J. reine angew. Math. **638** (2010), 1—67
DOI 10.1515/CRELLE.2010.001

Journal für die reine und
angewandte Mathematik

Waring's problem in function fields

By *Yu-Ru Liu*[1] at Waterloo and *Trevor D. Wooley*[2] at Bristol

Abstract. Let $\mathbb{F}_q[t]$ denote the ring of polynomials over the finite field $\mathbb{F}_q$ of characteristic p, and write $\mathbb{J}_q^k[t]$ for the additive closure of the set of kth powers of polynomials in $\mathbb{F}_q[t]$. Define $G_q(k)$ to be the least integer s satisfying the property that every polynomial in $\mathbb{J}_q^k[t]$ of sufficiently large degree admits a strict representation as a sum of s kth powers. We employ a version of the Hardy-Littlewood method involving the use of smooth polynomials in order to establish a bound of the shape $G_q(k) \leqq Ck \log k + O(k \log\log k)$. Here, the coefficient C is equal to 1 when $k < p$, and C is given explicitly in terms of k and p when $k > p$, but in any case satisfies $C \leqq 4/3$. There are associated conclusions for the solubility of diagonal equations over $\mathbb{F}_q[t]$, and for exceptional set estimates in Waring's problem.

1. Introduction

A striking theme in arithmetic concerns the remarkable similarity between the ring of rational integers $\mathbb{Z}$ on the one hand, and the polynomial rings in a single variable $\mathbb{F}_q[t]$, defined over the finite fields $\mathbb{F}_q$ having q elements, on the other. The analogy between $\mathbb{Z}$ and $\mathbb{F}_q[t]$ is but one in a family that in general relates number fields to function fields. In at least one respect it is surprising that these rings should resemble one another so faithfully, for whereas the characteristic of $\mathbb{Z}$ is zero, that of $\mathbb{F}_q[t]$ is equal to the characteristic of $\mathbb{F}_q$, a positive (prime) number that we denote by $\mathrm{ch}(\mathbb{F}_q)$. A significant desideratum in translating conclusions from $\mathbb{Z}$ to $\mathbb{F}_q[t]$, therefore, is the derivation of results uniform in the characteristic. In this paper we investigate the analogue of Waring's problem over $\mathbb{F}_q[t]$, our aim being to establish conclusions that are relatively robust to changes in the characteristic of $\mathbb{F}_q$. We concentrate, in particular, on methods having the potential to impact questions that concern the density of rational points on algebraic varieties in function fields, a topic to which we intend to return on a future occasion.

Some preparation is required before we can announce our principal conclusions. Let k be an integer with $k \geqq 2$, let $s \in \mathbb{N}$, and consider a polynomial m in $\mathbb{F}_q[t]$. We seek to de-

[1] Research supported in part by an NSERC discovery grant. This work started during a visit of the first author to the University of Michigan, Ann Arbor, in 2004. She would like to thank the Mathematics Department at Michigan for its kind hospitality.
[2] Research supported in part by NSF grant DMS-0601367.

termine the circumstances in which m admits a representation

$$m = x_1^k + x_2^k + \cdots + x_s^k, \tag{1.1}$$

with $x_i \in \mathbb{F}_q[t]$ $(1 \leqq i \leqq s)$. It is possible that a representation of the shape (1.1) is obstructed for every natural number s. For example, if the characteristic p of $\mathbb{F}_q$ divides k, then $x_1^k + \cdots + x_s^k = (x_1^{k/p} + \cdots + x_s^{k/p})^p$, and thus m necessarily fails to admit a representation of the shape (1.1) whenever $m \notin \mathbb{F}_q[t^p]$, no matter how large s may be. In order to accomodate this and other intrinsic obstructions, we define $\mathbb{J}_q^k[t]$ to be the additive closure of the set of kth powers of polynomials in $\mathbb{F}_q[t]$, and we restrict attention to those m lying in the subring $\mathbb{J}_q^k[t]$ of $\mathbb{F}_q[t]$. It is convenient also to define $\mathbb{J}_q^k$ to be the additive closure of the set of kth powers of elements of $\mathbb{F}_q$.

As is the case for the rational integers $\mathbb{Z}$, two variants of Waring's problem over $\mathbb{F}_q[t]$ demand attention. In the first (*unrestricted*) variant, one seeks to establish the existence of a number s_0 with the property that, whenever $m \in \mathbb{J}_q^k[t]$ and $s \geqq s_0$, then the equation (1.1) is soluble with $x_i \in \mathbb{F}_q[t]$ $(1 \leqq i \leqq s)$. Should such a number s_0 exist, we define $v_q(k)$ to be the least permissible choice for s_0. The problem of establishing the existence of $v_q(k)$ was addressed first by Paley [17] in 1933. A feature of Paley's approach to this problem, in common with the strategies of subsequent authors, is that a representation is sought first for the polynomial t, and from this representation all others follow by substitution. In order to achieve success with such a strategy, one must clearly engineer extensive cancellation amongst monomials t^n of large degree, and indeed the degree of the kth powers of polynomials x_i^k utilised in such a representation (1.1) must usually be at least k times as large as the degree of the polynomial to be represented. This unrestricted variant therefore resembles not the classical version of Waring's problem, but rather the "easier" Waring problem in which the kth powers of integers x^k are replaced by $\pm x^k$ (see [11], §21.7, for example). Methods currently employed in the analysis of the unrestricted variant of Waring's problem over $\mathbb{F}_q[t]$ are apparently of little use in the investigation of the density of rational points on algebraic varieties. Thus, although we will have more to say about this unrestricted problem elsewhere, our focus in this paper is on the analogous *restricted* variant of Waring's problem.

Further discussion requires a formal definition. When $m \in \mathbb{F}_q[t]$, write $\operatorname{ord} m$ for the degree of m. We say that m is an *exceptional element* of $\mathbb{J}_q^k[t]$ when its leading coefficient lies in $\mathbb{F}_q \backslash \mathbb{J}_q^k$, and in addition k divides $\operatorname{ord} m$. The strongest constraint on the degrees of the variables that might still permit the existence of a representation of the shape (1.1) is plainly $\operatorname{ord} x_i \leqq \lceil (\operatorname{ord} m)/k \rceil$ $(1 \leqq i \leqq s)$. When $\operatorname{ch}(\mathbb{F}_q) < k$, however, it is possible that $\mathbb{J}_q^k$ is not equal to $\mathbb{F}_q$, and then the leading coefficient of m need not be an element of $\mathbb{J}_q^k$. If k divides $\operatorname{ord} m$, so that m is an exceptional polynomial, such circumstances obstruct the existence of a representation (1.1) of m with the variables x_i satisfying the above constraint on their degrees[3]. Motivated by these observations, given $k \in \mathbb{N}$ with $k \geqq 2$, we define $P = P_k(m)$ by setting $P = \lceil (\operatorname{ord} m)/k \rceil$ when m is not exceptional, and when m is exceptional we define $P = (\operatorname{ord} m)/k + 1$. Notice, in particular, that when m is not exceptional, then P is the unique integer satisfying $k(P-1) < \operatorname{ord} m \leqq kP$. We say that m

[3] We are grateful to an individual involved in the refereeing process for raising this issue. By applying familiar estimates of Weil, one may show that such exceptional polynomials are absent whenever $q > (k-1)^2$.

admits a *strict representation* as a sum of s kth powers when for some $x_i \in \mathbb{F}_q[t]$ with $\operatorname{ord} x_i \leqq P_k(m)$ $(1 \leqq i \leqq s)$, the equation (1.1) is satisfied. We now introduce an analogue for this *strict polynomial Waring problem* of the function $G(k)$ familiar from the classical theory. When k and q are natural numbers exceeding 1, define $G_q(k)$ to be the least integer s_1 satisfying the property that, whenever $s \geqq s_1$ and $m \in \mathbb{J}_q^k[t]$ has degree sufficiently large in terms of k, s and q, then m admits a strict representation of the shape (1.1). The primary goal of this paper is the proof of the uniform upper bound for $G_q(k)$ provided in Theorem 1.1 below.

Before describing this theorem, we introduce some additional notation. First, to each exponent k and finite field $\mathbb{F}_q$ we associate an integer $\gamma = \gamma_q(k)$ defined in terms of $p = \operatorname{ch}(\mathbb{F}_q)$ as follows. We write k in base p, say $k = a_0 + a_1 p + \cdots + a_n p^n$, where $0 \leqq a_i \leqq p-1$ $(0 \leqq i \leqq n)$, and then put $\gamma_q(k) = a_0 + a_1 + \cdots + a_n$. It is apparent that for each q and k one has $\gamma_q(k) \leqq k$, and also that when $k \geqq 2$ and $\operatorname{ch}(\mathbb{F}_q) \nmid k$, then $\gamma_q(k) \geqq 2$. In addition, we define $A = A_q(k)$ by putting

$$A_q(k) = \begin{cases} 1, & \text{when } \operatorname{ch}(\mathbb{F}_q) > k, \\ (1 - 2^{-\gamma_q(k)})^{-1}, & \text{when } \operatorname{ch}(\mathbb{F}_q) < k. \end{cases} \tag{1.2}$$

Finally, when x is a positive real number, we write $\operatorname{Log} x$ for $\max\{1, \log x\}$, and put

$$\hat{G}_q(k) = Ak(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + A \operatorname{Log}\operatorname{Log} k / \operatorname{Log} k). \tag{1.3}$$

Theorem 1.1. *There is a positive absolute constant C_1 with the property that whenever k and q are natural numbers with $\operatorname{ch}(\mathbb{F}_q) \nmid k$, then*

$$G_q(k) \leqq \hat{G}_q(k) + C_1 k \sqrt{\operatorname{Log}\operatorname{Log} k} / \operatorname{Log} k.$$

Meanwhile, when $\operatorname{ch}(\mathbb{F}_q) \mid k$, one has $G_q(k) = G_q\big(k/\operatorname{ch}(\mathbb{F}_q)\big)$.

Some comments are in order concerning the general features of the bound for $G_q(k)$ provided by Theorem 1.1. First, when $\operatorname{ch}(\mathbb{F}_q) \nmid k$, the lower bound $\gamma_q(k) \geqq 2$ ensures that the coefficient A appearing in (1.3) satisfies $1 \leqq A \leqq 4/3$. When $\operatorname{ch}(\mathbb{F}_q) \mid k$, meanwhile, it follows from Theorem 1.1 that $G_q(k) = G_q(k_0)$, where k_0 is the largest divisor of k coprime to q. But the first conclusion of Theorem 1.1 may be used to bound $G_q(k_0)$, and thus one obtains a bound of the same shape, but quantitatively stronger. Finally, when $\gamma_q(k) > 3 \operatorname{Log}\operatorname{Log} k$, one has $|A_q(k) - 1| < 1/(\operatorname{Log} k)^2$. In these circumstances one may replace A by 1 in the upper bound provided by Theorem 1.1 at the cost of increasing the absolute constant C_1.

Almost all work concerning $G_q(k)$ hitherto has been restricted to those situations wherein $\operatorname{ch}(\mathbb{F}_q) > k$. Under this condition, Kubota [13], [14] applied a variant of the Hardy-Littlewood (circle) method involving analogues of Weyl's inequality and Hua's lemma in order to establish that $G_q(k) \leqq 2^k + 1$. By making use of a modification of Vinogradov's mean value theorem, Car [1], [2] obtained the upper bound $G_q(k) \leqq 2k(k-1)\log 2 + 2k + 3$, superior for large k, subject to the same constraint $\operatorname{ch}(\mathbb{F}_q) > k$. In the former work, the use of Weyl differencing on certain generating functions involving kth powers of polynomials produces factors of $k!$ within the arguments of the resulting exponential sums. Since these factors are zero when $\operatorname{ch}(\mathbb{F}_q) \leqq k$, such methods are ineffective in providing non-trivial estimates for the generating functions essential to the

application of the circle method. The work of Car [1], [2] involving Vinogradov's mean value theorem, on the other hand, demands that the polynomials $x_1^j + \cdots + x_k^j$ be independent for $1 \leqq j \leqq k$, and such fails when $\mathrm{ch}(\mathbb{F}_q) \leqq k$. Again, therefore, one encounters a formidable barrier to the extension of these methods to small characteristic. Both the independent work of Matthews [16] (unpublished) and of Webb [26] is subject to the same limitations.

Aside from the improvement in the quality of the estimate provided by Theorem 1.1 over those available hitherto, a notable feature of our work is its relative robustness to changes in the characteristic of the ambient field $\mathbb{F}_q$. We surmount the barriers that previously obstructed viable conclusions for $\mathrm{ch}(\mathbb{F}_q) \leqq k$ by applying the large sieve to obtain a substitute for Weyl's inequality, thereby avoiding the problematic use of Weyl differencing. Such an approach requires the availability of suitable mean value estimates for auxiliary exponential sums. Here we avoid barriers and complications arising from Vinogradov's methods and diminishing range arguments, adapting the theory of smooth Weyl sums to the function field setting through the introduction of exponential sums over smooth polynomials. It is in this step that the iterative methods of Vaughan [22] and the second author [27] play an important rôle, and that the parameter $\gamma_q(k)$ enters the scene. Repeated efficient differencing analogous to that introduced in [27] inherits some of the features of Weyl differencing, and so the number of efficient differences that may be usefully extracted is limited in a manner determined by the divisibility of various binomial coefficients by $\mathrm{ch}(\mathbb{F}_q)$.

Earlier authors have bounded $G_q(k)$ in special situations with $\mathrm{ch}(\mathbb{F}_q) \leqq k$. Cherly [7] and Car and Cherly [5] have addressed cases wherein $k = 3$ and q is a power of 2, applying methods based on the use of Poisson summation to establish that $G_{2^h}(3) \leqq 11$. The latter conclusion has recently been refined by Gallardo [9], and by Car and Gallardo [6], using quite different methods, so that the upper bound 11 can now be replaced by 7 for $h > 4$, by 8 for $h = 4$, and by 10 when $1 \leqq h \leqq 3$. Kubota [14], Theorem 37, meanwhile, made use of diminishing ranges to obtain an upper bound for $G_q(k)$ not far short of $6k \log k + O(k)$. Here we note that Kubota imposes the restriction $k \mid P_k(m)$ for the polynomials m that are to be represented, and we remark also that his exposition contains some (potentially fixable) errors.

