - \lceil 2\sqrt{k} \rceil + 2)(\lceil 2\sqrt{k} \rceil - 2) \geqslant \tfrac{4}{3}(k-6) + 1$$

and hence we confirm that $t_0 \leqslant s_1$, as desired.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Meanwhile, the bound $\Delta < \frac{2}{3}(k-6)$ ensures that

$$\begin{aligned} kr - \tfrac{1}{2}r(r+1) - \Delta &\geqslant (k-r)r + (\tfrac{1}{2}r(r-1) + \Delta) - 2\Delta \\ &> \tfrac{1}{2}r(r-1) + \Delta + (r(k-r) - \tfrac{4}{3}(k-6)) \\ &\geqslant \tfrac{1}{2}r(r-1) + \Delta + 1. \end{aligned}$$

Since $k \geqslant 7$, moreover, one has

$$\begin{aligned} kr - \tfrac{1}{2}r(r+1) - \Delta &\geqslant k(r-1) - \tfrac{1}{2}r(r+1) \geqslant k(r-1) - \tfrac{1}{2}r(k-3) \\ &= \tfrac{1}{2}(k+3)r - k > 2r - 1. \end{aligned}$$

Then we have $t_0 \geqslant \max\{2r-1, \lceil \frac{1}{2}r(r-1) + \Delta \rceil\}$, confirming the final claimed bound. In view of our earlier discussion, the proof of Theorem 1.1 is complete.

We turn now to the proof of Corollary 1.2. We suppose again that $k \geqslant 7$, and we put

$$s = \tfrac{1}{2}k(k+1) - \lceil \tfrac{7}{3}k \rceil.$$

Again defining Δ as in (10.1), in which $r = k - \lceil 2\sqrt{k} \rceil + 2$, we find that

$$\begin{aligned} \Delta &\leqslant \sum_{m=1}^{k-5} \frac{m(k-4-m)}{k(k+1)/2 - (k-4) - (7k/3 + 2/3) - m} \\ &\leqslant \frac{(k-3)(k-4)(k-5)}{3k^2 - 23k + 50} < \frac{1}{3}k. \end{aligned}$$

Hence, we deduce that

$$\begin{aligned} &kr - \tfrac{1}{2}r(r-1) - \Delta \\ &> k(k - \lceil 2\sqrt{k} \rceil + 2) - \tfrac{1}{2}(k - \lceil 2\sqrt{k} \rceil + 2)(k - \lceil 2\sqrt{k} \rceil + 1) - \tfrac{1}{3}k \\ &= \tfrac{1}{2}k(k+1) - \tfrac{1}{2}(\lceil 2\sqrt{k} \rceil - 1)(\lceil 2\sqrt{k} \rceil - 2) - \tfrac{1}{3}k \\ &\geqslant \tfrac{1}{2}k(k+1) - \sqrt{k}(2\sqrt{k} - 1) - \tfrac{1}{3}k > s. \end{aligned}$$

We therefore deduce from Theorem 1.1 that since

$$s < kr - \frac{1}{2}r(r-1) - \sum_{m=1}^{r-1} \frac{m(r-m)}{s-r-m},$$

then $J_{s,k}(X) \ll X^{s+\varepsilon}$. This completes the proof of the corollary.

§11. *A refinement of the core iteration.* Our goal in this section is to outline an extension of our basic method that permits, for large exponents k, the refinement of Corollary 1.2 to deliver Theorem 1.3. The details of this extension are complicated enough that we aim for a somewhat abbreviated account, exploiting the discussion of §§2–10 so as to provide an outline.

In §2, we fixed r to be a parameter satisfying $1 \leqslant r \leqslant k - \lceil 2\sqrt{k} \rceil + 2$ in order to ensure that, as the iteration bounding $K_{a,b}^{r,r}(X)$ in terms of related mean values

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

$K^{r,r}_{a',b'}(X)$ proceeds, the exponents a' and b' satisfy the condition $a' \leqslant b'/\sqrt{k}$. The point of the latter constraint, in fact, is to ensure that the iteration tree of mean values does not encounter a situation in which $b' < a'$, which would be fatal for the method. By relaxing this condition, but pruning the iteration tree, we permit the possibility that a' may be much closer to b' in size, with the exponent mean s_0 increased so that it becomes closer to $\frac{1}{2}k(k+1)$.

Let $l = \lceil k^{1/3} \rceil$ and put $r = k - l$. We take s to be a natural number satisfying

$$\tfrac{1}{2}k(k+1) - 3k \leqslant s + r \leqslant \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3}.$$

We take R and N to be natural numbers sufficiently large in terms of s and k in the same manner as in §2, and define B, θ and δ as in (2.8). Other aspects of our initial set-up follow those of §2, *mutatis mutandis*. Lemma 6.1 remains valid provided that $(k-m)b \geqslant (m+1)a$. If instead one has $(k-m)b < (m+1)a$, then one may make use of an alternative inequality based on the application of Hölder's inequality.

LEMMA 11.1. *Let m be an integer with $0 \leqslant m \leqslant r-1$. Suppose that a and b are integers with $0 \leqslant a < b \leqslant \theta^{-1}$. Then one has*

$$K^{m+1,r}_{a,b}(X) \ll (J_{s+r}(X/M^a))^{\omega_1} (J_{s+r}(X/M^b))^{\omega_2} (K^{m,r}_{a,b}(X))^{\omega_3},$$

where

$$\omega_1 = \frac{s}{(s+r)(s-m)}, \qquad \omega_2 = \frac{r}{(s+r)(s-m)} \qquad \text{and} \qquad \omega_3 = \frac{s-m-1}{s-m}.$$

Proof. On considering the underlying Diophantine systems, it follows from (2.12) and (2.14) that for some integers ξ and η, one has

$$K^{m+1,r}_{a,b}(X) \leqslant \oint |\mathfrak{F}^m_a(\boldsymbol{\alpha};\xi)^2 \mathfrak{f}_a(\boldsymbol{\alpha};\xi)^2 \mathfrak{F}^r_b(\boldsymbol{\alpha};\eta)^2 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2m-2}|\, d\boldsymbol{\alpha}.$$

Then, by Hölder's inequality, we obtain

$$K^{m+1,r}_{a,b}(X) \leqslant I_1^{\psi_1} I_2^{\psi_2} I_3^{\psi_3} I_4^{\psi_4} I_5^{\psi_5},$$

where

$$I_1 = \oint |\mathfrak{F}^m_a(\boldsymbol{\alpha};\xi)^4 \mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2s+2r-4m}|\, d\boldsymbol{\alpha},$$

$$I_2 = \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)|^{2s+2r}\, d\boldsymbol{\alpha}, \qquad I_3 = \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)|^{2s+2r}\, d\boldsymbol{\alpha},$$

$$I_4 = \oint |\mathfrak{F}^m_a(\boldsymbol{\alpha};\xi)^2 \mathfrak{F}^r_b(\boldsymbol{\alpha};\eta)^2 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2m}|\, d\boldsymbol{\alpha},$$

$$I_5 = \oint |\mathfrak{F}^m_a(\boldsymbol{\alpha};\xi)^2 \mathfrak{F}^r_b(\boldsymbol{\alpha};\eta)^4 \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s-2r-2m}|\, d\boldsymbol{\alpha},$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

$$\psi_1 = \frac{1}{2s-2m}, \qquad \psi_2 = \frac{s-r}{(s+r)(2s-2m)}, \qquad \psi_3 = \omega_2,$$
$$\psi_4 = \frac{s-m-2}{s-m} \quad \text{and} \quad \psi_5 = \frac{1}{s-m}.$$

A further consideration of the underlying Diophantine systems reveals that $I_1 \leqslant I_2$ and $I_5 \leqslant I_4$, and thus it follows from Lemma 2.2 and (2.12) that

$$K_{a,b}^{m+1,r}(X) \ll (J_{s+r}(X/M^a))^{\psi_1+\psi_2}(J_{s+r}(X/M^b))^{\omega_2}(K_{a,b}^{m,r}(X))^{\psi_4+\psi_5}.$$

The conclusion of the lemma follows at once. □

Our substitute for Lemma 7.2 must offer a surrogate for the upper bound supplied by Lemma 6.1 in those circumstances wherein m and a are both large. In this context, we introduce the parameter $u = u(a,b)$ defined by

$$u(a,b) = rb/(a+b). \tag{11.1}$$

Notice that when $0 \leqslant m \leqslant u-1$, one then has

$$(k-m)b - ma > (k-r)b = lb.$$

We recall also the definitions of ϕ_m and ϕ^* from (7.1) and (7.2), and also write

$$\varphi_0 = \frac{s(r-u)}{(s+r)(s-u)} \quad \text{and} \quad \varphi_1 = \frac{r(r-u)}{(s+r)(s-u)}.$$

LEMMA 11.2. *Suppose that a and b are integers with $0 \leqslant a < b \leqslant \theta^{-1}$, and define $u(a,b)$ by means of (11.1). Then, whenever a' is an integer with $a' \geqslant a$ for which $(k-r+1)b \geqslant ra'$, and u is an integer with $0 \leqslant u \leqslant u(a,b)$, one has*

$$[[K_{a,b}^{r,r}(X)]] \ll ((X/M^a)^{\varphi_0}(X/M^b)^{\phi^*+\varphi_1})^{\Lambda+\delta} \prod_{m=0}^{u-1} [[I_{b,b_m}^{r,r}(X)]]^{\phi_m},$$

where we write $b_m = (k-m)b - ma'$.