The local solubility conditions associated with the representation problem (1.1) are somewhat more complicated than is the case for the classical version of Waring's problem. Suppose that $\mathrm{ch}(\mathbb{F}_q) = p$. When $p \mid k$, we have already noted that (1.1) is soluble only when $m \in \mathbb{F}_q[t^p]$. A second less obvious condition for solubility presents itself when k is a multiple of a *q^b-norm* for some natural number b. In order to describe this condition, suppose that $q = p^h$. Let $l \in \mathbb{N}$, and let a be a divisor of lh with $1 \leqq a < lh$. Then it follows from [8], §1.1 that whenever $\varpi \in \mathbb{F}_q[t]$ is an irreducible polynomial of degree l, and k is a multiple of $N = (p^{lh} - 1)/(p^a - 1)$, then there exist polynomials $m \in \mathbb{F}_q[t]$ for which (1.1) admits no solutions modulo ϖ. In brief, the map defined by taking x to $x^N \pmod{\varpi}$ is the norm map from $\mathbb{F}_q[t]/(\varpi)$ down to a subfield of the latter having p^a elements. Each $m \in \mathbb{F}_q[t]$ for which m modulo ϖ does not belong to this subfield (in fact, the bulk of $\mathbb{F}_q[t]$) fails to be represented in the shape (1.1), and this failure is detected by a local condition at the place ϖ. As we shall see in §5, for all k and q, provided that $s \geqq 2k + 1$, all local solubility conditions are embodied within the constraint $m \in \mathbb{J}_q^k[t]$ in (1.1). In addition, when $\mathrm{ch}(\mathbb{F}_q) > k$ one has $\mathbb{J}_q^k[t] = \mathbb{F}_q[t]$.

Before leaving Theorem 1.1, we remark that the analysis underlying the derivation of the lower order terms in (1.3) may be applied without substantive modification in the classical version of Waring's problem. Thus, writing $G(k)$ for the least integer s_2 with the property that whenever $s \geqq s_2$, then every sufficiently large natural number is the sum of at most s kth powers of positive integers, one has

$$G(k) \leqq k\big(\log k + \log\log k + 2 + \log\log k/\log k + O(\sqrt{\log\log k}/\log k)\big).$$

This refines an earlier bound of the second author [29], Theorem 1.4, in which the final two terms contained in the outer set of parentheses are replaced simply by $O(\log\log k/\log k)$.

The theory of exponential sums over smooth polynomials developed in §§2–14 puts at our disposal a flexible variant of the circle method with wide applicability. We illustrate this point with two immediate consequences of our methods. In §15 we establish that, in the sense of natural density, almost all $m \in \mathbb{F}_q[t]$ admit a strict representation in the shape (1.1) whenever $s \geqq \frac{1}{2}Ak\big(\operatorname{Log} k + O(\operatorname{Log}\operatorname{Log} k)\big)$. In order to be precise, we introduce some additional notation. When N is a large natural number, denote by $\mathscr{E}_{s,k}(N)$ the set of polynomials $m \in \mathbb{J}_q^k[t]$ with $\operatorname{ord} m \leqq N$ that do not admit a strict representation in the shape (1.1). We write $E_{s,k}(N)$ for the cardinality of $\mathscr{E}_{s,k}(N)$. Let the characteristic of $\mathbb{F}_q$ be p, and suppose that p^τ is the largest power of p dividing k. We define $G_q^+(k)$ to be the smallest integer s_3 with the property that whenever $s \geqq s_3$, then $E_{s,k}(N) = o(q^{N/p^\tau})$ as $N \to \infty$.

Theorem 1.2. *There is a positive absolute constant C_2 with the property that whenever k and q are natural numbers with $\operatorname{ch}(\mathbb{F}_q) \nmid k$, then*

$$G_q^+(k) \leqq \frac{1}{2}\hat{G}_q(k) + C_2 k\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k.$$

When $\operatorname{ch}(\mathbb{F}_q) \mid k$, meanwhile, one has $G_q^+(k) = G_q^+\big(k/\operatorname{ch}(\mathbb{F}_q)\big)$.

In §16, we discuss the density of solutions of diagonal equations in $\mathbb{F}_q[t]$. Given $s, k \in \mathbb{N}$, and fixed coefficients $a_i \in \mathbb{F}_q[t]$ $(1 \leqq i \leqq s)$, denote by $N_s(B; \boldsymbol{a})$ the number of solutions of the equation

$$a_1 x_1^k + \cdots + a_s x_s^k = 0, \tag{1.4}$$

with $\boldsymbol{x} \in \mathbb{F}_q[t]^s$ and $\operatorname{ord} x_i \leqq B$ $(1 \leqq i \leqq s)$.

Theorem 1.3. *Let k and q be natural numbers with $\operatorname{ch}(\mathbb{F}_q) \nmid k$. There is a positive absolute constant C_3 with the property that whenever s is a natural number with*

$$s \geqq \hat{G}_q(k) + C_3 k\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k,$$

then the equation (1.4) satisfies the following quantitative local-to-global principle. Let $\boldsymbol{a} \in (\mathbb{F}_q[t]\backslash\{0\})^s$, and suppose that the equation (1.4) has non-trivial solutions in all completions $\mathbb{F}_q(t)_\varpi$ of $\mathbb{F}_q(t)$. Then one has $N_s(B; \boldsymbol{a}) \gg (q^B)^{s-k}$.

The Lang-Tsen theory of C_i-fields (see, in particular, [15], Theorem 8) shows that the equation (1.4) possesses a solution $\boldsymbol{x} \in \mathbb{F}_q[t]^s \setminus \{\mathbf{0}\}$ whenever $s > k^2$. The local solubility hypothesis of Theorem 1.3 is consequently satisfied automatically under the same condition. Rather than merely establishing the existence of non-trivial solutions of equation (1.4), our objective is instead the proof of a Hasse principle with good control of the associated density of solutions. We note in this context that weak approximation follows by our methods as soon as $s \geqq \hat{G}_q(k) + C_3 k \sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k$.

A perspective on Waring's problem in $\mathbb{F}_q[t]$ has been presented by Effinger and Hayes [8] that differs from that motivating the discourse of this paper. As an analogue of the function $G(k)$ familiar from the classical version of Waring's problem, Effinger and Hayes define a function $\mathscr{G}(k)$ associated with the collection $\mathscr{F}_k$ of all polynomial rings $\mathbb{F}_q[t]$ having characteristic exceeding k (see [8], Definition 1.13). They define $\mathscr{G}(k)$ to be the least integer s with the property that, with the exception of at most finitely many polynomials from the whole collection $\mathscr{F}_k$, whenever $m \in \mathbb{F}_q[t]$ and $\mathbb{F}_q[t] \in \mathscr{F}_k$, then m has a strict representation in the shape (1.1). The upper bound $\mathscr{G}(k) < \infty$ is asserted by [8], Theorem 1.9, and the refinement $\mathscr{G}(k) \leqq k^2 2^k$ may be extracted from the discussion following the statement of [8], Theorem 8.15. Unfortunately, there is apparently an error in the proof of [8], Theorem 8.11, that invalidates these conclusions. The last line of the proof of this theorem asserts, inter alia, that the function $(d + q^{d-2})^{2^{1-d}}$ is a bounded function of d when the principal conclusion demands instead that it be a bounded function of q. We have not found a means to repair the proof of this version of Weyl's inequality in such a manner that a direct proof of [8], Theorems 8.15 and 1.9 may be recovered. However, by employing an alternative strategy we have obtained an upper bound for $\mathscr{G}(k)$ somewhat sharper than that claimed by Effinger and Hayes [8]. We will report on this work elsewhere.

The reader will discern a number of avenues available for future research stemming from the ideas presented herein, and we plan to pursue several in future papers. Our most immediate concern is the explicit computation of bounds for $G_q(k)$ for smaller values of k. There is also the problem of obtaining the expected asymptotic formula for the number of solutions of (1.1), and likewise for quite general systems of homogeneous equations over $\mathbb{F}_q[t]$. Finally, we intend to consider bounds for $v_q(k)$ going beyond the trivial relation $v_q(k) \leqq G_q(k) + 1$ that, in combination with the conclusion of Theorem 1.1, already yields improvements in the results of Vaserstein [21] relating to the ring $\mathbb{F}_q[t]$ for smaller q. This list by no means exhausts the menu available for the enthusiast. For example, Car [4] has considered an analogue of $G_q(k)$ for field extensions of $\mathbb{F}_q(t)$, and presumably our methods extend to this situation with additional effort.

We describe the key elements of the circle method as it applies to $\mathbb{F}_q[t]$ in §2. Polynomials having only small degree irreducible divisors (that is, *smooth polynomials*) play a distinguished rôle in our method, and so in §3 we discuss their distribution in sufficient detail for later application. In §4 we build on this work to obtain major arc approximations for smooth Weyl sums, with a similar analysis for complete Weyl sums, and thus in §5 we derive a satisfactory lower bound for the major arc contribution. As is familiar to aficionados of the modern circle method, there is a gap between the domains accessible to major and minor arc treatments, and so in §6 we develop appropriate pruning technology. Then, in §7, we move on to consider mean values of smooth Weyl sums, beginning first with a fundamental lemma, then in §8 establishing an efficient differencing process for mean values, and finally deriving permissible exponents for these mean values in §9. Following some prelim-

inary manoeuvres in §10, analogues of Weyl's estimates for exponential sums follow via the large sieve in §§11 to 13, with large moduli handled in §11, small moduli in §12, and explicit Weyl estimates derived in §13. The latter are then applied in §14 in order to bound $G_q(k)$, and thereby we complete the proof of Theorem 1.1. Finally, in §15 we apply the methods developed for our work on $G_q(k)$ in order rapidly to establish Theorem 1.2, the proof of Theorem 1.3 in §16 being similarly swift.

It is convenient throughout to reserve uppercase Latin letters for positive real numbers, and lowercase Latin letters (with the exception of d, e, i, j, k, n, q, r, s, t) for polynomials in $\mathbb{F}_q[t]$. We reserve q for the cardinality of the finite field $\mathbb{F}_q$ and t for the indeterminate underlying the ring $\mathbb{F}_q[t]$. The letter e will be associated with the exponential function, and d, i, j, k, n, r, s with positive integers. Irreducible polynomials ϖ will be supposed throughout to be monic, and we write $\varpi^r \| x$ when $\varpi^r \mid x$ but $\varpi^{r+1} \nmid x$. We denote the cardinality of a set $\mathfrak{X}$ by $\operatorname{card}(\mathfrak{X})$. Throughout, the letter ε will denote a sufficiently small positive number. We use $\ll$ and $\gg$ to denote Vinogradov's well-known notation, implicit constants depending at most on ε, unless otherwise indicated. In an effort to simplify our analysis, we adopt the convention that whenever ε appears in a statement, then we are implicitly asserting that for each $\varepsilon > 0$ the statement holds for sufficiently large values of the main parameter. Note that the "value" of ε may consequently change from statement to statement, and hence also the dependence of implicit constants on ε. Finally, from time to time we make use of vector notation in order to save space. Thus, for example, we may abbreviate $(c_1, \dots, c_t)$ to $\boldsymbol{c}$.

2. The circle method for polynomial rings

While the circle method for $\mathbb{F}_q[t]$ mirrors the classical version familiar from applications over $\mathbb{Z}$, the substantial differences in detail between these rings demand explanation. Our goal in the present section is to introduce such notation and basic notions as are subsequently needed to initiate discussion of the key components of this version of the circle method.

Associated with the polynomial ring $\mathbb{F}_q[t]$ defined over the field $\mathbb{F}_q$ is its field of fractions $\mathbb{K} = \mathbb{F}_q(t)$. Write $\mathbb{K}_\infty = \mathbb{F}_q(\!(1/t)\!)$ for the completion of $\mathbb{F}_q(t)$ at ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i \leqq n} a_i t^i$ for some $n \in \mathbb{Z}$ and coefficients $a_i = a_i(\alpha)$ in $\mathbb{F}_q$ $(i \leqq n)$. Our previous definition of $\operatorname{ord} m$ for polynomials m now extends to elements α of $\mathbb{K}_\infty$ by defining $\operatorname{ord} \alpha$ to be the largest integer i for which $a_i(\alpha) \neq 0$. We then write $\langle \alpha \rangle$ for $q^{\operatorname{ord} \alpha}$. In this context, we adopt the convention that $\operatorname{ord} 0 = -\infty$ and $\langle 0 \rangle = 0$. Consider next the compact additive subgroup $\mathbb{T}$ of $\mathbb{K}_\infty$ defined by $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle < 1\}$. Every element α of $\mathbb{K}_\infty$ can be written uniquely in the shape $\alpha = [\alpha] + \|\alpha\|$, where $[\alpha] \in \mathbb{F}_q[t]$ and $\|\alpha\| \in \mathbb{T}$, and we may normalise any Haar measure $d\alpha$ on $\mathbb{K}_\infty$ in such a manner that $\int_{\mathbb{T}} 1 \, d\alpha = 1$.

We are now equipped to define an analogue of the exponential function. Suppose that $\operatorname{ch}(\mathbb{F}_q) = p$. There is a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e\big(\operatorname{tr}(a)/p\big)$, where we write $e(z)$ for $e^{2\pi i z}$, and where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denotes the familiar trace map. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q\big(a_{-1}(\alpha)\big)$. It is often convenient to refer to $a_{-1}(\alpha)$

as being the residue of α, an element of $\mathbb{F}_q$ that we abbreviate to $\operatorname{res}\alpha$. In this guise we have $e(\alpha) = e_q(\operatorname{res}\alpha)$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [14], Lemma 1, takes the shape

$$\int_{\mathbb{T}} e(h\alpha)\,d\alpha = \begin{cases} 0, & \text{when } h \in \mathbb{F}_q[t]\backslash\{0\}, \\ 1, & \text{when } h = 0. \end{cases} \tag{2.1}$$

In order better to highlight parallels between the application of the circle method over $\mathbb{Z}$ and that over $\mathbb{F}_q[t]$, we adopt the convention that whenever X is a real number, then $\hat{X}$ denotes q^X. Next, when R and P are positive numbers with $R \leqq P$, we denote by $\mathscr{A}(P,R)$ the set of *degree R-smooth polynomials*, that is

$$\mathscr{A}(P,R) = \{x \in \mathbb{F}_q[t] : \langle x\rangle \leqq \hat{P}, \text{ and } \varpi \mid x \Rightarrow \langle \varpi\rangle \leqq \hat{R}\}. \tag{2.2}$$

Here and elsewhere we adopt the convention that whenever ϖ is used to denote a polynomial, then this polynomial is assumed to be irreducible and monic. We fix a natural number k with $k \geqq 2$, and then define the classical Weyl sum $F(\alpha) = F(\alpha; P)$, and smooth Weyl sum $f(\alpha) = f(\alpha; P, R)$, by putting

$$F(\alpha;P) = \sum_{\langle x\rangle \leqq \hat{P}} e(\alpha x^k) \quad \text{and} \quad f(\alpha;P,R) = \sum_{x \in \mathscr{A}(P,R)} e(\alpha x^k). \tag{2.3}$$

We seek a strict representation of a given polynomial m of large degree as the sum of s kth powers, with s chosen suitably large in terms of k. To this end we define $P = P_k(m)$ as in §1, we take $\eta > 0$ sufficiently small in terms of k and s, and we consider the number $R(m) = R_{s,k}(m;\eta)$ of representations of m in the shape

$$m = x_1^k + x_2^k + y_1^k + y_2^k + \cdots + y_{s-2}^k, \tag{2.4}$$

with $\langle x_i\rangle \leqq \hat{P}$ $(i = 1, 2)$ and $y_j \in \mathscr{A}(P, \eta P)$ $(1 \leqq j \leqq s-2)$. We note that $R(m)$ provides a lower bound for the number of strict representations of m in the shape (1.1). When $\mathscr{B}$ is a measurable subset of $\mathbb{T}$, define

$$\mathscr{R}_s(m;\mathscr{B}) = \int_{\mathscr{B}} F(\alpha)^2 f(\alpha)^{s-2} e(-m\alpha)\,d\alpha. \tag{2.5}$$

Here and throughout, whenever the secondary parameters of the exponential sums are suppressed, then $F(\alpha)$ and $f(\alpha)$ respectively are used to denote $F(\alpha;P)$ and $f(\alpha;P,R)$, with $P = P_k(m)$ and $R = \eta P$. It follows from (2.1) that $R(m) = \mathscr{R}_s(m;\mathbb{T})$. A heuristic argument suggests that when $s \geqq k+1$ and the necessary local conditions are met, then $R(m)$ should be of order $\hat{P}^{s-k}$. We confirm this expectation with the number of variables inflated by a factor roughly of $\log k$.

We analyse the integral (2.5) via the Hardy-Littlewood (circle) method, and to this end we define sets of *major* and *minor arcs* corresponding to well and poorly approximable elements of $\mathbb{T}$. Let W be a positive parameter with $2W < kP$. Given polynomials a and g with $(a,g) = 1$ and g monic, we define the *Farey arc* $\mathfrak{M}(g,a) = \mathfrak{M}(g,a;W)$ about a/g associated with the parameter W by

$$\mathfrak{M}(g,a;W) = \{\alpha \in \mathbb{K}_\infty : \langle g\alpha - a\rangle < \hat{W}\hat{P}^{-k}\}. \tag{2.6}$$

The set of *major arcs* $\mathfrak{M}(W)$ is defined to be the union of the sets $\mathfrak{M}(g,a;W)$ with

$$a,g\in \mathbb{F}_q[t],\quad g \text{ monic},\quad 0\leqq \langle a\rangle < \langle g\rangle \leqq \hat{W} \quad \text{and} \quad (a,g)=1. \tag{2.7}$$

It is apparent from (2.6) and (2.7) that $\mathfrak{M}(W)\subseteqq \mathbb{T}$. We write $\mathfrak{m}(W)=\mathbb{T}\setminus\mathfrak{M}(W)$ for the complementary set of *minor arcs*. As the reader will easily verify, the conditions (2.6) and (2.7) ensure that the arcs $\mathfrak{M}(g,a;W)$ comprising $\mathfrak{M}(W)$ are disjoint. When W is a positive parameter satisfying $3W<kP$, it is useful also to define the set of arcs $\mathfrak{N}(W)$ to be the union of the sets

$$\mathfrak{N}(g,a;W)=\{\alpha\in \mathbb{K}_\infty : \langle g\alpha-a\rangle < \langle g\rangle \hat{W}\hat{P}^{-k}\} \tag{2.8}$$

with polynomials a and g subject to (2.7). Again one has $\mathfrak{N}(W)\subseteqq\mathbb{T}$, and the arcs $\mathfrak{N}(g,a;W)$ comprising $\mathfrak{N}(W)$ are disjoint. Finally, we write $\mathfrak{n}(W)=\mathbb{T}\setminus\mathfrak{N}(W)$.

Our strategy for estimating $R(m)$ is now familiar from the classical version of the circle method. We put $V=\left[\frac{1}{12}\log_q P\right]$, and we write $\mathfrak{N}=\mathfrak{N}(V)$ and $\mathfrak{n}=\mathfrak{n}(V)$. Here and elsewhere we use $\log_q x$ to denote $(\log x)/(\log q)$. In §4 we derive asymptotic formulae for the generating functions $F(\alpha)$ and $f(\alpha)$ valid for $\alpha\in\mathfrak{N}$. These formulae are then converted in §5 to an asymptotic formula for the total major arc contribution, and indeed we are able to establish the asymptotic relation

$$\mathscr{R}_s(m;\mathfrak{N})=c_{s,k}(m;\eta)\hat{P}^{s-k}+o(\hat{P}^{s-k}), \tag{2.9}$$

valid for $s\geqq 2k+1$, wherein $c_{s,k}(m;\eta)$ is a number depending at most on η, q, s, k and m. Provided that $m\in \mathbb{J}_q^k[t]$, it transpires that $c_{s,k}(m;\eta)>0$. The goal of §§6 to 14 is then to derive the appropriate complementary minor arc bound $\mathscr{R}_s(m;\mathfrak{n})=o(\hat{P}^{s-k})$, valid for

$$s\geqq \hat{G}_q(k)+C_1 k\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k, \tag{2.10}$$

with C_1 a suitably large positive absolute constant. On combining the last estimate with (2.5) and (2.9), we deduce that whenever $m\in\mathbb{J}_q^k[t]$ and s satisfies (2.10), then $R(m)\gg\hat{P}^{s-k}$, and consequently Theorem 1.1 follows at once.

Throughout our applications of the circle method in §§4–16 inclusive, unless stated otherwise we suppose that $\operatorname{ch}(\mathbb{F}_q)\nmid k$.

3. A quasi-ordering on the ring of polynomials

By analogy with the familiar formulation of the circle method for $\mathbb{Z}$, one expects that asymptotic formulae for the generating functions $F(\alpha)$ and $f(\alpha)$, valid for $\alpha\in\mathfrak{N}$, will follow via partial summation. However, the ordering on $\mathbb{F}_q[t]$ provided by the degree of a polynomial is too coarse to permit such arguments to succeed. For example, one may have $e(\alpha x^k)\neq e(\alpha y^k)$ even when $\langle x\rangle=\langle y\rangle$. We surmount this difficulty by introducing a finer notion of size that distinguishes between distinct polynomials, and thereby facilitates arguments involving the use of partial summation. In this section we establish such properties of various counting functions for polynomials in arithmetic progressions, and for smooth polynomials, as are required in subsequent sections of this paper.

Before defining our measure of the size of a polynomial, we recall that the set of non-zero elements $\mathbb{F}_q^\times$ of a finite field $\mathbb{F}_q$ forms a cyclic group of order $q-1$. Let $\xi \in \mathbb{F}_q^\times$ be a fixed generator of this cyclic group. Formally defining $\xi^{-\infty}$ to be the element 0 of $\mathbb{F}_q$, it follows that every element of $\mathbb{F}_q$ can be written uniquely in the form ξ^i for some index i from the set $\mathscr{I} = \{-\infty, 0, 1, \dots, q-2\}$. We define a bijection $\langle \cdot \rangle_\xi$ from $\mathbb{F}_q[t]$ to the non-negative integers as follows. When $a \in \mathbb{F}_q$, we define the index $v \in \mathscr{I}$ associated with a via the relation $a = \xi^v$, and then put $\langle a \rangle_\xi = v+1$ when $v \in \mathscr{I} \backslash \{-\infty\}$, and $\langle a \rangle_\xi = 0$ when $v = -\infty$. Given a polynomial $m = a_0 + a_1 t + \cdots + a_N t^N$ in $\mathbb{F}_q[t]$, we then define $\langle m \rangle_\xi$ by

$$\langle m \rangle_\xi = \sum_{i=0}^{N} \langle a_i \rangle_\xi q^i. \tag{3.1}$$

The polynomial ring $\mathbb{F}_q[t]$ now inherits an ordering from the non-negative integers. When $a, b \in \mathbb{F}_q[t]$, we write $a \prec b$ when $\langle a \rangle_\xi < \langle b \rangle_\xi$, and we write $a \leqq b$ when either $a \prec b$ or $a = b$. Also, we write $a \succ b$ and $a \geqq b$ when $b \prec a$ and $b \leqq a$, respectively. As is apparent from (3.1), whenever $a, b \in \mathbb{F}_q[t]$ and the degree of b exceeds that of a, then $\langle b \rangle_\xi > \langle a \rangle_\xi$. Indeed, if the degree of m is N, then one has $q\hat{N} > \langle m \rangle_\xi \geqq \hat{N}$.

It is convenient to have available a map $T_\xi(\cdot)$ from the non-negative integers to $\mathbb{F}_q[t]$ that inverts that defined via (3.1). For this purpose, when u is an integer with $0 \leqq u \leqq q-1$, we define $T_\xi(u)$ by putting $T_\xi(u) = \xi^{u-1}$ when $u \in \{1, 2, \dots, q-1\}$, and $T_\xi(u) = 0$ when $u = 0$. Next, given a non-negative integer v, we write v in base q as $v = v_0 + v_1 q + \cdots + v_N q^N$, with $0 \leqq v_i \leqq q-1$ $(0 \leqq i \leqq N)$, and then put $T_\xi(v) = T_\xi(v_0) + T_\xi(v_1)t + \cdots + T_\xi(v_N)t^N$.

We may now discuss the distribution of polynomials in arithmetic progressions.

Lemma 3.1. *Let g and r be elements of $\mathbb{F}_q[t]$. Then whenever $X \in \mathbb{N}$, we have*

$$\operatorname{card}\{m \in \mathbb{F}_q[t] : \langle m \rangle_\xi \leqq X \text{ and } m \equiv r \pmod g\} = X/\langle g \rangle + O(1).$$

Proof. When $W \in \mathbb{N}$ and $g, r \in \mathbb{F}_q[t]$, we define $\mathscr{Z}_{g,r}(W)$ to be the set of polynomials $m \in \mathbb{F}_q[t]$ for which $\langle m \rangle_\xi \leqq W$ and $m \equiv r \pmod g$, and we write $Z_{g,r}(W)$ for $\operatorname{card}\big(\mathscr{Z}_{g,r}(W)\big)$. Note that there is no loss in supposing that $\operatorname{ord} r < \operatorname{ord} g$, for one may reduce r modulo g. Under this assumption, if $m \in \mathscr{Z}_{g,r}(W)$ and we subtract r from m, then it is only the monomials with degree smaller than $\operatorname{ord} g$ that are affected, whence

$$|\langle m \rangle_\xi - \langle m - r \rangle_\xi| \leqq \sum_{i=0}^{\operatorname{ord} g - 1} (q-1)q^i < \langle g \rangle.$$

Thus we see that whenever $m \in \mathscr{Z}_{g,a}(W)$, then $m \pm r \in \mathscr{Z}_{g,a\pm r}(W + \langle g \rangle)$, whence

$$Z_{g,0}(W - \langle g \rangle) \leqq Z_{g,r}(W) \leqq Z_{g,0}(W + \langle g \rangle). \tag{3.2}$$

Every polynomial $m \in \mathbb{F}_q[t]$ belongs to some residue class modulo g, and so by averaging over the elements $r \in \mathbb{F}_q[t]$ with $0 \leqq \langle r \rangle < \langle g \rangle$ within (3.2), we obtain

$$Z_{g,0}(W - \langle g \rangle) \leqq (W+1)/\langle g \rangle \leqq Z_{g,0}(W + \langle g \rangle).$$

It therefore follows that

$$\langle g\rangle^{-1}(X-\langle g\rangle+1)\leqq Z_{g,0}(X)\leqq \langle g\rangle^{-1}(X+\langle g\rangle+1),$$

and so the proof of the lemma is completed by reference to (3.2).

We now analyse the distribution of refined smooth polynomials. Given positive numbers X and Y with $Y\leqq X$, define the set of Y-smooth polynomials

$$\tilde{\mathscr{A}}_\xi(X,Y)=\{n\in\mathbb{F}_q[t]:\langle n\rangle_\xi\leqq X \text{ and } \varpi\,|\,n\Rightarrow\langle\varpi\rangle_\xi\leqq Y\},$$

and write $\tilde{A}_\xi(X,Y)=\operatorname{card}\big(\tilde{\mathscr{A}}_\xi(X,Y)\big)$. One readily confirms the relation

$$\mathscr{A}(P,R)=\tilde{\mathscr{A}}_\xi(q\hat{P}-1,2\hat{R}-1), \tag{3.3}$$

and so the set $\tilde{\mathscr{A}}_\xi(X,Y)$ offers a refinement of the set $\mathscr{A}(P,R)$.

Before announcing an asymptotic formula for $\operatorname{card}\big(\tilde{\mathscr{A}}_\xi(X,Y)\big)$, it is helpful to introduce some notation. When X and Y are positive numbers with $Y<X$, define

$$\Pi_q(X,Y)=\prod_{Y<\langle\varpi\rangle_\xi\leqq X}\varpi,\quad \rho_q(X,Y)=\sum_{\substack{d\,|\,\Pi_q(X,Y)\\ \langle d\rangle_\xi\leqq X}}^{\dagger}\mu(d)\langle d\rangle^{-1}, \tag{3.4}$$

and

$$E(X,Y)=\operatorname{card}\{d\in\mathbb{F}_q[t]:d \text{ monic}, \langle d\rangle_\xi\leqq X \text{ and } \varpi\,|\,d\Rightarrow Y<\langle\varpi\rangle_\xi\leqq X\}. \tag{3.5}$$

Here, we use $\mu(\cdot)$ to denote the Möbius function on $\mathbb{F}_q[t]$, and throughout, whenever we apply the decoration $\dagger$ to a summation or product, we implicitly assume that the latter is restricted to monic polynomials.

Lemma 3.2. *Suppose that X and Y are positive numbers with $Y<X$. Then $E(X,Y)\ll X/\log(2Y)$.*

Proof. Write $L(W)=[\log_q W]$ for $W=X,Y$. Then an upper bound for $E(X,Y)$ is provided by sieving out the zero congruence class modulo ϖ, for each irreducible ϖ with $\operatorname{ord}\varpi\leqq\min\Big\{L(Y),\frac{1}{2}L(X)\Big\}$, from the polynomials d with $\operatorname{ord}d\leqq L(X)$. A modicum of computation leads from Hsu [12], Theorem 3.2, to the upper bound

$$E(X,Y)\ll\frac{q^{L(X)}}{\min\Big\{L(Y),\frac{1}{2}L(X)\Big\}}\ll\frac{X}{\log(2Y)},$$

and this completes the proof of the lemma.

Lemma 3.3. *Let X and Y be positive numbers with $1\leqq Y<X$. Then*

$$\tilde{A}_\xi(X,Y)=\rho_q(X,Y)X+O\big(X/\log(2Y)\big).$$

Proof. If n is an element of $\tilde{\mathscr{A}}_\xi(X, Y)$, then $\langle n\rangle_\xi \leqq X$. The monic divisors of n are polynomials of degree at most $\operatorname{ord} n$, whence of size at most $\langle n\rangle_\xi \leqq X$. By the inclusion-exclusion principle, therefore, one has

$$\sum_{n\in\tilde{\mathscr{A}}_\xi(X,Y)} 1 = \sum_{\substack{d\mid \Pi_q(X,Y)\\ \langle d\rangle_\xi\leqq X}}^{\dagger} \mu(d) \sum_{\substack{\langle m\rangle_\xi\leqq X\\ d\mid m}} 1.$$

An application of Lemma 3.1 consequently reveals that

$$\tilde{A}_\xi(X, Y) = \sum_{\substack{d\mid \Pi_q(X,Y)\\ \langle d\rangle_\xi\leqq X}}^{\dagger} \mu(d)\big(X/\langle d\rangle + O(1)\big) = \rho_q(X, Y)X + O\big(E(X, Y)\big),$$

and so the proof of the lemma follows by making use of Lemma 3.2.