Proof. By following the argument of the proof of Lemma 7.1, though substituting Lemma 11.1 in place of Lemma 6.1 when $u \leqslant m \leqslant r-1$, we deduce that

$$K_{a,b}^{r,r}(X) \ll (J_{s+r}(X/M^b))^{\phi^*}(J_{s+r}(X/M^a))^{\varphi_0}(J_{s+r}(X/M^b))^{\varphi_1} \times \prod_{m=0}^{u-1} ((M^{b_m-a})^s I_{b,b_m}^{r,r}(X))^{\phi_m}.$$

It may be useful here to note that

$$\sum_{m=u}^{r-1} \phi_m = (s-r)\sum_{m=u}^{r-1}(s_{m+1}^{-1} - s_m^{-1}) = (s-r)\left(\frac{1}{s-r} - \frac{1}{s-u}\right) = \frac{r-u}{s-u}.$$

Thus, on recalling the definitions (2.21) to (2.23), we obtain the conclusion of the lemma, just as in the argument delivering Lemma 7.2. □

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We next combine iterated applications of Lemma 11.2 so as to engineer a block multigrade process analogous to that delivered by Lemma 7.3. Before announcing the lemma that summarizes this process, we pause to modify the notation of §7. We consider R-tuples $\mathbf{h}$ just as in the preamble to Lemma 7.3. The sequences $(a_n) = (a_n(\mathbf{m};\mathbf{h}))$ and $(b_n) = (b_n(\mathbf{m};\mathbf{h}))$ are now defined by putting

$$a_0 = \lfloor b/l \rfloor \quad \text{and} \quad b_0 = b$$

and then applying the iterative relations (7.7). We then define $u_n(\mathbf{m};\mathbf{h})$ by putting

$$u_n(\mathbf{m};\mathbf{h}) = rb_{n-1}/(a_{n-1} + b_{n-1}). \tag{11.2}$$

We emphasize here that, since a_{n-1} and b_{n-1} depend at most on the first $n-1$ coordinates of $\mathbf{m}$ and $\mathbf{h}$, then the same holds for $u_n(\mathbf{m};\mathbf{h})$. We use the notation

$$\prod_{\mathbf{0}\leqslant\mathbf{m}\leqslant\mathbf{u}-1}$$

as shorthand for the ordered product

$$\prod_{0\leqslant m_1\leqslant u_1-1}\ \prod_{0\leqslant m_2\leqslant u_2-1}\ \cdots\ \prod_{0\leqslant m_R\leqslant u_R-1}.$$

Finally, we redefine the quantity $\Theta_n(\mathbf{m};\mathbf{h})$ for $0 \leqslant n \leqslant R$ by putting

$$\Theta_n(\mathbf{m};\mathbf{h}) = (X/M^{b/2})^{-\Lambda-\delta}[[K^{r,r}_{a_n,b_n}(X)]] + M^{-3sk^Rb}. \tag{11.3}$$

LEMMA 11.3. *Suppose that a and b are integers with*

$$0 \leqslant a < b \leqslant (16Rk^{2R}\theta)^{-1},$$

and suppose further that $a \leqslant b/l$. Suppose also that $u_1, \dots, u_R$ are integers with $0 \leqslant u_i \leqslant u_i(\mathbf{m};\mathbf{h})$ $(1 \leqslant i \leqslant R)$. Then there exists a choice for $\mathbf{h}(\mathbf{m}) \in [0,\infty)^R$, satisfying the condition that $0 \leqslant h_n(\mathbf{m}) \leqslant 15k^Rb$ $(1 \leqslant n \leqslant R)$, and for which one has

$$(X/M^{b/2})^{-\Lambda-\delta}[[K^{r,r}_{a,b}(X)]] \ll \prod_{\mathbf{0}\leqslant\mathbf{m}\leqslant\mathbf{u}-1} \Theta_R(\mathbf{m};\mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}}.$$

Proof. One may follow the inductive strategy adopted in the proof of Lemma 7.3. The key difference in the present setting is that Lemma 11.2 contains additional factors in the estimate made available for $[[K^{r,r}_{a,b}(X)]]$. However, it follows from Lemma 11.2 that whenever $u \leqslant u(a,b)$, then

$$(X/M^{b/2})^{-\Lambda-\delta}[[K^{r,r}_{a,b}(X)]] \ll (M^{(\Lambda+\delta)b})^{\Omega} \prod_{m=0}^{u-1} ((X/M^{b/2})^{-\Lambda-\delta}[[I^{r,r}_{b,b_m}(X)]])^{\phi_m},$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

where

$$\Omega = \frac{1}{2} - \frac{1}{2}\sum_{m=0}^{u-1} \phi_m - (\phi^* + \varphi_1).$$

But we have

$$\sum_{m=0}^{u-1} \phi_m = (s-r)\sum_{m=0}^{u-1}\left(\frac{1}{s-m-1} - \frac{1}{s-m}\right) = \frac{u(s-r)}{s(s-u)}$$

and hence $2s(s-u)(s+r)\Omega$ is equal to

$$\begin{aligned} &-s(s+r)(s-u) - u(s-r)(s+r) + 2r(s-u)(s+r) - 2r(r-u)s \\ &\quad = -s^3 + rs^2 + urs - ur^2 = -(s-r)(s^2 - ur). \end{aligned}$$

Since we may suppose that $s > r$, $s > u$ and $s^2 > ur$, we find that $\Omega < 0$ and hence

$$(X/M^{b/2})^{-\Lambda-\delta}[[K_{a,b}^{r,r}(X)]] \ll \prod_{m=0}^{u-1}((X/M^{b/2})^{-\Lambda-\delta}[[I_{b,b_m}^{r,r}(X)]])^{\phi_m}.$$

This relation serves as a substitute for Lemma 7.2 in the proof of Lemma 7.3, the proof of which now applies without serious modification. This completes our account of the proof of Lemma 11.3. □

We must now grapple with the somewhat daunting task of developing an analogue of Lemma 8.2 in the current setting. We now define the sequences $(\tilde{a}_n) = (\tilde{a}_n(\mathbf{m}))$ and $(\tilde{b}_n) = (\tilde{b}_n(\mathbf{m}))$ by putting

$$\tilde{a}_0 = 1/l \quad \text{and} \quad \tilde{b}_0 = 1,$$

and then applying the relations (8.3). We define the parameters $\tilde{u}_i = \tilde{u}_i(\mathbf{m})$ and $\tilde{v}_i = \tilde{v}_i(\mathbf{m})$ for $1 \leqslant i \leqslant R$ by putting

$$\tilde{u}_i(\mathbf{m}) = r\tilde{b}_{i-1}/(\tilde{a}_{i-1} + \tilde{b}_{i-1}) \quad \text{and} \quad \tilde{v}_i(\mathbf{m}) = \lfloor \tilde{u}_i(\mathbf{m}) \rfloor. \tag{11.4}$$

Next, we define the positive real number s_0 by means of the relation

$$s_0^R = s^R \sum_{m_1=0}^{\tilde{v}_1-1}\sum_{m_2=0}^{\tilde{v}_2-1}\cdots\sum_{m_R=0}^{\tilde{v}_R-1} \phi_{m_1}\phi_{m_2}\cdots\phi_{m_R}\tilde{b}_R(\mathbf{m}), \tag{11.5}$$

and then put

$$k_{\mathbf{m}} = \tilde{b}_R(\mathbf{m}) \quad \text{and} \quad \rho_{\mathbf{m}} = \tilde{b}_R(\mathbf{m})(s/s_0)^R \quad (\mathbf{m} \in [0, r-1]^R). \tag{11.6}$$

We note here that the values of $k_{\mathbf{m}}$ and $\rho_{\mathbf{m}}$ are not relevant when $\mathbf{m}$ does not satisfy the condition $0 \leqslant m_i \leqslant \tilde{v}_i - 1$ $(1 \leqslant i \leqslant R)$, and so we are indifferent to the values stemming from (11.6) in such circumstances.

Before proceeding further, we pause to relate u_i and $\tilde{u}_i$.

LEMMA 11.4. *Suppose that* $a \leqslant b/l$ *and* $0 \leqslant h_n(\mathbf{m}) \leqslant 16k^R b$ $(1 \leqslant n \leqslant R)$. *Then one has* $0 \leqslant \tilde{u}_n(\mathbf{m}) \leqslant u_n(\mathbf{m}; \mathbf{h})$ $(1 \leqslant n \leqslant R)$.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Proof. We prove the asserted inequalities by induction, beginning with the case $n = 1$. From (11.4), we find on the one hand that

$$\tilde{u}_1 = r\tilde{b}_0/(\tilde{a}_0 + \tilde{b}_0) = r/(1 + 1/l),$$

whilst, on the other, from (11.2), one has

$$u_1 = rb_0/(a_0 + b_0) = r/(1 + a_0/b) \geqslant r(1 + 1/l).$$

Thus $\tilde{u}_1 \leqslant u_1$, confirming the inductive hypothesis when $n = 1$. Suppose next that $n \geqslant 1$ and $\tilde{u}_n \leqslant u_n$. One has

$$\frac{b_{n+1}}{a_{n+1} + b_{n+1}} \geqslant \frac{\tilde{b}_{n+1}}{\tilde{a}_{n+1} + \tilde{b}_{n+1}} \tag{11.7}$$

if and only if $b_{n+1}/a_{n+1} \geqslant \tilde{b}_{n+1}/\tilde{a}_{n+1}$, which is to say that

$$((k - m_{n+1})b_n - m_{n+1}a_n + h_{n+1})/b_n \geqslant ((k - m_{n+1})\tilde{b}_n - m_{n+1}\tilde{a}_n)/\tilde{b}_n.$$

This lower bound is satisfied if and only if $m_{n+1}\tilde{a}_n/\tilde{b}_n \geqslant (m_{n+1}a_n - h_{n+1})/b_n$. The latter is automatically satisfied when either $m_{n+1} = 0$ or $h_{n+1} \geqslant m_{n+1}a_n$, and otherwise it is equivalent to the upper bound

$$\frac{\tilde{b}_n}{\tilde{a}_n + \tilde{b}_n} \leqslant \frac{b_n}{a_n + b_n - h_{n+1}/m_{n+1}}.$$

However, when $m_{n+1} > 0$, in view of our hypothesis $\tilde{u}_n \leqslant u_n$, one has

$$\frac{\tilde{b}_n}{\tilde{a}_n + \tilde{b}_n} \leqslant \frac{b_n}{a_n + b_n} \leqslant \frac{b_n}{a_n + b_n - h_{n+1}/m_{n+1}}.$$

Thus, we conclude from (11.2), (11.4) and (11.7) that $\tilde{u}_{n+1} \leqslant u_{n+1}$. This confirms the inductive hypothesis and hence we deduce that $0 \leqslant \tilde{u}_n \leqslant u_n$ for $1 \leqslant n \leqslant R$, as claimed. □

We next introduce some additional quantities of use in our ultimate application of Lemma 8.1. Define the exponents $\beta_{\mathbf{m}}^{(l)}$ and $\gamma_{\mathbf{m}}^{(l)}$ just as in the discussion following (8.8) above. We now put

$$B_n = \sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_n=0}^{\tilde{v}_n-1} \beta_{\mathbf{m}}^{(n)} \tilde{b}_n(\mathbf{m}) \quad \text{and} \quad A_n = \sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_n=0}^{\tilde{v}_n-1} \beta_{\mathbf{m}}^{(n)} \tilde{a}_n(\mathbf{m}). \tag{11.8}$$

In order to understand these sequences, we introduce some auxiliary sequences $\tilde{A}_n$ and $\tilde{B}_n$ as follows. We put

$$\mathfrak{a} = \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 3k^{2/3} \quad \text{and} \quad \mathfrak{b} = \tfrac{1}{2}k(k-1) + 3k^{5/3}. \tag{11.9}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

The sequence $\tilde{B}_n$ is then defined for $n \geqslant 1$ by means of the relations

$$s\tilde{B}_1 = \mathfrak{a} - \mathfrak{b}/l, \qquad s^2\tilde{B}_2 = \mathfrak{a}(\mathfrak{a} - \mathfrak{b}/l) - r\mathfrak{b} \tag{11.10}$$

and

$$s^2\tilde{B}_{n+2} = s\mathfrak{a}\tilde{B}_{n+1} - r\mathfrak{b}\tilde{B}_n \quad (n \geqslant 1). \tag{11.11}$$

Finally, we put

$$\theta_\pm = \tfrac{1}{2}(\mathfrak{a} \pm \sqrt{\mathfrak{a}^2 - 4r\mathfrak{b}}). \tag{11.12}$$

LEMMA 11.5. *When $n \geqslant 1$, one has $B_n \geqslant \tilde{B}_n$. In particular, one has the lower bound $B_R \geqslant \tilde{B}_R$ and hence*

$$s_0^R \geqslant \frac{\theta_+^{R+1} - \theta_-^{R+1}}{\theta_+ - \theta_-} - \frac{\theta_+\theta_-}{lr}\left(\frac{\theta_+^R - \theta_-^R}{\theta_+ - \theta_-}\right).$$

Proof. We have

$$B_{n+1} = \sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_n=0}^{\tilde{v}_n-1} \beta_{\mathbf{m}}^{(n)} \sum_{m_{n+1}=0}^{\tilde{v}_{n+1}-1} \phi_{m_{n+1}} \tilde{b}_{n+1}(\mathbf{m}). \tag{11.13}$$

The innermost sum here is

$$\sum_{m_{n+1}=0}^{\tilde{v}_{n+1}-1} \phi_{m_{n+1}} \tilde{b}_{n+1}(\mathbf{m}) = \mathfrak{B}(\tilde{v}_{n+1})\tilde{b}_n(\mathbf{m}) - \mathfrak{A}(\tilde{v}_{n+1})\tilde{a}_n(\mathbf{m}), \tag{11.14}$$

where

$$\mathfrak{B}(u) = \sum_{m=0}^{u-1}(k-m)\phi_m \quad \text{and} \quad \mathfrak{A}(u) = \sum_{m=0}^{u-1} m\phi_m.$$

We observe that when u is a positive integer, one has

$$\begin{aligned}\mathfrak{B}(u) &= \sum_{m=0}^{u-1} \frac{(k-m)(s-r)}{(s-m)(s-m-1)} \\ &= \sum_{m=0}^{u-1}\left(\frac{(r-m)(k-m)}{s-m} - \frac{(r-m-1)(k-m-1)}{s-m-1} - \frac{r-m-1}{s-m-1}\right),\end{aligned}$$

whence

$$\begin{aligned}s\mathfrak{B}(u) &= kr - \frac{s(r-u)(k-u)}{s-u} - s\sum_{m=1}^{u}\frac{r-m}{s-m} \\ &= u(k+r-u) - \frac{u(r-u)(k-u)}{s-u} - \frac{1}{2}r(r-1) \\ &\quad + \frac{1}{2}(r-u-1)(r-u) - \sum_{m=1}^{u}\frac{m(r-m)}{s-m}.\end{aligned}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Thus, we conclude that

$$s\mathfrak{B}(u) = ku - \frac{1}{2}u(u-1) - \frac{u(r-u)(k-u)}{s-u} - \sum_{m=1}^{u} \frac{m(r-m)}{s-m}. \tag{11.15}$$

One finds in like manner that

$$\begin{aligned} s\mathfrak{A}(u) &= sk\sum_{m=0}^{u-1}\phi_m - s\sum_{m=0}^{u-1}(k-m)\phi_m \\ &= \frac{ku(s-r)}{s-u} - \left(ku - \frac{1}{2}u(u-1) - \frac{u(r-u)(k-u)}{s-u}\right. \\ &\quad \left. - \sum_{m=1}^{u}\frac{m(r-m)}{s-m}\right) \\ &= \frac{1}{2}u(u-1) - \frac{u^2(r-u)}{s-u} + \sum_{m=1}^{u}\frac{m(r-m)}{s-m}. \end{aligned} \tag{11.16}$$

Write

$$v = \tilde{v}_{n+1}, \qquad h = r - v = k - l - v \quad \text{and} \quad \widetilde{\Delta} = \sum_{m=1}^{v}\frac{m(r-m)}{s-m}.$$