It is convenient for future reference to record an estimate for the relative density $\rho_q(X, Y)$ in terms of the familiar Dickman function $\rho(u)$. We recall at this point that $\rho(u)$ is defined for real numbers u to be the unique continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ $(u > 1)$ satisfying the initial conditions $\rho(u) = 0$ for $u \leqq 0$, and $\rho(u) = 1$ for $0 < u \leqq 1$.

Lemma 3.4. *When R and P are positive numbers with $P \geqq 1$ and $2P/\log(2P) < R < P$, one has*

$$\rho_q(q\hat{\boldsymbol{P}} - 1, 2\hat{\boldsymbol{R}} - 1) = \rho(P/R) + O(P^{-1/2}).$$

Proof. Estimates for the number of smooth polynomials available in the literature (see [3], Proposition II.4, or alternatively [18] or [20]) provide the formula

$$\operatorname{card}\big(\mathscr{A}(P, R)\big) = \rho(P/R)q\hat{\boldsymbol{P}} + O(2^{P/R}\hat{\boldsymbol{P}}/R).$$

On the other hand, it follows from Lemma 3.3 that

$$\tilde{A}_\xi(q\hat{\boldsymbol{P}} - 1, 2\hat{\boldsymbol{R}} - 1) = \rho_q(q\hat{\boldsymbol{P}} - 1, 2\hat{\boldsymbol{R}} - 1)q\hat{\boldsymbol{P}} + O(\hat{\boldsymbol{P}}/R).$$

When $2P/\log(2P) < R < P$, therefore, we may conclude from (3.3) that

$$\rho_q(q\hat{\boldsymbol{P}} - 1, 2\hat{\boldsymbol{R}} - 1) - \rho(P/R) \ll 2^{P/R}R^{-1} \ll P^{-1/2},$$

and thus the proof of the lemma is complete.

4. Major arc approximations for exponential sums

In order to obtain the asymptotic formula for the major arc contribution given by (2.9), one must establish control of the generating functions $F(\alpha)$ and $f(\alpha)$ for $\alpha \in \mathfrak{N}$. Our goal in this section is to obtain asymptotic formulae for these exponential sums and certain associated generating functions of use on the set of major arcs. When α is close to a rational point a/g of small height, it transpires that $F(\alpha)$ is easily approximated in terms of the local generating function $S(g, a)$, defined for $a, g \in \mathbb{F}_q[t]$ by

$$S(g, a) = \sum_{\langle r\rangle<\langle g\rangle} e(ar^k/g). \tag{4.1}$$

Lemma 4.1. (i) *Suppose that* $\alpha \in \mathbb{T}$, *and that* $\alpha = a/g + \beta$ *with* $a, g \in \mathbb{F}_q[t]$, $0 \leqq \langle a \rangle < \langle g \rangle \leqq \hat{\boldsymbol{P}}$ *and* $\langle \beta \rangle < \langle g \rangle^{-1} \hat{\boldsymbol{P}}^{1-k}$. *Then* $F(\alpha; P) = \langle g \rangle^{-1} S(g, a) F(\beta; P)$.

(ii) *When* $\langle \beta \rangle < \hat{\boldsymbol{P}}^{1-k}$, *one has* $F(\beta; P) \ll \hat{\boldsymbol{P}}(1 + \hat{\boldsymbol{P}}^k \langle \beta \rangle)^{-1/k}$.

(iii) *When* $(g, a) = 1$, *one has* $S(g, a) \ll \langle g \rangle^{1-1/k}$.

Proof. The conclusion of part (i) of the lemma is [14], Proposition 4, and that of part (iii) is estimate (a) of [14], Lemma 22. It remains to establish part (ii). When $\langle \beta \rangle \leqq \hat{\boldsymbol{P}}^{-k}$ the desired bound is immediate from the trivial estimate $F(\beta; P) \ll \hat{\boldsymbol{P}}$. We may suppose henceforth, therefore, that $\hat{\boldsymbol{P}}^{-k} < \langle \beta \rangle < \hat{\boldsymbol{P}}^{1-k}$. Put $L = -\operatorname{ord} \beta$, so that $L = kP - N$ for some integer N with $1 \leqq N \leqq P - 1$. We may write β in the form $\beta = \sum_{i \leqq -L} b_i t^i$, with $b_i \in \mathbb{F}_q$ $(i \leqq -L)$ and $b_{-L} \neq 0$. Next let r be a non-negative parameter with $r \leqq P$, and consider the contribution within the exponential sum $F(\beta; P)$ defined by (2.3) arising from those terms x with $\operatorname{ord} x = P - r$. We write $x = c_0 + c_1 t + \cdots + c_{P-r} t^{P-r}$, with $c_i \in \mathbb{F}_q$ $(0 \leqq i \leqq P - r)$ and $c_{P-r} \neq 0$.

Suppose temporarily that $N > rk - 1$, and write $M = P + r(k-1) - N - 1$, so that $0 \leqq M < P - r$ and $r < P/k$. Let $\Xi(\boldsymbol{c})$ denote the coefficient of t^{L-1} in the expansion of x^k. The monomials occurring in $\Xi(\boldsymbol{c})$ take the shape $c_0^{\kappa_0} c_1^{\kappa_1} \dots c_{P-r}^{\kappa_{P-r}}$, where the exponents κ_i $(0 \leqq i \leqq P - r)$ are non-negative integers with

$$\kappa_0 + \kappa_1 + \cdots + \kappa_{P-r} = k \quad \text{and} \quad \kappa_1 + 2\kappa_2 + \cdots + (P-r)\kappa_{P-r} = L - 1. \tag{4.2}$$

It follows from (4.2) that

$$\kappa_1 + \cdots + \kappa_{M-1} + \kappa_{M+1} + \cdots + \kappa_{P-r} \leqq k - \kappa_M,$$

and hence that

$$\begin{aligned}(k - \kappa_M)(P - r) \geqq L - 1 - \kappa_M M &= kP - N - 1 - \kappa_M\big(P + r(k-1) - N - 1\big) \\ &= (k - \kappa_M)(P - r) + (\kappa_M - 1)(N + 1 - rk).\end{aligned}$$

Our hypothesis that $N > rk - 1$ consequently ensures that $\kappa_M \leqq 1$. On making use also of (4.2), we deduce in addition that when $\kappa_M = 1$, one necessarily has $\kappa_{P-r} = k - 1$ and $\kappa_i = 0$ $(0 \leqq i < P - r, i \neq M)$. It follows that for a suitable polynomial $\Upsilon(\boldsymbol{c})$ in the variables c_i $(0 \leqq i \leqq P - r, i \neq M)$, one may write $\Xi(\boldsymbol{c}) = kc_M c_{P-r}^{k-1} + \Upsilon(\boldsymbol{c})$. Plainly, moreover, the coefficients of the terms t^j in the expansion of x^k with degree $j \geqq L$ cannot involve any positive power of c_M. We therefore deduce that the contribution of these terms x within the sum defining $F(\alpha; P)$ in (2.3) is bounded above by

$$\left| \sum_{\operatorname{ord} x = P - r} e(\beta x^k) \right| \leqq \sum_{\substack{c_i \in \mathbb{F}_q \\ (0 \leqq i < P-r,\, i \neq M)}} \sum_{c_{P-r} \in \mathbb{F}_q^\times} \left| \sum_{c_M \in \mathbb{F}_q} e_q(k b_{-L} c_M c_{P-r}^{k-1}) \right|. \tag{4.3}$$

Since the coefficient $kb_{-L}c_{P-r}^{k-1}$ of c_M in the innermost sum on the right-hand side of (4.3) is non-zero, this sum is necessarily zero, and hence the left-hand side of (4.3) is zero

whenever $0 \leqq r < (N+1)/k$. On noting that $P - (N+1)/k = -(\operatorname{ord}\beta + 1)/k$, we therefore deduce from (2.3) that

$$|F(\beta;P)| = \Big| \sum_{\operatorname{ord} x \leqq -(\operatorname{ord}\beta+1)/k} e(\beta x^k) \Big| \leqq \sum_{\langle x\rangle \leqq \langle\beta\rangle^{-1/k}} 1.$$

In this way we conclude that in the circumstances at hand, one has $|F(\beta;P)| \ll \langle\beta\rangle^{-1/k}$, and this suffices to complete the proof of the lemma.

Before discussing the asymptotic behavior of the smooth Weyl sum $f(\alpha;P,R)$ for $\alpha \in \mathfrak{N}$, we require a technical lemma. It is useful in this context to write m_+ for the successor of the polynomial $m \in \mathbb{F}_q[t]$ when viewed according to the quasi-ordering on $\mathbb{F}_q[t]$, so that $m_+ = T_\xi(\langle m\rangle_\xi + 1)$ and $\langle m_+\rangle_\xi = \langle m\rangle_\xi + 1$.

Lemma 4.2. *Suppose that P and X are natural numbers with $1 \leqq X \leqq q\hat{P} - 1$. Then whenever $\beta \in \mathbb{T}$ satisfies $\langle\beta\rangle < \hat{P}^{1-k}$, one has*

$$\operatorname{card}\{m \in \mathbb{F}_q[t] : \langle m\rangle_\xi \leqq X \text{ and } e(\beta m^k) \neq e(\beta m_+^k)\} \ll 1 + \hat{P}^k\langle\beta\rangle. \tag{4.4}$$

Proof. There is at most one polynomial m counted on the left-hand side of (4.4) for which $\operatorname{ord} m_+ > P$, namely that with $\langle m\rangle_\xi = q\hat{P} - 1$, and its contribution is plainly accomodated by the right-hand side of (4.4). Consider then a polynomial m counted on the left-hand side of (4.4), and suppose that $\langle m\rangle_\xi < q\hat{P} - 1$. The situations in which $\operatorname{ord}\beta < -kP - 1$ may be disposed of at once. For whenever $\langle m\rangle_\xi \leqq X$, one has $\operatorname{ord}(\beta m^k) \leqq kP + \operatorname{ord}\beta < -1$. In view of our earlier assumption, a similar argument yields the bound $\operatorname{ord}(\beta m_+^k) < -1$, and thus we see that in the situation at hand one has $e(\beta m^k) = 1 = e(\beta m_+^k)$. The bound (4.4) is therefore trivial for $\operatorname{ord}\beta < -kP - 1$.

We are left to consider the situations in which $\langle\beta\rangle < \hat{P}^{1-k}$ and yet $\operatorname{ord}\beta \geqq -kP - 1$. In such circumstances, one has $\operatorname{ord}\beta = L$, with $L = N - kP - 1$ for some natural number N satisfying $0 \leqq N \leqq P$. We may write $\beta = \sum_{i \leqq L} b_i t^i$, where $b_i \in \mathbb{F}_q$ $(i \leqq L)$ and $b_L \neq 0$. Let r be a non-negative integer with $r \leqq P$, and consider the contribution on the left-hand side of (4.4) arising from those terms m with $\operatorname{ord} m = P - r$. If $r > N/k + 1$, then an argument paralleling that of the first paragraph establishes that $\operatorname{ord}(\beta m^k) < -1$ and $\operatorname{ord}(\beta m_+^k) < -1$, so that $e(\beta m^k) = 1 = e(\beta m_+^k)$. Such terms do not contribute to the left-hand side of (4.4), so we suppose instead that $r \leqq N/k + 1$. We may write $m = c_0 + c_1 t + \cdots + c_{P-r}t^{P-r}$, where $c_i \in \mathbb{F}_q$ $(0 \leqq i \leqq P - r)$ and $c_{P-r} \neq 0$. If $\operatorname{ord}(m_+) > \operatorname{ord}(m)$, then necessarily $c_i = \xi^{q-2}$ $(0 \leqq i \leqq P - r)$, so that m is uniquely determined. Otherwise, in view of our earlier observations, we may write $m_+ = c_0^+ + c_1^+ t + \cdots + c_{P-r}^+ t^{P-r}$, where $c_i^+ \in \mathbb{F}_q$ $(0 \leqq i \leqq P - r)$ and $c_{P-r}^+ \neq 0$. It then follows that m^k and m_+^k may be written in the form

$$m^k = \sum_{j=0}^{k(P-r)} a_j t^j \quad \text{and} \quad m_+^k = \sum_{j=0}^{k(P-r)} a_j^+ t^j, \tag{4.5}$$

where $a_j, a_j^+ \in \mathbb{F}_q$ $(0 \leqq j \leqq k(P-r))$. Put $M = P + r(k-1)$. Then a consideration of the multinomial expansion of m^k reveals that for $kr < u \leqq N$, one has

$$a_{kP-u} = kc_{M-u}c_{P-r}^{k-1} + \Omega_u(\boldsymbol{c}), \tag{4.6}$$

for some $\Omega_u(\boldsymbol{c}) \in \mathbb{F}_q[c_{M-u+1}, \dots, c_{P-r}]$. One also has $a_{kP-kr} = c_{P-r}^k$ and $a_{kP-u} = 0$ for $u < kr$. Similar relations hold for coefficients decorated with a superscript $+$.

It is apparent from (4.5) that

$$\operatorname{res}(\beta m^k) - \operatorname{res}(\beta m_+^k) = \sum_{i=kr}^{N} (a_{kP-i} - a_{kP-i}^+) b_{i-kP-1}.$$

Thus we see that when $e(\beta m^k) \neq e(\beta m_+^k)$, the relation $a_{kP-i} = a_{kP-i}^+$ cannot hold for every index i with $kr \leqq i \leqq N$. But it is a consequence of (4.6) that when $kr < w \leqq N$ and $c_{M-v} = c_{M-v}^+$ for $kr \leqq v < w$, and in addition $a_{kP-w} = a_{kP-w}^+$, then in fact $c_{M-w} = c_{M-w}^+$. When $e(\beta m^k) \neq e(\beta m_+^k)$ and $\operatorname{ord}(m_+) = \operatorname{ord}(m)$, therefore, one has $c_{M-v} \neq c_{M-v}^+$ for some index v with $kr \leqq v \leqq N$. In view of the definition of M, we thus conclude that $c_v \neq c_v^+$ for some index v with $P + r(k-1) - N \leqq v \leqq P - r$.