Then we see from (11.15) that $s\mathfrak{B}(v)$ is equal to

$$\begin{aligned} &k(k-l-h) - \frac{1}{2}(k-l-h)(k-l-h-1) - \frac{h(l+h)(k-l-h)}{s-k+l+h} - \widetilde{\Delta} \\ &\quad = \frac{1}{2}k(k+1) - \frac{1}{2}(l+h)(l+h+1) - \frac{h(l+h)(k-l-h)}{s-k+l+h} - \widetilde{\Delta}. \end{aligned}$$

Also, from (11.16), we find that $s\mathfrak{A}(v)$ is equal to

$$\begin{aligned} &\frac{1}{2}(k-l-h)(k-l-h-1) - \frac{h(k-l-h)^2}{s-k+l+h} + \widetilde{\Delta} \\ &\quad = \frac{1}{2}k(k-1) - (l+h)k + \frac{1}{2}(l+h)(l+h+1) - \frac{h(k-l-h)^2}{s-k+l+h} + \widetilde{\Delta}. \end{aligned}$$

On substituting these formulae into (11.14), we find that

$$s\sum_{m_{n+1}=0}^{\tilde{v}_{n+1}-1}\phi_{m_{n+1}}\tilde{b}_{n+1}(\mathbf{m}) = \mathfrak{a}_0\tilde{b}_n(\mathbf{m}) - \mathfrak{b}_0\tilde{a}_n(\mathbf{m}) - \Upsilon, \tag{11.17}$$

where

$$\begin{aligned} \mathfrak{a}_0 &= \tfrac{1}{2}k(k+1) - \tfrac{1}{2}l(l+1) - \widetilde{\Delta}, \\ \mathfrak{b}_0 &= \tfrac{1}{2}k(k-1) - lk + \tfrac{1}{2}l(l+1) + \widetilde{\Delta} \end{aligned}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

and

$$\Upsilon = \Big(lh + \frac{1}{2}h(h+1)\Big)(\tilde{a}_n + \tilde{b}_n) + \frac{h(l+h)(k-l-h)}{s-k+l+h}\tilde{b}_n \\ - \Big(hk + \frac{h(k-l-h)^2}{s-k+l+h}\Big)\tilde{a}_n. \tag{11.18}$$

We next seek to estimate the expression Υ, this requiring us to obtain an upper bound for h. We begin with a proof that $\tilde{v}_n(\mathbf{m}) \geqslant k(1-2/l)$ for $1 \leqslant n \leqslant R$. Note first that, since we assume k to be sufficiently large and $l = \lceil k^{1/3} \rceil$, one finds from (11.4) that

$$\tilde{u}_1 = r\tilde{b}_0/(\tilde{a}_0 + \tilde{b}_0) = (k-l)/(1+1/l) > k - 2k/l + 1.$$

Meanwhile, when $n \geqslant 1$, the condition

$$m_n \leqslant \tilde{v}_n \leqslant \tilde{u}_n = r\tilde{b}_{n-1}/(\tilde{a}_{n-1} + \tilde{b}_{n-1})$$

that follows from (11.4) ensures that

$$\tilde{b}_n = k\tilde{b}_{n-1} - m_n(\tilde{a}_{n-1} + \tilde{b}_{n-1}) \geqslant (k-r)\tilde{b}_{n-1} = l\tilde{b}_{n-1},$$

whence

$$\tilde{u}_{n+1} = r\tilde{b}_n/(\tilde{a}_n + \tilde{b}_n) = r/(1 + \tilde{b}_{n-1}/\tilde{b}_n) \geqslant r/(1+1/l) > k - 2k/l + 1.$$

We therefore deduce that $\tilde{v}_n \geqslant k(1-2/l)$ for $n \geqslant 1$, as we had claimed. It follows, in particular, that

$$h = k - l - v \leqslant k - l - k(1-2/l) \leqslant 2k/l \leqslant 2k^{2/3}.$$

We use this opportunity also to recall the bounds $s \geqslant \frac{1}{2}k(k+1) - 4k$ and $l \leqslant k^{1/3} + 1$.

Before exploiting the crude bound for h just obtained, we make use of the more opaque though stronger bound

$$h = r - \lfloor r\tilde{b}_n/(\tilde{a}_n + \tilde{b}_n) \rfloor \leqslant r\tilde{a}_n/(\tilde{a}_n + \tilde{b}_n) + 1.$$

On substituting these bounds into (11.18), we see that

$$\begin{aligned} \Upsilon &\leqslant (l + \tfrac{1}{2}(h+1))r\tilde{a}_n + (l + \tfrac{1}{2}(h+1))(\tilde{a}_n + \tilde{b}_n) + 9k^{1/3}\tilde{b}_n \\ &\leqslant 2k^{5/3}\tilde{a}_n + 2k^{2/3}\tilde{b}_n. \end{aligned}$$

Finally, we observe that

$$\widetilde{\Delta} \leqslant \sum_{m=1}^{k-4} \frac{m(k-3-m)}{s-k+4} \leqslant \frac{(k-2)(k-3)(k-4)/6}{k(k+1)/2 - 5k + 4} < \frac{1}{3}k + 1.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

By combining these estimates with (11.17), we arrive at the relation

$$\begin{aligned} s\sum_{m_{n+1}=0}^{\tilde{v}_{n+1}-1}\phi_{m_{n+1}}\tilde{b}_{n+1}(\mathbf{m}) &\geqslant \Big(\frac{1}{2}k(k+1)-\frac{1}{3}k-3k^{2/3}\Big)\tilde{b}_n(\mathbf{m})\\ &\quad -\Big(\frac{1}{2}k(k-1)+3k^{5/3}\Big)\tilde{a}_n(\mathbf{m})\\ &= \mathfrak{a}\tilde{b}_n(\mathbf{m})-\mathfrak{b}\tilde{a}_n(\mathbf{m}). \end{aligned}$$

Then we deduce from (11.13) that

$$sB_{n+1}\geqslant \mathfrak{a}B_n-\mathfrak{b}A_n \quad (n\geqslant 1). \tag{11.19}$$

On the other hand, we have

$$\begin{aligned} s\sum_{m_{n+1}=0}^{\tilde{v}_{n+1}-1}\phi_{m_{n+1}}\tilde{a}_{n+1}(\mathbf{m}) &= s\tilde{b}_n(\mathbf{m})\sum_{m=0}^{\tilde{v}_{n+1}-1}\phi_m\\ &= \tilde{b}_n(\mathbf{m})\frac{\tilde{v}_{n+1}(s-r)}{s-\tilde{v}_{n+1}}\leqslant r\tilde{b}_n(\mathbf{m}), \end{aligned}$$

whence

$$sA_{n+1}\leqslant rB_n \quad (n\geqslant 1). \tag{11.20}$$

By combining (11.19) and (11.20), we conclude at this point that

$$s^2B_{n+2}\geqslant s\mathfrak{a}B_{n+1}-r\mathfrak{b}B_n \quad (n\geqslant 1). \tag{11.21}$$

In addition, we have the initial data

$$sB_1\geqslant \mathfrak{a}\tilde{b}_0-\mathfrak{b}\tilde{a}_0=\mathfrak{a}-\mathfrak{b}/l \quad \text{and} \quad sA_1\leqslant r\tilde{b}_0=r$$

and hence

$$s^2B_2\geqslant s\mathfrak{a}B_1-s\mathfrak{b}A_1\geqslant \mathfrak{a}(\mathfrak{a}-\mathfrak{b}/l)-\mathfrak{b}r.$$

Our goal is now to extract from the recurrence inequality (11.21) a lower bound for B_n. Were we to be presented with an equation, this would be straightforward, but in present circumstances we must work less directly by relating B_n to $\tilde{B}_n$. By reference to (11.11), we see that $\tilde{B}_n$ satisfies a recurrence equation related to the inequality (11.19).

Our first observation is that the recurrence formula (11.11) has a solution of the shape

$$s^n\tilde{B}_n=\sigma_+\theta_+^n+\sigma_-\theta_-^n \quad (n\geqslant 1),$$

where

$$\sigma_+\theta_++\sigma_-\theta_-=s\tilde{B}_1=\mathfrak{a}-\mathfrak{b}/l$$

and

$$\sigma_+\theta_+^2+\sigma_-\theta_-^2=s^2\tilde{B}_2=\mathfrak{a}(\mathfrak{a}-\mathfrak{b}/l)-\mathfrak{b}r.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Then we deduce that

$$s^n \tilde{B}_n = \frac{\theta_+^{n+1} - \theta_-^{n+1}}{\theta_+ - \theta_-} - \frac{\theta_+\theta_-}{lr}\left(\frac{\theta_+^n - \theta_-^n}{\theta_+ - \theta_-}\right). \tag{11.22}$$

Note that since k is large, it follows from (11.9) and (11.12) that

$$\begin{aligned} \theta_+ &= \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 3k^{2/3} - \mathfrak{b}r/\mathfrak{a} + O((\mathfrak{b}r)^2/\mathfrak{a}^3) \\ &\geqslant \tfrac{1}{2}k(k-1) - \tfrac{1}{3}k - 7k^{2/3} \end{aligned} \tag{11.23}$$

and

$$\theta_- \leqslant \mathfrak{b}r/\mathfrak{a} + O((\mathfrak{b}r)^2/\mathfrak{a}^3) \leqslant k + 7k^{2/3}.$$

Thus, in particular, we deduce from (11.22) that $\tilde{B}_n$ is positive for every natural number n.

We now reinterpret the recurrence inequality (11.21) as a recurrence equation with variable shifts. Let (g_n) be a sequence of positive real numbers. Then, for an appropriate choice of this sequence (g_n), the recurrence sequence B_n may be interpreted as the solution of the new recurrence sequence

$$s^2 B_{n+2} = s\mathfrak{a}B_{n+1} - r\mathfrak{b}B_n + g_n \quad (n \geqslant 1), \tag{11.24}$$

with the initial data

$$sB_1 = \mathfrak{a} - \mathfrak{b}/l + g_1 \quad \text{and} \quad s^2 B_2 = \mathfrak{a}(\mathfrak{a} - \mathfrak{b}/l + g_1) - \mathfrak{b}r + g_2. \tag{11.25}$$

Define the real numbers $\tilde{g}_n$ by means of the relation

$$\tilde{g}_n = s^n(B_n - \tilde{B}_n). \tag{11.26}$$

Thus, in particular, it follows from (11.10) and (11.25) that

$$\tilde{g}_1 = g_1 \quad \text{and} \quad \tilde{g}_2 = \mathfrak{a}g_1 + g_2 \tag{11.27}$$

and from (11.11) and (11.24) that

$$\tilde{g}_{n+2} = \mathfrak{a}\tilde{g}_{n+1} - r\mathfrak{b}\tilde{g}_n + g_n \quad (n \geqslant 1). \tag{11.28}$$

We claim that $\tilde{g}_n \geqslant 0$, whence also $B_n \geqslant \tilde{B}_n$, for each natural number n.

In order to verify the last claim, we prove by induction that for each natural number n, one has

$$\tilde{g}_{n+1} \geqslant s\tilde{g}_n\tilde{B}_{n+1}/\tilde{B}_n. \tag{11.29}$$

We first confirm this inductive hypothesis for $n = 1$. Here we note that when $\tilde{g}_1 = g_1 = 0$, then the trivial lower bound $\tilde{g}_2 = g_2 \geqslant 0$ that follows from (11.27) suffices to confirm (11.29). When $g_1 \neq 0$, meanwhile, we find from (11.10) and (11.27) that

$$\tilde{g}_2 = \tilde{g}_1\left(\frac{\mathfrak{a}g_1 + g_2}{g_1}\right) = \tilde{g}_1(\mathfrak{a} + g_2/g_1).$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

The positivity of g_1, g_2 and

$$\mathfrak{a} - \mathfrak{b}/l = \tfrac{1}{2}k(k+1) + O(k^{5/3})$$

consequently ensures that

$$\tilde{g}_2 \geqslant \tilde{g}_1\mathfrak{a} \geqslant \tilde{g}_1\left(\frac{\mathfrak{a}(\mathfrak{a} - \mathfrak{b}/l) - \mathfrak{b}r}{\mathfrak{a} - \mathfrak{b}/l}\right) = s\tilde{g}_1\tilde{B}_2/\tilde{B}_1.$$

This confirms the inductive hypothesis when $n = 1$.

Suppose next that $n \geqslant 2$ and

$$\tilde{g}_n \geqslant s\tilde{g}_{n-1}\tilde{B}_n/\tilde{B}_{n-1}.$$

Then, on making use of (11.11) and (11.28), one deduces that

$$\begin{aligned}\tilde{g}_{n+1} - s\tilde{g}_n\tilde{B}_{n+1}/\tilde{B}_n &= (\mathfrak{a}\tilde{g}_n - r\mathfrak{b}\tilde{g}_{n-1} + g_{n-1}) - \tilde{g}_n(\mathfrak{a}\tilde{B}_n - s^{-1}r\mathfrak{b}\tilde{B}_{n-1})/\tilde{B}_n \\ &\geqslant (s^{-1}r\mathfrak{b}\tilde{B}_{n-1}/\tilde{B}_n)(\tilde{g}_n - s\tilde{g}_{n-1}\tilde{B}_n/\tilde{B}_{n-1}) \geqslant 0.\end{aligned}$$

This confirms the inductive hypothesis with $n+1$ in place of n, and so by applying induction we deduce that (11.29) holds for every natural number n. A particular consequence of the lower bound (11.29) is that $\tilde{g}_n \geqslant 0$ for every natural number n. Finally, we conclude from (11.26) that $B_n \geqslant \tilde{B}_n$ for every natural number n.

In order to complete the proof of the lemma, we note first from (11.5) and (11.8) that $s_0^R = s^R B_R$. Since $B_R \geqslant \tilde{B}_R$, the final conclusion of the lemma follows from (11.22). □

We next turn to the problem of controlling the behaviour of a_R and b_R.

LEMMA 11.6. *Suppose that the tuples* $\mathbf{m}$ *and* $\mathbf{h}(\mathbf{m})$ *satisfy the conditions*

$$1 \leqslant m_n \leqslant \tilde{u}_n(\mathbf{m}) - 1 \quad \textit{and} \quad 0 \leqslant h_n(\mathbf{m}) \leqslant 15k^R b \quad (1 \leqslant n \leqslant R).$$

Then one has

$$k_{\mathbf{m}}b \leqslant b_R(\mathbf{m}; \mathbf{h}) \leqslant k_{\mathbf{m}}b + 16k^{2R}b$$

and furthermore

$$a_R(\mathbf{m}; \mathbf{h}) \leqslant b_R(\mathbf{m}; \mathbf{h})/l.$$

Proof. We again make use of auxiliary recurrence sequences in order to disentangle information on recurrence inequalities. Write

$$h_1^*(\mathbf{m}) = h_1(\mathbf{m}) + m_1(b/l - a_0)$$

and

$$h_n^*(\mathbf{m}) = h_n(\mathbf{m}) \quad (n > 1).$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Then we find that

$$h_1^*(\mathbf{m}) \leqslant h_1(\mathbf{m}) + m_1 \leqslant h_1(\mathbf{m}) + k < 16k^R b$$

and

$$h_n^*(\mathbf{m}) = h_n(\mathbf{m}) \leqslant 15k^R b \quad (n > 1).$$

We define the sequences $(a_n^*) = (a_n^*(\mathbf{m}; \mathbf{h}))$ and $(b_n^*) = (b_n^*(\mathbf{m}; \mathbf{h}))$ by means of the relations

$$a_0^* = b/l \quad \text{and} \quad b_0^* = b,$$

and

$$a_n^* = b_{n-1}^* \quad \text{and} \quad b_n^* = (k - m_n)b_{n-1}^* - m_n a_{n-1}^* + h_n^*(\mathbf{m}) \quad (1 \leqslant n \leqslant R).$$

It follows that $a_n = a_n^*$ and $b_n = b_n^*$ for $n \geqslant 1$. We next put

$$g_n^* = b_n^* - \tilde{b}_n b \quad (n \geqslant 0) \tag{11.30}$$

and we seek to show in the first instance that $g_n^* \geqslant 0$ for each n. This of course implies in particular that $b_R^* \geqslant \tilde{b}_R b = k_{\mathbf{m}} b$.