Now suppose that $e(\beta m^k) \neq e(\beta m_+^k)$, and let v denote the largest index with $P - N \leqq v \leqq P$ for which $c_v \neq c_v^+$. The polynomials m and m_+ take the forms

$$m = c_P t^P + \cdots + c_{v+1} t^{v+1} + \xi^s t^v + \xi^{q-2} t^{v-1} + \xi^{q-2} t^{v-2} + \cdots + \xi^{q-2}$$

and

$$m_+ = c_P t^P + \cdots + c_{v+1} t^{v+1} + \xi^{s+1} t^v,$$

where $s \in \{-\infty, 0, 1, \dots, q-3\}$ and $c_i \in \mathbb{F}_q$ $(v+1 \leqq i \leqq P)$. Here, if $v = P$, then we understand the last condition to be moot, and when $s = -\infty$, we interpret $s+1$ to be 0. In these circumstances, the number of available choices for s and $\boldsymbol{c}$ is $(q-1)q^{P-v}$. Summing over the available choices of v with $P - N \leqq v \leqq P$, we deduce that the total number of possible choices for m with $\langle m \rangle_\xi \leqq X$ and $e(\beta m^k) \neq e(\beta m_+^k)$ is at most $1 + q^{N+1} = 1 + q^{kP+2+\operatorname{ord}\beta}$, and the conclusion of the lemma follows at once.

We are now equipped to establish a major arc approximation to $f(\alpha; P, R)$.

Lemma 4.3. *Let P and R be positive numbers with $P \geqq 1$ and*

$$2P/\log(2P) < R < P - \log P.$$

Suppose that $\alpha \in \mathbb{T}$, that a and g are elements of $\mathbb{F}_q[t]$ with g monic and $(a, g) = 1$, and write $\beta = \alpha - a/g$. Then whenever $\langle g \rangle \leqq \hat{\boldsymbol{R}}$ and $\langle \beta \rangle < \hat{\boldsymbol{P}}^{1-k}$, one has

$$f(\alpha; P, R) - \langle g \rangle^{-1} S(g, a) \rho(P/R) F(\beta; P) \ll \langle g \rangle \hat{\boldsymbol{P}} (\log \hat{\boldsymbol{P}})^{-1/2} (1 + \hat{\boldsymbol{P}}^k \langle \beta \rangle).$$

Proof. Rather than tackling $f(\alpha; P, R)$ directly, we initially consider the sum

$$\tilde{f}_\xi(\alpha; X, Y) = \sum_{\substack{x \in \mathscr{A}_\xi(X, Y) \\ \langle x \rangle_\xi > Y}} e(\alpha x^k).$$

Recall (3.4) and suppose that X and Y are positive numbers with $1 \leqq Y < X$. Then by the inclusion-exclusion principle, one has

$$\sum_{\substack{x \in \mathscr{A}_\xi(X,Y) \\ x \equiv r \,(\mathrm{mod}\, g)}} 1 = \sum_{\substack{d \mid \Pi_q(X,Y) \\ \langle d \rangle_\xi \leqq X}}^{\dagger} \mu(d) \sum_{\substack{\langle m \rangle_\xi \leqq X \\ m \equiv r \,(\mathrm{mod}\, g) \\ d \mid m}} 1.$$

If $d \mid \Pi_q(X, Y)$ and both d and g are monic, it follows that when $\langle g \rangle_\xi \leqq Y$ one has $(g, d) = 1$. Recalling (3.5) and applying the Chinese Remainder Theorem in combination with Lemma 3.1, therefore, we deduce that

$$\begin{aligned} \sum_{\substack{x \in \mathscr{A}_\xi(X,Y) \\ x \equiv r \,(\mathrm{mod}\, g)}} 1 &= \sum_{\substack{d \mid \Pi_q(X,Y) \\ \langle d \rangle_\xi \leqq X}}^{\dagger} \mu(d)\big(X/\langle gd \rangle + O(1)\big) \\ &= \langle g \rangle^{-1} X \sum_{\substack{d \mid \Pi_q(X,Y) \\ \langle d \rangle_\xi \leqq X}}^{\dagger} \mu(d) \langle d \rangle^{-1} + E(X, Y). \end{aligned}$$

Applying Lemma 3.2 to both the latter formula and the case $g = 1$ of the same relation, we find that

$$\sum_{\substack{x \in \mathscr{A}_\xi(X,Y) \\ x \equiv r \,(\mathrm{mod}\, g)}} 1 = \langle g \rangle^{-1} \sum_{x \in \mathscr{A}_\xi(X,Y)} 1 + O\big(X/\log(2Y)\big),$$

whence

$$\sum_{x \in \mathscr{A}_\xi(X,Y)} e(ax^k/g) - \langle g \rangle^{-1} S(g, a) \sum_{x \in \mathscr{A}_\xi(X,Y)} 1 \ll \langle g \rangle X/\log(2Y). \tag{4.7}$$

When W is a positive number with $Y < W \leqq X$, write

$$\mathscr{S}(W) = \sum_{x \in \mathscr{A}_\xi(W,Y)} \big(e(ax^k/g) - \langle g \rangle^{-1} S(g, a)\big).$$

In these circumstances (4.7) yields the estimate $\mathscr{S}(W) = O\big(\langle g \rangle X/\log(2Y)\big)$, and so it follows by partial summation that

$$\begin{aligned} \sum_{\substack{x \in \mathscr{A}_\xi(X,Y) \\ \langle x \rangle_\xi > Y}} \big(e(\alpha x^k) - \langle g \rangle^{-1} S(g, a) e(\beta x^k)\big) &= \sum_{\substack{Y < W \leqq X \\ W = \langle x \rangle_\xi}} \mathscr{S}(W)\big(e(\beta x^k) - e(\beta x_+^k)\big) \\ &\quad + O\big(\langle g \rangle X/\log(2Y)\big). \end{aligned}$$

In view of the conclusion of Lemma 4.2, therefore, when $1 \leqq X \leqq q\hat{\boldsymbol{P}} - 1$ and $\langle \beta \rangle < \hat{\boldsymbol{P}}^{1-k}$, we have

$$\tilde{f}_\xi(\alpha; X, Y) - \langle g \rangle^{-1} S(g, a) \tilde{f}_\xi(\beta; X, Y) \ll \langle g \rangle X\big(\log(2Y)\big)^{-1}(1 + \hat{\boldsymbol{P}}^k \langle \beta \rangle). \tag{4.8}$$

On applying partial summation we obtain

$$\begin{aligned} \tilde{f}_\xi(\beta; X, Y) &= \sum_{\substack{Y < W \leqq X \\ W = \langle x \rangle_\xi}} \tilde{A}_\xi(W, Y)\big(e(\beta x^k) - e(\beta x_+^k)\big) \\ &\quad + \tilde{A}_\xi(X, Y) e\big(\beta T_\xi([X] + 1)^k\big) - \tilde{A}_\xi(Y, Y) e\big(\beta T_\xi([Y + 1])^k\big). \end{aligned}$$

Thus, on writing

$$\Upsilon_\xi(\beta;X,Y)=\sum_{\substack{Y<W\leqq X\\ W=\langle x\rangle_\xi}} W\big(e(\beta x^k)-e(\beta x_+^k)\big)$$
$$+Xe\big(\beta T_\xi([X]+1)^k\big)-Ye\big(\beta T_\xi([Y]+1)^k\big),$$

it follows from Lemmata 3.3 and 4.2 that when $1\leqq X\leqq q\hat{P}-1$, one has

$$\tilde{f}_\xi(\beta;X,Y)-\rho_q(X,Y)\Upsilon_\xi(\beta;X,Y)\ll X\big(\log(2Y)\big)^{-1}(1+\hat{P}^k\langle\beta\rangle). \tag{4.9}$$

We now put $X=q\hat{P}-1$ and $Y=2\hat{R}-1$. The hypotheses of the statement of the lemma then permit us to assume that $Y\ll\hat{P}(\log\hat{P})^{-1/2}$ and $\log Y\gg(\log\hat{P})^{1/2}$. But on recalling (2.3), a modicum of computation reveals that

$$\Upsilon_\xi(\beta;X,Y)=\sum_{\substack{Y<W\leqq X\\ W=\langle x\rangle_\xi}} e(\beta x^k)=F(\beta;P)+O\big(\hat{P}(\log\hat{P})^{-1/2}\big)$$

and

$$f(\alpha;P,R)=\sum_{x\in\mathscr{A}_\xi(X,Y)} e(\alpha x^k)=\tilde{f}_\xi(\alpha;X,Y)+O\big(\hat{P}(\log\hat{P})^{-1/2}\big).$$

Hence, by substituting (4.9) into (4.8), we deduce that

$$f(\alpha;P,R)-\langle g\rangle^{-1}S(g,a)\rho_q(q\hat{P}-1,2\hat{R}-1)F(\beta;P)\ll\langle g\rangle\hat{P}(\log\hat{P})^{-1/2}(1+\hat{P}^k\langle\beta\rangle),$$

and the conclusion of the lemma is now confirmed by recalling Lemma 3.4.

5. A lower bound for the major arc contribution

The sets $\mathfrak{N}(g,a;V)$ comprising $\mathfrak{N}$ are sufficiently sparse and narrow that the derivation of the asymptotic relation (2.9) is now essentially routine. In preparation for our proof of this formula, we introduce the *singular integral*

$$J_{s,k}(m)=\int_{\langle\beta\rangle<(q\hat{P})^{1-k}} F(\beta)^s e(-\beta m)\,d\beta, \tag{5.1}$$

and the *singular series*

$$\mathfrak{S}_{s,k}(m)=\sum_{g\in\mathbb{F}_q[t]}{}^{\dagger}\,\mathfrak{A}_s(g;m), \tag{5.2}$$

in which we have written

$$\mathfrak{A}_s(g;m)=\langle g\rangle^{-s}\sum_{\substack{\langle a\rangle<\langle g\rangle\\ (a,g)=1}} S(g,a)^s e(-ma/g). \tag{5.3}$$

Lemma 5.1. *Suppose that η and R are positive numbers with $\eta<1$ and $\eta P<R\leqq P-\log P$. Then whenever $s\geqq 2k+1$, one has $\mathfrak{S}_{s,k}(m)\ll 1$ and $J_{s,k}(m)\ll\hat{P}^{s-k}$, and furthermore*

$$\mathscr{R}_s(m;\mathfrak{N})-\rho(P/R)^{s-2}\mathfrak{S}_{s,k}(m)J_{s,k}(m)\ll\hat{P}^{s-k}\hat{V}^{-1/k}.$$

Proof. Define $F^*(\alpha)$ for $\alpha \in \mathfrak{N}$ by taking $F^*(\alpha) = \langle g\rangle^{-1} S(g,a) F(\beta)$ when $\alpha = \beta + a/g$ lies in $\mathfrak{N}(g,a;V) \subseteqq \mathfrak{N}$. Then for $\alpha \in \mathfrak{N}$, it follows from (2.8) and Lemma 4.1(i) that $F(\alpha) = F^*(\alpha)$, and from Lemma 4.3 that $f(\alpha) = \rho(P/R)F^*(\alpha) + O(\hat{P}\hat{V}^{-4})$. The bound

$$F(\alpha)^2 f(\alpha)^{s-2} - \rho(P/R)^{s-2} F^*(\alpha)^s \ll \hat{P}^s \hat{V}^{-4}$$

therefore holds uniformly for $\alpha \in \mathfrak{N}$. But the measure of $\mathfrak{N}$ is $O(\hat{V}^3 \hat{P}^{-k})$, and so

$$\int_{\mathfrak{N}} \big(F(\alpha)^2 f(\alpha)^{s-2} - \rho(P/R)^{s-2} F^*(\alpha)^s\big) e(-m\alpha)\, d\alpha \ll \hat{P}^{s-k} \hat{V}^{-1}. \tag{5.4}$$

Furthermore, from the definition of $\mathfrak{N}$, we have

$$\int_{\mathfrak{N}} F^*(\alpha)^s e(-m\alpha)\, d\alpha = \mathfrak{S}(m;V) J(m;V-kP), \tag{5.5}$$

where

$$J(m;W) = \int_{\langle\beta\rangle < \hat{W}} F(\beta)^s e(-\beta m)\, d\beta \quad \text{and} \quad \mathfrak{S}(m;W) = \sum_{\langle g\rangle \leqq \hat{W}}{}^{\dagger} \mathfrak{A}_s(g;m). \tag{5.6}$$

When $\hat{W} < (q\hat{P})^{1-k}$, it follows on combining (5.1) and (5.6), and then applying Lemma 4.1(ii), that one has the estimate

$$J_{s,k}(m) - J(m;W) \ll \hat{P}^s \int_{\langle\beta\rangle \geqq \hat{W}} (1 + \hat{P}^k \langle\beta\rangle)^{-s/k}\, d\beta.$$

But equation (3) of [14] shows that when $l \in \mathbb{Z}$, the measure of the set of points β in $\mathbb{T}$ with $\langle\beta\rangle < q^l$ is at most q^l. When $s \geqq k+1$, one therefore finds that

$$J(m;V-kP) - J_{s,k}(m) \ll \hat{P}^s \sum_{l=V-kP}^{\infty} q^{l+1}(1+q^{l+kP})^{-s/k} \ll \hat{P}^{s-k}\hat{V}^{-1/k}, \tag{5.7}$$

and with the same condition on s, a similar argument yields

$$J_{s,k}(m) \ll \hat{P}^s \int_{\langle\beta\rangle < (q\hat{P})^{1-k}} (1 + \hat{P}^k \langle\beta\rangle)^{-s/k}\, d\beta \ll \hat{P}^{s-k}. \tag{5.8}$$

Employing the conclusion of Lemma 4.1(iii) within (5.3), we next find that $\mathfrak{A}_s(g;m) \ll \langle g\rangle^{1-s/k}$. Then for $s \geqq 2k+1$, it follows from (5.2) and (5.6) that

$$\mathfrak{S}(m;V) - \mathfrak{S}_{s,k}(m) \ll \sum_{\langle g\rangle > \hat{V}}{}^{\dagger} \langle g\rangle^{1-s/k} \ll \sum_{h=V+1}^{\infty} (q^h)^{2-s/k} \ll \hat{V}^{-1/k}, \tag{5.9}$$

and with the same condition on s, a parallel argument leads to the estimate

$$\mathfrak{S}_{s,k}(m) \ll \sum_{g \in \mathbb{F}_q[t]}{}^{\dagger} \langle g\rangle^{1-s/k} \ll \sum_{h=0}^{\infty} (q^h)^{2-s/k} \ll 1. \tag{5.10}$$

Finally, on substituting (5.7) and (5.9) into (5.5), and then employing the estimates (5.8) and (5.10), we conclude that

$$\int_{\mathfrak{N}} F^*(\alpha)^s e(-m\alpha)\,d\alpha - \mathfrak{S}_{s,k}(m)J_{s,k}(m) \ll \hat{P}^{s-k}\hat{V}^{-1/k}.$$

The proof of the lemma is completed by reference to (5.4).

We show next that under mild hypotheses, the singular series is well-behaved.