We prove that $g_n^* \geqslant 0$ for each n by induction. Observe first that by applying (11.30) in combination with the recurrence relations for $\tilde{a}_n$, $\tilde{b}_n$, a_n^*, b_n^*, we obtain

$$\begin{aligned} g_0^*\tilde{b}_1 - \tilde{b}_0 g_1^* = {} & (b_0^* - \tilde{b}_0 b)((k - m_1)\tilde{b}_0 - m_1\tilde{a}_0) \\ & - \tilde{b}_0((k - m_1)(b_0^* - \tilde{b}_0 b) - m_1(a_0^* - \tilde{a}_0 b) + h_1^*), \end{aligned}$$

whence $g_0^*\tilde{b}_1 - \tilde{b}_0 g_1^* = -h_1^* \leqslant 0$. Moreover, if we assume that

$$g_{n-1}^*\tilde{b}_n - \tilde{b}_{n-1} g_n^* \leqslant 0, \tag{11.31}$$

then we find in like manner that

$$\begin{aligned} g_n^*\tilde{b}_{n+1} - \tilde{b}_n g_{n+1}^* = {} & (b_n^* - \tilde{b}_n b)((k - m_{n+1})\tilde{b}_n - m_{n+1}\tilde{a}_n) \\ & - \tilde{b}_n((k - m_{n+1})(b_n^* - \tilde{b}_n b) - m_{n+1}(a_n^* - \tilde{a}_n b) + h_{n+1}^*). \end{aligned}$$

Thus, we obtain the bound

$$\begin{aligned} g_n^*\tilde{b}_{n+1} - \tilde{b}_n g_{n+1}^* &\leqslant m_{n+1}(a_n^*\tilde{b}_n - b_n^*\tilde{a}_n) \\ &= m_{n+1}((g_{n-1}^* + \tilde{b}_{n-1} b)\tilde{b}_n - (g_n^* + \tilde{b}_n b)\tilde{b}_{n-1}) \\ &= m_{n+1}(g_{n-1}^*\tilde{b}_n - g_n^*\tilde{b}_{n-1}). \end{aligned}$$

We thus conclude from (11.31) that $g_n^*\tilde{b}_{n+1} - \tilde{b}_n g_{n+1}^* \leqslant 0$, thereby confirming the inductive hypothesis (11.31) with $n + 1$ in place of n. We therefore deduce by induction that $g_{n-1}^*\tilde{b}_n \leqslant \tilde{b}_{n-1} g_n^*$ for every n, whence

$$g_n^* \geqslant g_{n-1}^*\tilde{b}_n/\tilde{b}_{n-1} \geqslant 0 \quad (n \geqslant 1). \tag{11.32}$$

In this way, we therefore conclude that $b_R = b_R^* \geqslant \tilde{b}_R b = k_{\mathbf{m}} b$, as desired.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Having confirmed the lower bound on $b_R(\mathbf{m};\mathbf{h})$ claimed in the statement of the lemma, we turn our attention next to the upper bound. Observe that the recurrence relations for $\tilde{a}_n$, $\tilde{b}_n$, a_n^*, b_n^* lead us from (11.30) to the relations

$$\begin{aligned} g_1^* &= (k-m_1)(b_0^*-\tilde{b}_0 b)-m_1(a_0^*-\tilde{a}_0 b)+h_1^*(\mathbf{m}) \\ &= h_1^*(\mathbf{m}) \leqslant 15k^R b \end{aligned}$$

and

$$g_n^* = (k-m_n)g_{n-1}^* - m_n g_{n-2}^* + h_n^*(\mathbf{m}) \quad (n \geqslant 2).$$

In particular, we have the trivial upper bound

$$g_n^* \leqslant k g_{n-1}^* + 15k^R b \quad (n \geqslant 2)$$

and so we deduce by induction that

$$g_n^* \leqslant 15k^R b(1+k+\cdots+k^{n-1}) \leqslant 16k^{R+n}b.$$

Hence, on recalling (11.30) once again, we obtain the bound

$$b_R^* \leqslant \tilde{b}_R b + 16k^{2R}b = k_{\mathbf{m}} b + 16k^{2R}b.$$

Collecting together the conclusions of the last two paragraphs, we find that

$$k_{\mathbf{m}} b \leqslant b_R(\mathbf{m};\mathbf{h}) \leqslant k_{\mathbf{m}} b + 16k^{2R}b,$$

thereby confirming the first assertion of the lemma. It remains now only to bound a_R in terms of b_R. To this end, we observe that for each $n \geqslant 0$, it follows from (11.4) and our hypothesis $m_{n+1} \leqslant \tilde{u}_n(\mathbf{m}) - 1$ that $m_{n+1} \leqslant r\tilde{b}_n/(\tilde{a}_n + \tilde{b}_n)$ and hence

$$\tilde{b}_{n+1} = (k-m_{n+1})\tilde{b}_n - m_{n+1}\tilde{a}_n \geqslant (k-r)\tilde{b}_n = l\tilde{b}_n.$$

We therefore deduce from (11.32) that $g_{n+1}^* \geqslant l g_n^*$ for $n \geqslant 0$. Consequently, recalling again the relation (11.30), we see that

$$b_R = b_R^* = \tilde{b}_R b + g_R^* \geqslant l(\tilde{b}_{R-1}b + g_{R-1}^*) = l b_{R-1}^* = l a_R.$$

We have therefore shown that $a_R \leqslant b_R/l$, as desired. This completes the proof of the lemma. □

Before initiating our discussion of the next lemma, we observe that in view of (11.23) and our hypotheses concerning s, one has

$$\theta_+ + r \geqslant \tfrac{1}{2}k(k-1) - \tfrac{1}{3}k - 7k^{2/3} + (k-l) > s + r.$$

Then it follows that, provided R is sufficiently large in terms of s and k, one has $s < \theta_+$, and so we deduce from Lemma 11.5 that

$$s < s_0. \tag{11.33}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

LEMMA 11.7. *Suppose that $\Lambda \geqslant 0$, let a and b be integers with $0 \leqslant a < b \leqslant (20Rk^{2R}\theta)^{-1}$ and suppose further that $a \leqslant b/l$. Suppose in addition that there are real numbers ψ, c and γ, with*

$$0 \leqslant c \leqslant (2\delta)^{-1}\theta, \qquad \gamma \geqslant -sb \qquad \text{and} \qquad \psi \geqslant 0,$$

such that

$$X^{\Lambda}M^{\Lambda\psi} \ll X^{c\delta}M^{-\gamma}[[K_{a,b}^{r,r}(X)]]. \tag{11.34}$$

Then, for some $\mathbf{m} \in [0, r-1]^R$, there are a real number h with $0 \leqslant h \leqslant 16k^{2R}b$ and positive integers a' and b' with $a' \leqslant b'/l$, such that

$$X^{\Lambda}M^{\Lambda\psi'} \ll X^{c'\delta}M^{-\gamma'}[[K_{a',b'}^{r,r}(X)]], \tag{11.35}$$

where ψ', c', γ' and b' are real numbers satisfying the conditions

$$\psi' = \rho_{\mathbf{m}}(\psi + (\tfrac{1}{2} - r/s)b), \qquad c' = \rho_{\mathbf{m}}(c+1), \qquad \gamma' = \rho_{\mathbf{m}}\gamma, \qquad b' = k_{\mathbf{m}}b + h.$$

Moreover, the real number $k_{\mathbf{m}}$ satisfies $2^R \leqslant k_{\mathbf{m}} \leqslant k^R$.

Proof. We deduce from the postulated bound (11.34), together with Lemmas 11.3 and 11.4, that there exists a choice $\mathbf{h} = \mathbf{h}(\mathbf{m})$ of tuples, with

$$0 \leqslant h_n(\mathbf{m}) \leqslant 15k^R b \quad (1 \leqslant n \leqslant R),$$

such that

$$X^{\Lambda}M^{\Lambda\psi} \ll X^{(c+1)\delta}M^{-\gamma}(X/M^{b/2})^{\Lambda} \prod_{\mathbf{0} \leqslant \mathbf{m} \leqslant \tilde{\mathbf{u}}-1} \Theta_R(\mathbf{m}; \mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}}.$$

Consequently, one has

$$\prod_{\mathbf{0} \leqslant \mathbf{m} \leqslant \tilde{\mathbf{u}}-1} \Theta_R(\mathbf{m}; \mathbf{h})^{\phi_{m_1}\cdots\phi_{m_R}} \gg X^{-(c+1)\delta}M^{\Lambda(\psi+b/2)+\gamma}.$$

Note that from (7.1) one has

$$\sum_{m=0}^{v-1} \phi_m = \frac{v(s-r)}{s(s-v)} \leqslant \frac{r}{s},$$

so that

$$\sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_R=0}^{\tilde{v}_R-1} \phi_{m_1}\cdots\phi_{m_R} \leqslant (r/s)^R \leqslant r/s.$$

Then we deduce from the definition (11.3) of $\Theta_n(\mathbf{m}; \mathbf{h})$ that

$$\prod_{\mathbf{0} \leqslant \mathbf{m} \leqslant \tilde{\mathbf{u}}-1} (X^{-\Lambda}[[K_{a_R,b_R}^{r,r}(X)]] + M^{-3sk^R b})^{\phi_{m_1}\cdots\phi_{m_R}} \gg X^{-(c+1)\delta}M^{\Lambda(\psi+(1/2-r/s)b)+\gamma}. \tag{11.36}$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

Put

$$\Omega = B_R = \sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_R=0}^{\tilde{v}_R-1} \beta_{\mathbf{m}}^{(R)} \tilde{b}_R(\mathbf{m}), \tag{11.37}$$

so that in view of Lemma 11.5 one has $\Omega \geqslant \tilde{B}_R$. Then an application of Lemma 8.1 to (11.36) yields the relation

$$\sum_{m_1=0}^{\tilde{v}_1-1} \cdots \sum_{m_R=0}^{\tilde{v}_R-1} (X^{-\Lambda}[[K^{r,r}_{a_R,b_R}(X)]] + M^{-3sk^Rb})^{\Omega/\tilde{b}_R(\mathbf{m})} \gg X^{-(c+1)\delta} M^{\Lambda(\psi+(1/2-r/s)b)+\gamma}.$$

We see from (11.5) and (11.37) that $\Omega = (s_0/s)^R$, and so it follows from (11.6) that $\Omega/\tilde{b}_R(\mathbf{m}) = 1/\rho_{\mathbf{m}}$. Thus, we conclude that for some R-tuple $\mathbf{m}$, one has

$$\begin{aligned} X^{-\Lambda}[[K^{r,r}_{a_R,b_R}(X)]] + M^{-3sk^Rb} &\gg X^{-\rho_{\mathbf{m}}(c+1)\delta} M^{\Lambda\rho_{\mathbf{m}}(\psi+(1/2-r/s)b)+\rho_{\mathbf{m}}\gamma} \\ &\gg X^{-c'\delta} M^{\Lambda\psi'+\gamma'}. \end{aligned} \tag{11.38}$$

We must again handle the removal of the term M^{-3sk^Rb} on the left-hand side of (11.38). We note that, just as in the concluding paragraph of the proof of Lemma 11.6, one has $\tilde{b}_{n+1} \geqslant l\tilde{b}_n$ $(n \geqslant 0)$ and hence $\tilde{b}_n(\mathbf{m}) \geqslant 0$. Hence, a direct induction leads from (8.3) to the upper bound $\tilde{b}_R(\mathbf{m}) \leqslant k^R$, and we find by means of (11.6) and (11.33) that

$$\rho_{\mathbf{m}} = \tilde{b}_R(\mathbf{m})(s/s_0)^R < \tilde{b}_R(\mathbf{m}) \leqslant k^R.$$

We may therefore follow the analysis leading to (8.16), *mutatis mutandis*, to conclude as before that

$$X^{-\Lambda}[[K^{r,r}_{a_R,b_R}(X)]] \gg X^{-c'\delta} M^{\Lambda\psi'+\gamma'}.$$

We find from Lemma 11.6 that one has $a_R \leqslant b_R/l$, and that

$$k_{\mathbf{m}}b \leqslant b_R \leqslant k_{\mathbf{m}}b + 16k^{2R}b.$$

Then we conclude that there exist integers $b' = b_R$, $a' = a_R$ and h satisfying the conditions

$$0 \leqslant h \leqslant 16k^{2R}b, \qquad b' = k_{\mathbf{m}}b + h \qquad \text{and} \qquad a' \leqslant b'/l,$$

for which

$$X^{-\Lambda}[[K^{r,r}_{a',b'}(X)]] \gg X^{-c'\delta} M^{\Lambda\psi'+\gamma'}.$$

The desired conclusion (11.35) follows at once, together with its associated conditions.

The only task that remains is to confirm the bounds $2^R \leqslant k_{\mathbf{m}} \leqslant k^R$. On the one hand, just as in the proof of Lemma 11.6, one has $\tilde{b}_{n+1} \geqslant l\tilde{b}_n$ for each $n \geqslant 0$. Then an inductive argument confirms that $k_{\mathbf{m}} = \tilde{b}_R \geqslant l^R\tilde{b}_0 \geqslant 2^R$. On the other hand, we have already shown that $\tilde{b}_R \leqslant k^R$ and thus $k_{\mathbf{m}} = \tilde{b}_R \leqslant k^R$. This completes the proof of the lemma. □

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We now employ the conclusion of the last lemma to bound $J_{s+r}(X)$.

THEOREM 11.8. *Suppose that s, k and r are natural numbers with k sufficiently large, $r = k - \lceil k^{1/3} \rceil$ and $1 \leqslant s \leqslant s_1$, where*

$$s_1 = \frac{1}{2}\Big(\frac{1}{2}k(k+1) - \frac{1}{3}k - 3k^{2/3}\Big) \times \Big(1 + \sqrt{1 - \frac{4r(k(k-1)/2 + 3k^{5/3})}{(k(k+1)/2 - k/3 - 3k^{2/3})^2}}\Big).$$

Then, for each $\varepsilon > 0$, one has $J_{s+r}(X) \ll X^{s+r+\varepsilon}$.

Proof. Defining s_0 via (11.5) as in the preamble to Lemma 11.4, one finds that there are no serious modifications required in order to apply the argument of the proof of Theorem 2.1 to pass from Lemma 11.7 to the conclusion of the theorem, but with s_0 in place of $s_1 = \theta_+$. The argument leading to (11.33) shows, however, that whenever $s < s_1$, one has also that $s < s_0$. The conclusion of the theorem is now immediate. □

In order to establish Theorem 1.3, we have only to note that, on recalling (11.23), one finds that

$$\begin{aligned} s_1 + r = \theta_+ + k - l &\geqslant \tfrac{1}{2}k(k-1) - \tfrac{1}{3}k - 7k^{2/3} + (k - k^{1/3}) \\ &\geqslant \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3}. \end{aligned}$$

Thus, whenever

$$1 \leqslant s \leqslant \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3},$$

one has $J_{s,k}(X) \ll X^{s+\varepsilon}$.

§12. *Some consequences of Theorem 1.3.* We finish this paper by turning our attention to a few consequences of the asymptotically sharpest of our conclusions, namely Theorem 1.3. We begin by proving Theorem 1.5. Suppose that k is a sufficiently large natural number and put

$$\mathfrak{s} = \lfloor \tfrac{1}{2}k(k+1) - \tfrac{1}{3}k - 8k^{2/3} \rfloor.$$

In addition, take $s = \frac{1}{2}k(k+1)$ and put $\Delta = s - \mathfrak{s}$. Then we find that

$$\Delta \leqslant \tfrac{1}{3}k + 8k^{2/3} + 1. \tag{12.1}$$

Consequently, on making use of the trivial estimate $f_k(\boldsymbol{\alpha}; X) = O(X)$, we deduce from (2.1) in combination with Theorem 1.3 that

$$\begin{aligned} J_{s,k}(X) = \oint |f_k(\boldsymbol{\alpha}; X)|^{2\mathfrak{s}+2\Delta}\, d\boldsymbol{\alpha} &\ll X^{2\Delta} \oint |f_k(\boldsymbol{\alpha}; X)|^{2\mathfrak{s}}\, d\boldsymbol{\alpha} \\ &\ll X^{2\Delta} J_{\mathfrak{s},k}(X) \ll X^{\mathfrak{s}+2\Delta+\varepsilon} \ll X^{s+\Delta+\varepsilon}. \end{aligned}$$

The conclusion of Theorem 1.5 is now immediate.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

We next point out an application of Theorem 1.3 to Tarry's problem. Recall the definition of the natural number $W(k,h)$ associated with the system of equations (1.5).