Lemma 5.2. *Suppose that $m \in \mathbb{J}_q^k[t]$ and $s \geqq 2k+1$. Then $1 \ll \mathfrak{S}_{s,k}(m) \ll 1$.*

Proof. We suppose that $s \geqq 2k+1$ throughout the proof of this lemma[4]. Define the local density $\mathfrak{Q}_{\varpi,s}(m)$ associated with the completion $\mathbb{F}_q(t)_\varpi$ of $\mathbb{F}_q(t)$ by

$$\mathfrak{Q}_{\varpi,s}(m) = 1 + \sum_{h=1}^{\infty} \mathfrak{A}_s(\varpi^h; m).$$

Then the argument of the proof of [14], Lemma 23 shows that the infinite product $\prod_{\varpi} \mathfrak{Q}_{\varpi,s}(m)$ converges absolutely to $\mathfrak{S}_{s,k}(m)$. Next, let $M_s(g;m)$ denote the number of solutions of the congruence $x_1^k + \cdots + x_s^k \equiv m \pmod{g}$, with $\langle x_i\rangle < \langle g\rangle$ $(1 \leqq i \leqq s)$. Then the argument of the proof of [14], Theorem 29 establishes that

$$\mathfrak{Q}_{\varpi,s}(m) = \lim_{h\to\infty} \langle\varpi\rangle^{h(1-s)} M_s(\varpi^h; m),$$

that

$$|\mathfrak{Q}_{\varpi,s}(m) - 1| \ll \sum_{h=1}^{\infty} \langle\varpi^h\rangle^{-1-1/k} \ll \langle\varpi\rangle^{-1-1/k},$$

and also that whenever $m \in \mathbb{J}_q^k[t]$, then $\mathfrak{Q}_{\varpi,s}(m) \geqq \langle\varpi\rangle^{1-s}$. Under the latter hypothesis, therefore, we deduce that there is a large positive number $A = A(q,s,k)$ for which

$$\mathfrak{S}_{s,k}(m) \gg \prod_{\langle\varpi\rangle > A} (1 - \langle\varpi\rangle^{-1-1/(2k)})^{-1}. \tag{5.11}$$

But the number of monic irreducible polynomials of degree h is at most q^h/h (see [19], page 13), whence $\sum_{\varpi} \langle\varpi\rangle^{-1-1/(2k)} \leqq \sum_h (hq^{h/(2k)})^{-1} \ll 1$. Consequently, on extracting logarithms, one finds that the infinite product (5.11) converges, and that $\mathfrak{S}_{s,k}(m) \gg 1$. The proof of the lemma is completed on recalling the estimate $\mathfrak{S}_{s,k}(m) \ll 1$ provided by Lemma 5.1.

We remark that with additional effort, the condition $s \geqq 2k+1$ could be relaxed to the less severe constraint $s \geqq k+1$. Furthermore, as is implicit in [14], Theorem 29, one has $\mathbb{J}_q^k[t] = \mathbb{F}_q[t]$ when $\mathrm{ch}(\mathbb{F}_q) > k$. It is also a consequence of the work presented here together with the conclusion of [14], Theorem 29, that whenever m is congruent to a sum of kth

[4] In [14], Lemma 23, the condition $s \geqq 3k+1$ is imposed instead, apparently as a result of an oversight.

powers modulo ϖ for all irreducible polynomials ϖ satisfying $\langle \varpi \rangle \leqq (k-1)^2$, then in fact $m \in \mathbb{J}_q^k[t]$.

Next we turn our attention to the singular integral $J_{s,k}(m)$, the analysis of which is in many ways simpler than in the analogous situation for $\mathbb{Z}$.

Lemma 5.3. *Suppose that $s \geqq k+1$. Then $\hat{P}^{s-k} \ll J_{s,k}(m) \ll \hat{P}^{s-k}$.*

Proof. Suppose that the leading coefficient of the polynomial m is $c(m)$. We define $b = b(m)$ to be $c(m)$ when k divides $\operatorname{ord} m$ and m is not exceptional, and otherwise we set $b(m)$ to be 0. In addition, we write $J_\infty(m) = J_\infty(m;q)$ for the number of solutions of the equation $x_1^k + \cdots + x_s^k = b$ with $\boldsymbol{x} \in \mathbb{F}_q^s \backslash \{\mathbf{0}\}$. Then it follows from [14], Lemma 17, that whenever $s \geqq k+1$, one has

$$J_{s,k}(m) = J_\infty(m)\hat{P}^{s-k} + O(\hat{P}^{s-k-1/k}), \tag{5.12}$$

and moreover that $1 \leqq J_\infty(m) \ll 1$. In order to confirm this assertion, one observes that the integration in (5.1) is over $\beta \in \mathbb{T}$ with $\operatorname{ord}\beta < -(k-1)(P+1)$, and further that $(k-1)(P+1) \leqq \operatorname{ord} m$, except possibly when $P \leqq 2k-1$. One may therefore apply [14], Lemma 17 with $m = P+1$ and $m' = (k-1)(P+1)$, and when P is large enough in terms of k it is only the cases (a) and (b) of this lemma that are relevant[5]. We note that when $b(m) \neq 0$, the lower bound $J_\infty(m) \geqq 1$ may be confirmed by following the argument of the proof of [14], Lemma 27. We remark that the same conclusion as above is implicit in Car [2], Proposition 9, and also that the conclusion of [14], Theorem 18 differs from what would be anticipated based on (5.12), owing to some oversights in the argument of [14].

On observing that when $\eta > 0$ and $R > \eta P$, one has $\rho(P/R) \gg 1$, we may combine Lemmata 5.1, 5.2 and 5.3 to obtain the following conclusion.

Lemma 5.4. *Suppose that η and R are positive numbers with $\eta < 1$ and $\eta P < R \leqq P - \log P$. Then whenever $m \in \mathbb{J}_q^k[t]$ and $s \geqq 2k+1$, one has $\mathscr{R}_s(m;\mathfrak{N}) \gg \hat{P}^{s-k}$.*

6. Pruning technology

The minor arc estimates that we obtain in §13 are insufficient to bound directly the quantity $\mathscr{R}_s(m;\mathfrak{n})$ defined in (2.5), and thus we are forced to employ pruning techniques to bridge the gap. In this context, we write $\mathfrak{P}$ for $\mathfrak{M}(P)$ and $\mathfrak{p}$ for $\mathfrak{m}(P)$, and we say that a positive number $u > 2k-2$ is *accessible to the exponent k* when there exists a positive number δ for which

$$\int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^u| \, d\alpha \ll \hat{P}^{u+2-k-\delta}. \tag{6.1}$$

Our goal in this section is to show that whenever u is accessible to the exponent k, and s is an even integer with $s - 2 \geqq u$, then

$$\int_{\mathfrak{n}} |F(\alpha)^2 f(\alpha)^{s-2}| \, d\alpha = o(\hat{P}^{s-k}). \tag{6.2}$$

[5] We emphasise that m and m' are integers in this context.

This estimate plainly implies that $\mathscr{R}_s(m;\mathfrak{n}) = o(\hat{\boldsymbol{P}}^{s-k})$, a bound required in the discussion concluding §2, and thus the focus of later sections is the pursuit of bounds of the shape (6.1).

We begin by analysing mean values of classical Weyl sums.

Lemma 6.1. *Whenever $u \geqq 2k+1$, one has*

$$\int_{\mathfrak{P}} |F(\alpha)|^u \, d\alpha \ll \hat{\boldsymbol{P}}^{u-k}.$$

Proof. Suppose that $\alpha \in \mathfrak{P}$, so that for some $a, g \in \mathbb{F}_q[t]$ with g monic, $0 \leqq \langle a \rangle < \langle g \rangle \leqq \hat{\boldsymbol{P}}$ and $(a,g) = 1$, one has $\alpha \in \mathfrak{M}(g,a;P)$. Making use of the definition of $\mathfrak{M}(g,a;P)$ together with Lemma 4.1, we find that

$$F(\alpha) \ll \hat{\boldsymbol{P}} \langle g \rangle^{-1/k} (1 + \hat{\boldsymbol{P}}^k \langle \alpha - a/g \rangle)^{-1/k}. \tag{6.3}$$

Consequently, one has

$$\int_{\mathfrak{P}} |F(\alpha)|^u \, d\alpha \ll \hat{\boldsymbol{P}}^u T_1 T_2, \tag{6.4}$$

where

$$T_1 = \sideset{}{^\dagger}\sum_{g \in \mathbb{F}_q[t]} \sum_{\substack{\langle a \rangle < \langle g \rangle \\ (a,g)=1}} \langle g \rangle^{-u/k} \quad \text{and} \quad T_2 = \int_{\langle \beta \rangle < \hat{\boldsymbol{P}}^{1-k}} (1 + \hat{\boldsymbol{P}}^k \langle \beta \rangle)^{-u/k} \, d\beta.$$

Since the number of monic polynomials $g \in \mathbb{F}_q[t]$ with $\langle g \rangle = q^l$ is equal to q^l, we see that whenever $u \geqq 2k+1$, one has

$$T_1 \leqq \sideset{}{^\dagger}\sum_{g \in \mathbb{F}_q[t]} \langle g \rangle^{1-u/k} \leqq \sum_{h=0}^{\infty} (q^h)^{2-u/k} \ll 1. \tag{6.5}$$

Meanwhile, observing next that the measure of the set of points β in $\mathbb{T}$ with $\langle \beta \rangle = q^l$ is at most q^{l+1}, we deduce that

$$\begin{aligned} T_2 &\leqq \int_{\langle \beta \rangle < \hat{\boldsymbol{P}}^{-k}} d\beta + \int_{\langle \beta \rangle \geqq \hat{\boldsymbol{P}}^{-k}} (1 + \hat{\boldsymbol{P}}^k \langle \beta \rangle)^{-u/k} \, d\beta \\ &\leqq \hat{\boldsymbol{P}}^{-k} + \sum_{l=-kP}^{\infty} q^{l+1} (1 + q^{l+kP})^{-u/k} \\ &\ll \hat{\boldsymbol{P}}^{-k} + \hat{\boldsymbol{P}}^{-k} \sum_{h=0}^{\infty} q^{h(1-u/k)}. \end{aligned}$$

When $u \geqq k+1$, it therefore follows that $T_2 = O(\hat{\boldsymbol{P}}^{-k})$. The conclusion of the lemma follows on substituting this estimate together with (6.5) into (6.4).

Next we leverage control on the major arcs of mean values involving $F(\alpha)$ into control of mixed mean values involving also $f(\alpha)$.

Lemma 6.2. *Suppose that $u > 2k-2$ is accessible to the exponent k, and that v is an integer with $2v \geqq u$. Then we have*

$$\int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha \ll \hat{P}^{2v+2-k}. \tag{6.6}$$

Proof. When $\mathscr{B}$ is a measurable subset of $\mathbb{T}$, write

$$I(\mathscr{B}) = \int_{\mathscr{B}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha.$$

Then by applying Hölder's inequality, we obtain

$$I(\mathbb{T}) = I(\mathfrak{p}) + I(\mathfrak{P}) \ll I(\mathfrak{p}) + I_1^{1/(v+1)} I_2^{v/(v+1)}, \tag{6.7}$$

where we write

$$I_1 = \int_{\mathfrak{P}} |F(\alpha)|^{2v+2}\, d\alpha \quad \text{and} \quad I_2 = \int_{\mathbb{T}} |f(\alpha)|^{2v+2}\, d\alpha.$$

Since $2v+2$ is even, the integral I_2 counts the number of solutions of the equation

$$\sum_{i=1}^{v+1} (x_i^k - y_i^k) = 0,$$

with $x_i, y_i \in \mathscr{A}(P,R)$ $(1 \leqq i \leqq v+1)$. An upper bound for I_2 is therefore provided by permitting x_1 and y_1 to be any elements of $\mathbb{F}_q[t]$ with $\langle x_1 \rangle \leqq \hat{P}$ and $\langle y_1 \rangle \leqq \hat{P}$, whence

$$I_2 \leqq \int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha = I(\mathbb{T}).$$

It therefore follows from (6.7) that

$$I(\mathbb{T}) \ll I(\mathfrak{p}) + I_1. \tag{6.8}$$

But by hypothesis u is accessible to the exponent k, and $2v \geqq u$. Hence, on employing the trivial estimate $|F(\alpha)| = O(\hat{P})$, we find that there is a positive number δ for which $I(\mathfrak{p}) = O(\hat{P}^{2v+2-k-\delta})$. From Lemma 6.1, moreover, we have $I_1 = O(\hat{P}^{2v+2-k})$. We therefore deduce from (6.8) that $I(\mathbb{T}) = O(\hat{P}^{2v+2-k})$. This confirms (6.6), and so the proof of the lemma is complete.

We next show that in the mean value crucial to our application, the contribution of the arcs $\mathfrak{P}\backslash\mathfrak{N}$ is of smaller order than the expected main term.

Lemma 6.3. *Suppose that $u > 2k-2$ is accessible to the exponent k, and that s is an even integer with $s \geqq u+2$. Then we have*

$$\int_{\mathfrak{P}\backslash\mathfrak{N}} |F(\alpha)^2 f(\alpha)^{s-2}|\, d\alpha \ll \hat{P}^{s-k} \hat{V}^{-2/(ks)}.$$

Proof. An application of Hölder's inequality reveals that

$$\int_{\mathfrak{P}\setminus\mathfrak{N}} |F(\alpha)^2 f(\alpha)^{s-2}|\, d\alpha \leqq J_1^{1-2/s} J_2^{2/s}, \tag{6.9}$$

where

$$J_1 = \int_{\mathbb{T}} |f(\alpha)|^s\, d\alpha \quad \text{and} \quad J_2 = \int_{\mathfrak{P}\setminus\mathfrak{N}} |F(\alpha)|^s\, d\alpha. \tag{6.10}$$

But s is even, so that on considering the underlying equation we find that

$$J_1 \leqq \int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{s-2}|\, d\alpha.$$

Since $s-2 \geqq u$ and u is accessible to the exponent k, the upper bound $J_1 = O(\hat{P}^{s-k})$ therefore follows from Lemma 6.2.

In order to tackle J_2 we observe first that when $\alpha \in \mathfrak{M}(g,a;P) \subseteqq \mathfrak{P}$, it follows as in (6.3) that

$$F(\alpha) \ll \hat{P}(\langle g\rangle + \hat{P}^k \langle g\alpha - a\rangle)^{-1/k}.$$

But if $\alpha \in \mathfrak{P}\setminus\mathfrak{N}$, one necessarily has either $\langle g\rangle > \hat{V}$ or $\langle g\alpha - a\rangle > \hat{V}\hat{P}^{-k}$, whence $F(\alpha) \ll \hat{P}\hat{V}^{-1/k}$. Note that the hypotheses of the lemma ensure that $s \geqq 2k+2$. Then on substituting our estimate for $F(\alpha)$ into (6.10), we deduce from Lemma 6.1 that

$$J_2 \ll \hat{P}\hat{V}^{-1/k} \int_{\mathfrak{P}} |F(\alpha)|^{s-1}\, d\alpha \ll \hat{P}^{s-k}\hat{V}^{-1/k}.$$

The conclusion of the lemma follows on substituting the latter bound together with our earlier bound for J_1 into (6.9).