THEOREM 12.1. *When h and k are natural numbers with $h \geqslant 2$ and k sufficiently large, one has $W(k,h) \leqslant \frac{1}{2}k(k+1)+1$.*

Proof. The argument of the proof of [**15**, Theorem 1.3] shows that $W(k,h) \leqslant s$ whenever one can establish the estimate

$$J_{s,k+1}(X) = o(X^{2s-k(k+1)/2}).$$

But, as a consequence of Theorem 1.3, when k is sufficiently large and

$$1 \leqslant s \leqslant \tfrac{1}{2}(k+1)(k+2) - \tfrac{1}{3}(k+1) - 8(k+1)^{2/3}, \tag{12.2}$$

one has $J_{s,k+1}(X) \ll X^{s+\varepsilon}$. Observe, however, that $X^{s+\varepsilon} = o(X^{2s-k(k+1)/2})$ provided only that $s < 2s - \frac{1}{2}k(k+1)$, which is to say that $s \geqslant \frac{1}{2}k(k+1)+1$. Moreover, when k is sufficiently large, one finds that the value $s = \frac{1}{2}k(k+1)+1$ satisfies the condition (12.2) and thus we have $W(k,h) \leqslant \frac{1}{2}k(k+1)+1$. This completes the proof of the theorem. □

The problem of estimating $W(k,h)$ has been investigated extensively by Wright and Hua (see [**6**], [**7**] and [**21**]). Hua was able to show that $W(k,h) \leqslant k^2(\log k + O(1))$. This bound was improved in [**15**, Theorem 1.3] by means of the efficient congruencing method, delivering the upper bound $W(k,h) \leqslant k^2+k-2$. In our most recent work on multigrade efficient congruencing, this bound was further improved in [**19**, Theorem 12.1] to obtain $W(k,h) \leqslant \frac{5}{8}(k+1)^2$ for $k \geqslant 3$. The bound recorded in Theorem 12.1 above achieves the limit of the methods currently employed in which an elementary application of Vinogradov's mean value theorem is applied, as described in [**14**] and enhanced in [**19**, §12]. As far as the author is aware, there is no lower bound available on $W(k,h)$ superior to $W(k,h) \geqslant k+1$. There consequently remains a substantial gap between our upper and lower bounds in Tarry's problem.

Finally, we explore the consequences of Theorem 1.3 in the context of Waring's problem. When s and k are natural numbers, let $R_{s,k}(n)$ denote the number of representations of the natural number n as the sum of s kth powers of positive integers. A formal application of the circle method suggests that for $k \geqslant 3$ and $s \geqslant k+1$, one should have

$$R_{s,k}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)}\mathfrak{S}_{s,k}(n)n^{s/k-1} + o(n^{s/k-1}), \tag{12.3}$$

where

$$\mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}\Big(q^{-1}\sum_{r=1}^{q}e(ar^k/q)\Big)^s e(-na/q).$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

With suitable congruence conditions imposed on n, one has $1 \ll \mathfrak{S}_{s,k}(n) \ll n^{\varepsilon}$, so that the conjectured relation (12.3) constitutes an honest asymptotic formula. Let $\widetilde{G}(k)$ denote the least integer t with the property that, for all $s \geqslant t$, and all sufficiently large natural numbers n, one has the asymptotic formula (12.3). By combining the conclusion of Theorem 1.3 with our recent work concerning the asymptotic formula in Waring's problem [**16**], and the enhancement [**4**, Theorem 8.5] of Ford's work [**3**], we are able to derive new upper bounds for $\widetilde{G}(k)$ when k is sufficiently large.

THEOREM 12.2. *Let ξ denote the real root of the polynomial $6\xi^3 + 3\xi^2 - 1$ and put $C = (5 + 6\xi - 3\xi^2)/(2 + 6\xi)$, so that*

$$\xi = 0.424\,574\ldots \quad \text{and} \quad C = 1.540\,789\ldots.$$

Then, for large values of k, one has $\widetilde{G}(k) < Ck^2 + O(k^{5/3})$.

For comparison, in [**19**, Theorem 1.3], we derived an analogous bound in which C is replaced by the slightly larger number $1.542\,749\ldots$.

The Proof of Theorem 12.2. In general, we write $\Delta_{s,k}$ for the least real number with the property that, for all $\varepsilon > 0$, one has

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

Then it follows from [**19**, Lemma 10.7] that one has $\widetilde{G}(k) \leqslant \lfloor u_1(k) \rfloor + 1$, where

$$u_1(k) = \min_{\substack{1 \leqslant t \leqslant k^2-k+1 \\ \Delta_{t,k} < 1}} \min_{1 \leqslant w \leqslant k-1} \min_{v \geqslant 1} u_0(k, t, v, w)$$
$$2v + w(w-1) < 2t$$

and

$$u_0(k, t, v, w) = 2t - \frac{(1 - \Delta_{t,k})(2t - 2v - w(w-1))}{1 - \Delta_{t,k} + \Delta_{v,k}/w}.$$

Suppose that k is a large natural number and let β be a positive parameter to be determined in due course. We take

$$w = \lfloor \beta k \rfloor \quad \text{and} \quad v = \tfrac{1}{2}k(k+1).$$

Then it follows from Theorem 1.3, just as in the discussion leading to (12.1), that the exponent $\Delta_{v,k}$ is permissible, where

$$\Delta_{v,k} \leqslant \tfrac{1}{3}k + 8k^{2/3} + 1.$$

Also, by taking $t = k^2 - k + 1$, one sees from [**19**, Corollary 1.2] that $\Delta_{t,k} = 0$. Then we deduce that

$$u_1(k) \leqslant 2(k^2 - k + 1) - \frac{2k^2 - k(k+1) - (\beta k)^2 + O(k)}{1 + k/(3\beta k) + O(k^{-1/3})}.$$

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

It follows that

$$u_1(k)/(2k^2) \leqslant 1 - \frac{\beta(1-\beta^2)/2}{\beta + 1/3} + O(k^{-1/3})$$
$$= \frac{3\beta^3 + 3\beta + 2}{6\beta + 2} + O(k^{-1/3}).$$

A modest computation confirms that the optimal choice for the parameter β is ξ, where ξ is the real root of the polynomial equation $6\xi^3 + 3\xi^2 - 1 = 0$. With this choice for β, one finds that

$$u_1(k) \leqslant \left(\frac{5 + 6\xi - 3\xi^2}{2 + 6\xi}\right)k^2 + O(k^{5/3}).$$

The conclusion of Theorem 12.2 is now immediate. □

References

1. G. I. Arkhipov, V. N. Chubarikov and A. A. Karatsuba, *Trigonometric Sums in Number Theory and Analysis* (*de Gruyter Expositions in Mathematics* **39**), Walter de Gruyter (Berlin, 2004).
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), 633–682.
3. K. B. Ford, New estimates for mean values of Weyl sums. *Int. Math. Res. Not. IMRN* **1995**(3) (1995), 155–171.
4. K. B. Ford and T. D. Wooley, On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing. *Acta Math.* **213**(2) (2014), 199–236.
5. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edn., The Clarendon Press, Oxford University Press (Oxford, 1960).
6. L.-K. Hua, On Tarry's problem. *Q. J. Math. Oxford* **9** (1938), 315–320.
7. L.-K. Hua, Improvement of a result of Wright. *J. Lond. Math. Soc.* (2) **24** (1949), 157–159.
8. L.-K. Hua, *Additive Theory of Prime Numbers*, American Mathematical Society (Providence, RI, 1965).
9. R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge University Press (Cambridge, 1997).
10. R. C. Vaughan and T. D. Wooley, A special case of Vinogradov's mean value theorem. *Acta Arith.* **79**(3) (1997), 193–204.
11. I. M. Vinogradov, The method of trigonometrical sums in the theory of numbers. *Trav. Inst. Math. Stekloff* **23** (1947).
12. T. D. Wooley, On Vinogradov's mean value theorem. *Mathematika* **39**(2) (1992), 379–399.
13. T. D. Wooley, A note on simultaneous congruences. *J. Number Theory* **58**(2) (1996), 288–297.
14. T. D. Wooley, Some remarks on Vinogradov's mean value theorem and Tarry's problem. *Monatsh. Math.* **122**(3) (1996), 265–273.
15. T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing. *Ann. of Math.* (2) **175**(3) (2012), 1575–1627.
16. T. D. Wooley, The asymptotic formula in Waring's problem. *Int. Math. Res. Not. IMRN* **2012**(7) (2012), 1485–1504.
17. T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing, II. *Duke Math. J.* **162**(4) (2013), 673–730.
18. T. D. Wooley, Translation invariance, exponential sums, and Waring's problem. In *Proc. Int. Congr. Mathematicians (Seoul, Korea, 13–21 August 2014),* Vol. II, Kyung Moon Sa (Seoul, 2014), 505–529.
19. T. D. Wooley, Multigrade efficient congruencing and Vinogradov's mean value theorem. *Proc. Lond. Math. Soc.* (3) **111**(3) (2015), 519–560.

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press

20. T. D. Wooley, The cubic case of the main conjecture in Vinogradov's mean value theorem. *Adv. Math.* **294** (2016), 532–561.

21. E. M. Wright, The Prouhet–Lehmer problem. *J. Lond. Math. Soc.* (2) **23** (1948), 279–285.

Trevor D. Wooley,
School of Mathematics,
University of Bristol,
University Walk,
Clifton,
Bristol BS8 1TW,
U.K.
E-mail: matdw@bristol.ac.uk

https://doi.org/10.1112/S0025579316000279 Published online by Cambridge University Press