Since $\mathfrak{n} = \mathfrak{p} \cup (\mathfrak{P}\setminus\mathfrak{N})$, the estimate (6.2) follows on combining the conclusion of Lemma 6.3 with (6.1). We finish this section by collecting together the conclusions of Lemmata 5.4 and 6.3 to obtain the following lemma.

Lemma 6.4. *Suppose that η and R are positive numbers with $\eta < 1$ and $\eta P < R \leqq P - \log P$. Suppose also that $u > 2k-2$ is accessible to the exponent k, and that s is an even integer with $s \geqq u+2$. Then whenever $m \in \mathbb{J}_q^k[t]$, one has $\mathscr{R}_s(m;\mathfrak{P}) \gg \hat{P}^{s-k}$.*

7. The fundamental lemma for smooth Weyl sums

The goal of the next three sections is to derive, for natural numbers s, upper bounds for the mean values

$$S_s(P,R) = \int_{\mathbb{T}} |f(\alpha;P,R)|^{2s}\, d\alpha. \tag{7.1}$$

By orthogonality, the mean value $S_s(P,R)$ counts the number of solutions of the equation

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k, \tag{7.2}$$

with $x_i, y_i \in \mathscr{A}(P,R)$ $(1 \leqq i \leqq s)$. We estimate $S_s(P,R)$ via the iterative method introduced by Vaughan [22], in the variant permitting repeated efficient differencing established by the second author [27]. As in [22] and [27], our first step is a fundamental (auxiliary) lemma, and here we model our approach on that of [27]. Aside from leading to considerably sharper estimates, the latter also permits one to replace two smooth Weyl sums in (7.1) by corresponding classical Weyl sums, hence simplifying considerably the major arc analysis discussed above.

Before proceeding further, it is convenient to have available two technical lemmata that provide basic estimates of use in our subsequent deliberations. When $g \in \mathbb{F}_q[t]$, we denote by $s_0(g)$ the squarefree kernel of g, which is to say $s_0(g) = \prod_{\varpi \mid g} \varpi$. In addition, when L is a positive number, we define the set $\mathscr{C}_g(L)$ by

$$\mathscr{C}_g(L) = \{y \in \mathbb{F}_q[t] : y \text{ is monic}, \langle y\rangle \leqq \hat{L} \text{ and } s_0(y) \mid s_0(g)\}.$$

Lemma 7.1. *Let ε and A be fixed positive numbers. Then whenever $g \in \mathbb{F}_q[t]$, and L is a positive number for which $\langle g\rangle \leqq \hat{L}^A$, one has* $\operatorname{card}\big(\mathscr{C}_g(L)\big) \ll \hat{L}^{\varepsilon}$.

Proof. Observe first that there is no loss of generality in supposing that $\operatorname{ord} g \geqq 5$, for otherwise we may replace g by g^5 without adversely affecting the desired conclusions. Next, from the definition of $\mathscr{C}_g(L)$, one has

$$\operatorname{card}\big(\mathscr{C}_g(L)\big) \leqq \sum_{s_0(y) \mid s_0(g)} (\hat{L}/\langle y\rangle)^{\varepsilon} \leqq \hat{L}^{\varepsilon} \prod_{\varpi \mid g} (1 - \langle \varpi\rangle^{-\varepsilon})^{-1}. \tag{7.3}$$

Write $\psi(g)$ for $2^{1/\varepsilon} \log\langle g\rangle / \log\log\langle g\rangle$. We divide the product on the right-hand side of (7.3) according to the size of $\langle \varpi\rangle$. On the one hand,

$$\prod_{\substack{\varpi \mid g \\ \langle \varpi\rangle \leqq \psi(g)}} (1 - \langle \varpi\rangle^{-\varepsilon})^{-1} \leqq \prod_{\langle \varpi\rangle \leqq \psi(g)} (1 - q^{-\varepsilon})^{-1} \leqq \exp\big(-q \log(1 - q^{-\varepsilon}) \psi(g)\big).$$

On the other hand, since the number of monic irreducible divisors of g having degree exceeding $\log_q \psi(g)$ cannot exceed $(\operatorname{ord} g)/\big(\log_q \psi(g)\big)$, one has

$$\prod_{\substack{\varpi \mid g \\ \langle \varpi\rangle > \psi(g)}} (1 - \langle \varpi\rangle^{-\varepsilon})^{-1} \leqq \prod_{\substack{\varpi \mid g \\ \langle \varpi\rangle > \psi(g)}} 2 \leqq \exp\big(\log_q \langle g\rangle / \log_q \psi(g)\big).$$

On substituting the latter estimates into (7.3), we find that there is a positive number $B = B(q,\varepsilon)$ for which

$$\operatorname{card}\big(\mathscr{C}_g(L)\big) \leqq \hat{L}^{\varepsilon} \exp(B \log\langle g\rangle / \log\log\langle g\rangle) \ll \hat{L}^{2\varepsilon},$$

thereby confirming the conclusion of the lemma.

Write $\omega(g)$ for the number of distinct monic irreducible polynomials dividing g, and write $d_k(g)$ for the number of ways of writing g in the form $g = c g_1 \dots g_k$, with $c \in \mathbb{F}_q$, and with $g_i \in \mathbb{F}_q[t]$ $(1 \leqq i \leqq k)$ monic.

Corollary 7.2. *For each $k \in \mathbb{N}$, one has $d_k(g) \ll \langle g\rangle^{\varepsilon}$ and $k^{\omega(g)} \ll \langle g\rangle^{\varepsilon}$.*

Proof. The desired estimates follow at once from Lemma 7.1 on noting that, from the definition of $\mathscr{C}_g(L)$, one has $k^{\omega(g)} \leqq d_k(g) \ll \big(\mathscr{C}_g(\operatorname{ord} g)\big)^{k-1}$.

It is convenient also to have available a crude lower bound for $\operatorname{card}\big(\mathscr{A}(P,R)\big)$.

Lemma 7.3. *Suppose that R and P are positive numbers with $P \geqq 1$ and $R > P/\log(2P)$. Then* $\operatorname{card}\big(\mathscr{A}(P,R)\big) \gg \hat{P}^{1-\varepsilon}$.

Proof. Since for a fixed value of P, the cardinality of $\mathscr{A}(P,R)$ is an increasing function of R, there is no loss of generality in supposing that $R = P/\log(2P)$. By suitably adjusting the implicit constant in the lower bound supplied by the conclusion of the lemma, moreover, we may also suppose that P and R each exceed 6. Observe next that the cardinality of $\mathscr{A}(P,R)$ is equal to $q-1$ times the number of non-negative integral solutions $\boldsymbol{z}$ of the inequality

$$\sum_{\operatorname{ord}\varpi \leqq R} z_\varpi \operatorname{ord}\varpi \leqq P.$$

From [19], page 13, the number of monic irreducible polynomials of degree $[R]$ is at least $(q^{R-1} - 2q^{R/2})/R \geqq q^{R-2}/R$. Thus we find that $\operatorname{card}\big(\mathscr{A}(P,R)\big) \geqq Z(N,U)$, where $Z(N,U)$ denotes the number of non-negative integral solutions $\boldsymbol{u}$ of the inequality $u_1 + \cdots + u_N \leqq U$, with $N = [q^{R-2}/R]$ and $U = [P/R]$. But then $Z(N,U)$ is equal to the number of non-negative integral solutions $\boldsymbol{u}$ of the equation $u_0 + u_1 + \cdots + u_N = U$, and by [23], §1.5, Exercise 1, we therefore have $Z(N,U) = (N+U)!/(N!U!)$. In view of our assumption that $R = P/\log(2P)$, an application of Stirling's formula reveals that

$$\begin{aligned}\log Z(N,U) &\geqq N\log(1+U/N) + U\log(1+N/U) + O\big(\log(2U)\big)\\ &= P\log q - \big(\log(2P)\big)^2 + O\big(\log(2P)\big),\end{aligned}$$

whence for large values of P one obtains

$$\operatorname{card}\big(\mathscr{A}(P,R)\big) \geqq \hat{P}\exp\big(-2(\log\log\hat{P})^2\big) \gg \hat{P}^{1-\varepsilon}.$$

This completes the proof of the lemma.

We now advance to describe the fundamental lemma that underlies our efficient differencing method. This entails the introduction of some notation. Let P, Q, R be positive numbers with $1 \leqq R \leqq Q \leqq P$. Also, let r be a non-negative integer, and let C_i, C_i' be real numbers with $0 \leqq C_i' \leqq C_i \leqq P$ $(1 \leqq i \leqq r)$. We consider a subset $\mathscr{C}$ of polynomials $\boldsymbol{c}$ whose degrees lie in the box $[C_1', C_1] \times \cdots \times [C_r', C_r]$. For the sake of concision we write $\tilde{C}_j$ for the product $\hat{C}_1\hat{C}_2\ldots\hat{C}_j$, we write $\tilde{C}_j'$ for $\hat{C}_1'\hat{C}_2'\ldots\hat{C}_j'$, and we do likewise, in the obvious fashion, for other sets of parameters. We interpret an empty product of the latter type to be unity. Consider next a polynomial $\Psi(z;\boldsymbol{c})$ in the variables $z, c_1, \ldots, c_r$ of degree at least one in terms of z, having coefficients in $\mathbb{F}_q[t]$, and write $\Psi'(z;\boldsymbol{c})$ for $(\partial\Psi/\partial z)(z;\boldsymbol{c})$. We suppose throughout that s is a non-negative integer.

We denote by $S_s(P,Q,R) = S_s(P,Q,R;\Psi;\mathscr{C})$ the number of solutions of the equation

$$\Psi(z;\boldsymbol{b}) - \Psi(w;\boldsymbol{c}) = \sum_{j=1}^{s}(x_j^k - y_j^k), \tag{7.4}$$

with

$$x_j, y_j \in \mathscr{A}(Q,R) \quad (1 \leqq j \leqq s), \tag{7.5}$$

$$\langle z\rangle, \langle w\rangle \leqq \hat{\boldsymbol{P}} \quad \text{and} \quad \boldsymbol{b}, \boldsymbol{c} \in \mathscr{C}. \tag{7.6}$$

Here we adopt the convention that if $s = 0$, then the right-hand side of (7.4) is replaced by 0. Next, given a real number θ with $1 \leqq \hat{\boldsymbol{P}}^\theta < Q$, we define $T_s(P,Q,R;\theta) = T_s(P,Q,R;\theta;\Psi;\mathscr{C})$ to be the number of solutions of the equation

$$\Psi(z;\boldsymbol{c}) - \Psi(w;\boldsymbol{c}) = m^k \sum_{j=1}^{s} (u_j^k - v_j^k), \tag{7.7}$$

with z, w, $\boldsymbol{c}$ as in (7.6), and with

$$m \text{ monic} \quad \text{and} \quad \hat{\boldsymbol{P}}^\theta < \langle m\rangle \leqq \min\{\hat{\boldsymbol{Q}}, \hat{\boldsymbol{P}}^\theta \hat{\boldsymbol{R}}\}, \tag{7.8}$$

$$u_j, v_j \in \mathscr{A}(Q - \theta P, R) \quad (1 \leqq j \leqq s), \tag{7.9}$$

$$z \equiv w \pmod{m^k}. \tag{7.10}$$

Finally, we write $N_s(P,Q,R) = N_s(P,Q,R;\Psi;\mathscr{C})$ for the number of solutions of the equation (7.4) subject to (7.5) and (7.6) for which $\Psi'(z;\boldsymbol{b}) = \Psi'(w;\boldsymbol{c}) = 0$.

Lemma 7.4. *Suppose that $\theta = \theta(s,k;\Psi)$ satisfies the constraint $0 < \theta P < Q$. Then whenever s is a natural number, one has*

$$\begin{aligned} S_s(P,Q,R) \ll S_s(P,\theta P,R) + N_s(P,Q,R) + \hat{\boldsymbol{Q}}\hat{\boldsymbol{P}}^{\theta+\varepsilon} S_{s-1}(P,Q,R) \\ + \hat{\boldsymbol{P}}^{\varepsilon} \tilde{\boldsymbol{C}}_r (\hat{\boldsymbol{P}}^\theta \hat{\boldsymbol{R}})^{2s-1} T_s(P,Q,R;\theta). \end{aligned} \tag{7.11}$$

Proof. We divide the solutions of (7.4) counted by $S_s(P,Q,R)$ into four classes, and seek to establish that the contribution from each class is majorised by one of the terms on the right-hand side of (7.11). In order to describe our classification of these solutions, it is useful to introduce a notion modifying that of a divisor in a special way. When L is a positive number, we write $x\mathscr{D}(L)y$ when there is a divisor w of x with $\langle w\rangle \leqq \hat{\boldsymbol{L}}$ such that x/w is monic and has all of its irreducible factors amongst those of y.

Let S_1 denote the number of solutions of (7.4) satisfying (7.5) and (7.6) such that

$$\min\{\langle x_j\rangle, \langle y_j\rangle\} \leqq \hat{\boldsymbol{P}}^\theta \tag{7.12}$$

for some j with $1 \leqq j \leqq s$; let S_2 denote the number for which

$$\Psi'(z;\boldsymbol{b}) = 0 \quad \text{or} \quad \Psi'(w;\boldsymbol{c}) = 0; \tag{7.13}$$

let S_3 denote the number for which $\min\{\langle x_j\rangle, \langle y_j\rangle\} > \hat{\boldsymbol{P}}^\theta$ for $1 \leqq j \leqq s$, the condition (7.13) does not hold, and such that for some j with $1 \leqq j \leqq s$ one has

$$x_j \mathscr{D}(\theta P)\Psi'(z;\boldsymbol{b}) \quad \text{or} \quad y_j \mathscr{D}(\theta P)\Psi'(w;\boldsymbol{c}); \tag{7.14}$$

and let S_4 denote the number for which $\min\{\langle x_j\rangle, \langle y_j\rangle\} > \hat{P}^\theta$ for $1 \leqq j \leqq s$, the condition (7.13) does not hold, and such that (7.14) holds for no j with $1 \leqq j \leqq s$. Then

$$S_s(P, Q, R) \leqq 4 \max\{S_1, S_2, S_3, S_4\}. \tag{7.15}$$

We divide into cases.

(i) Suppose that $S_1 \geqq \max\{S_2, S_3, S_4\}$, so that from (7.15) one has $S_s(P, Q, R) \leqq 4S_1$. Define $G(\alpha; P) = G(\alpha; P; \mathscr{C})$ by

$$G(\alpha; P) = \sum_{z, \boldsymbol{b}} e\big(\alpha \Psi(z; \boldsymbol{b})\big),$$

where the summation is over z and $\boldsymbol{b}$ satisfying (7.6). Then on recalling (2.3), it is apparent from (7.12) that

$$S_1 \ll \int_{\mathbb{T}} |G(\alpha; P)^2 f(\alpha; \theta P, R) f(\alpha; Q, R)^{2s-1}| \, d\alpha.$$

By Hölder's inequality, one therefore has

$$S_s(P, Q, R) \ll \big(S_s(P, \theta P, R)\big)^{1/(2s)} \big(S_s(P, Q, R)\big)^{1-1/(2s)},$$

and so the upper bound (7.11) holds in the first case.

(ii) Suppose that $S_2 \geqq \max\{S_1, S_3, S_4\}$, so that from (7.15) one has $S_s(P, Q, R) \leqq 4S_2$. Now define $\tilde{G}(\alpha; P) = \tilde{G}(\alpha; P; \mathscr{C})$ by

$$\tilde{G}(\alpha; P) = \sum_{z, \boldsymbol{b}} e\big(\alpha \Psi(z; \boldsymbol{b})\big),$$

where the summation is over z and $\boldsymbol{b}$ satisfying (7.6) and the first condition of (7.13). Then we see that

$$S_2 \ll \int_{\mathbb{T}} |\tilde{G}(\alpha; P) G(\alpha; P) f(\alpha; Q, R)^{2s}| \, d\alpha.$$

By Schwarz's inequality, therefore, we have

$$S_s(P, Q, R) \ll \big(N_s(P, Q, R)\big)^{1/2} \big(S_s(P, Q, R)\big)^{1/2},$$

and so (7.11) holds also in the second case.

(iii) Suppose that $S_3 \geqq \max\{S_1, S_2, S_4\}$, so that from (7.15) one has

$$S_s(P, Q, R) \leqq 4S_3.$$

Given z and $\boldsymbol{b}$ satisfying (7.6) with $\Psi'(z; \boldsymbol{b}) \neq 0$, denote by $\mathscr{L}(z; \boldsymbol{b})$ the set of polynomials x for which $\langle x\rangle \leqq \hat{Q}$, and such that x has a divisor v with $\langle v\rangle \leqq \hat{P}^\theta$ with the property that x/v is monic and has all of its irreducible factors amongst those of $\Psi'(z; \boldsymbol{b})$. Define the exponential sum $H(\alpha; P, Q) = H(\alpha; P, Q; \mathscr{C})$ by

$$H(\alpha; P, Q) = \sum_{z, \boldsymbol{b}} \sum_{x \in \mathscr{L}(z; \boldsymbol{b})} e\big(\alpha\big(x^k + \Psi(z; \boldsymbol{b})\big)\big),$$

where the first summation is over z and $\boldsymbol{b}$ satisfying (7.6) subject to the condition that $\Psi'(z;\boldsymbol{b}) \neq 0$. Then

$$S_3 \ll \int_{\mathbb{T}} |H(\alpha;P,Q)G(\alpha;P)f(\alpha;Q,R)^{2s-1}|\,d\alpha,$$

so that by Schwarz's inequality,

$$S_3 \ll \big(S_s(P,Q,R)\big)^{1/2}\bigg(\int_{\mathbb{T}} |H(\alpha;P,Q)^2 f(\alpha;Q,R)^{2s-2}|\,d\alpha\bigg)^{1/2}.$$

It therefore follows from orthogonality that

$$S_s(P,Q,R) \ll \sum_{g,g'} V(g,g'), \tag{7.16}$$

where we write $V(g,g')$ for the number of solutions of the equation

$$\Psi(z;\boldsymbol{b}) + m^k x^k + x_1^k + \cdots + x_{s-1}^k = \Psi(w;\boldsymbol{c}) + n^k y^k + y_1^k + \cdots + y_{s-1}^k,$$

with z, w, $\boldsymbol{b}$, $\boldsymbol{c}$ satisfying (7.6), with x_j and y_j satisfying (7.5) for $1 \leqq j \leqq s-1$, and with

$$\Psi'(z;\boldsymbol{b}) \neq 0, \quad \Psi'(w;\boldsymbol{c}) \neq 0, \quad g \,|\, \Psi'(z;\boldsymbol{b}), \quad g' \,|\, \Psi'(w;\boldsymbol{c}), \quad \langle m\rangle \leqq \hat{\boldsymbol{P}}^\theta, \quad \langle n\rangle \leqq \hat{\boldsymbol{P}}^\theta,$$
$$x, y \text{ monic}, \quad \langle x\rangle \leqq \hat{\boldsymbol{Q}}\langle m\rangle^{-1}, \quad \langle y\rangle \leqq \hat{\boldsymbol{Q}}\langle n\rangle^{-1}, \quad s_0(x) = g, \quad s_0(y) = g'.$$

Now define $G_g(\alpha;P) = G_g(\alpha;P;\mathscr{C})$ by putting

$$G_g(\alpha;P) = \sum_{z,\boldsymbol{b}} e\big(\alpha\Psi(z;\boldsymbol{b})\big),$$

where the summation is over z and $\boldsymbol{b}$ satisfying (7.6), and subject to the conditions $\Psi'(z;\boldsymbol{b}) \neq 0$ and $g \,|\, \Psi'(z;\boldsymbol{b})$. Let δ be the total degree of Ψ. Then since $\langle z\rangle \leqq \hat{\boldsymbol{P}}$ and $\hat{C}_i \leqq \hat{\boldsymbol{P}}$ $(1 \leqq i \leqq r)$, we have $\langle \Psi'(z;\boldsymbol{b})\rangle \leqq \hat{\boldsymbol{P}}^\delta$. It therefore follows from (7.16) that

$$S_s(P,Q,R) \ll \int_{\mathbb{T}} |\mathscr{G}(\alpha)^2 f(\alpha;Q,R)^{2s-2}|\,d\alpha, \tag{7.17}$$

where we write

$$\mathscr{G}(\alpha) = \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^\delta} G_g(\alpha;P) \sum_{\langle m\rangle \leqq \hat{\boldsymbol{P}}^\theta} {\sum_{\langle x\rangle \leqq \hat{\boldsymbol{Q}}\langle m\rangle^{-1}}}^{\dagger} e(\alpha m^k x^k). \tag{7.18}$$
$$s_0(x)=g$$

Here, if g is not squarefree, we understand the third summation of (7.18) to be empty.

We now apply Cauchy's inequality to (7.18), obtaining the upper bound

$$|\mathscr{G}(\alpha)|^2 \leqq \mathscr{M} \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^\delta} |G_g(\alpha;P)|^2, \tag{7.19}$$

where

$$\mathscr{M} = \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^\delta} \bigg| \sum_{\langle m\rangle \leqq \hat{\boldsymbol{P}}^\theta} {\sum_{\langle x\rangle \leqq \hat{\boldsymbol{Q}}\langle m\rangle^{-1}}}^{\dagger} e(\alpha m^k x^k) \bigg|^2.$$
$$s_0(x)=g$$

Interchanging the order of summation in the last expression, and then applying Cauchy's inequality in combination with Lemma 7.1, we deduce that

$$\mathscr{M} = \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^{\delta}} \Bigg| \sideset{}{^{\dagger}}\sum_{\substack{\langle x\rangle \leqq \hat{\boldsymbol{Q}} \\ s_0(x)=g}} \sum_{\substack{\langle m\rangle \leqq \hat{\boldsymbol{P}}^{\theta} \\ \langle m\rangle \leqq \hat{\boldsymbol{Q}}\langle x\rangle^{-1}}} e(\alpha m^k x^k) \Bigg|^2$$

$$\ll \hat{\boldsymbol{P}}^{\varepsilon} \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^{\delta}} \sideset{}{^{\dagger}}\sum_{\substack{\langle x\rangle \leqq \hat{\boldsymbol{Q}} \\ s_0(x)=g}} \Bigg| \sum_{\substack{\langle m\rangle \leqq \hat{\boldsymbol{P}}^{\theta} \\ \langle m\rangle \leqq \hat{\boldsymbol{Q}}\langle x\rangle^{-1}}} e(\alpha m^k x^k) \Bigg|^2.$$

Consequently, on making a trivial estimate for the innermost sum in two different ways, we find that

$$\mathscr{M} \ll \hat{\boldsymbol{P}}^{\varepsilon} \sideset{}{^{\dagger}}\sum_{\langle x\rangle \leqq \hat{\boldsymbol{Q}}} \hat{\boldsymbol{P}}^{\theta}\hat{\boldsymbol{Q}}\langle x\rangle^{-1} \ll \hat{\boldsymbol{P}}^{\theta+\varepsilon}\hat{\boldsymbol{Q}}\log \hat{\boldsymbol{Q}}.$$

We now substitute the last estimate into (7.19), and from there into (7.17), obtaining the upper bound

$$S_s(P, Q, R) \ll \hat{\boldsymbol{P}}^{\theta+\varepsilon}\hat{\boldsymbol{Q}} \sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^{\delta}} \mathscr{J}(g), \tag{7.20}$$

where we have written

$$\mathscr{J}(g) = \int_{\mathbb{T}} |G_g(\alpha; P)^2 f(\alpha; Q, R)^{2s-2}|\, d\alpha.$$

By orthogonality, the integral $\mathscr{J}(g)$ counts the number of solutions of an equation of the shape (7.4), subject to (7.5) and (7.6), save with $s-1$ in place of s, and with $\Psi'(z;\boldsymbol{b}) \neq 0$, $\Psi'(w;\boldsymbol{c}) \neq 0$, $g \mid \Psi'(z;\boldsymbol{b})$ and $g \mid \Psi'(w;\boldsymbol{c})$. Note that for each fixed choice of z and $\boldsymbol{b}$, it follows from Corollary 7.2 that the number of possible divisors g of $\Psi'(z;\boldsymbol{b})$ is at most $O\big(\langle \Psi'(z;\boldsymbol{b})\rangle^{\varepsilon}\big) = O(\hat{\boldsymbol{P}}^{\delta\varepsilon})$, and likewise for $\Psi'(w;\boldsymbol{c})$. We therefore deduce that

$$\sum_{\langle g\rangle \leqq \hat{\boldsymbol{P}}^{\delta}} \mathscr{J}(g) \ll \hat{\boldsymbol{P}}^{\varepsilon} S_{s-1}(P, Q, R),$$

and from here, the relation (7.20) leads to the upper bound

$$S_s(P, Q, R) \ll \hat{\boldsymbol{P}}^{\theta+\varepsilon}\hat{\boldsymbol{Q}} S_{s-1}(P, Q, R).$$

This confirms (7.11) in the third case.

(iv) Suppose that $S_4 \geqq \max\{S_1, S_2, S_3\}$, so that from (7.15) one has

$$S_s(P, Q, R) \leqq 4S_4.$$

Then for a given solution of (7.4) satisfying (7.5) and (7.6) counted by S_4, we have

$$\langle x_j\rangle > \hat{\boldsymbol{P}}^{\theta}, \quad \langle y_j\rangle > \hat{\boldsymbol{P}}^{\theta} \quad (1 \leqq j \leqq s) \quad \text{and} \quad \Psi'(z;\boldsymbol{b}) \neq 0, \quad \Psi'(w;\boldsymbol{c}) \neq 0,$$

and neither

$$x_j \mathscr{D}(\theta P)\Psi'(z;\boldsymbol{b}) \quad \text{nor} \quad y_j \mathscr{D}(\theta P)\Psi'(w;\boldsymbol{c}) \quad (1 \leqq j \leqq s). \tag{7.21}$$

When $1 \leqq j \leqq s$, let $\tilde{m}_j$ denote the product of all the monic irreducible factors of x_j that are coprime to $\Psi'(z;\boldsymbol{b})$. If one were to have $\langle \tilde{m}_j \rangle \leqq \hat{P}^\theta$, then $x_j \mathscr{D}(\theta P)\Psi'(z;\boldsymbol{b})$, contradicting (7.21). Then we are forced to conclude that $\langle \tilde{m}_j \rangle > \hat{P}^\theta$. Let m_j be a monic divisor of $\tilde{m}_j$ of smallest degree satisfying the property that $\langle m_j \rangle > \hat{P}^\theta$. Since the degree of each irreducible factor of x_j is at most R, we may infer that

$$\hat{P}^\theta < \langle m_j \rangle \leqq \min\{\hat{Q}, \hat{P}^\theta \hat{R}\} \quad \text{and} \quad \big(m_j, \Psi'(z;\boldsymbol{b})\big) = 1.$$

Plainly, we may proceed in a similar manner with y_j for $1 \leqq j \leqq s$.

With the discussion of the previous paragraph in mind, we see that $S_4 \leqq V_1$, where V_1 denotes the number of solutions of the equation

$$\Psi(z;\boldsymbol{b}) + \sum_{j=1}^{s} (m_j u_j)^k = \Psi(w;\boldsymbol{c}) + \sum_{j=1}^{s} (n_j v_j)^k,$$

with z, w, $\boldsymbol{b}$, $\boldsymbol{c}$ satisfying (7.6), and subject to the condition that for $1 \leqq j \leqq s$ one has

$$\begin{gathered} m_j, n_j \text{ monic}, \quad \hat{P}^\theta < \langle m_j \rangle, \langle n_j \rangle \leqq \min\{\hat{Q}, \hat{P}^\theta \hat{R}\}, \\ \big(m_j, \Psi'(z;\boldsymbol{b})\big) = \big(n_j, \Psi'(w;\boldsymbol{c})\big) = 1, \\ u_j \in \mathscr{A}(Q - \operatorname{ord} m_j, R), \quad v_j \in \mathscr{A}(Q - \operatorname{ord} n_j, R). \end{gathered} \tag{7.22}$$

Now define $F_m(\alpha;P) = F_m(\alpha;P;\mathscr{C})$ by putting

$$F_m(\alpha;P) = \sum_{z,\boldsymbol{b}} e\big(\alpha \Psi(z;\boldsymbol{b})\big),$$

where the summation is over z and $\boldsymbol{b}$ satisfying (7.6) subject to the condition that $\big(m, \Psi'(z;\boldsymbol{b})\big) = 1$. Also, write

$$F_j(\alpha) = f(m_j^k \alpha; Q - \operatorname{ord} m_j, R) f(-n_j^k \alpha; Q - \operatorname{ord} n_j, R) \quad (1 \leqq j \leqq s).$$

Then it follows from orthogonality that

$$V_1 \leqq \sum_{\boldsymbol{m},\boldsymbol{n}} \int_{\mathbb{T}} F_M(\alpha;P) F_N(-\alpha;P) \prod_{j=1}^{s} F_j(\alpha)\, d\alpha, \tag{7.23}$$

where here, and in what follows, the summation over $\boldsymbol{m}$ and $\boldsymbol{n}$ is subject to (7.22), and we have written $M = m_1 \dots m_s$ and $N = n_1 \dots n_s$.

We next write

$$X_j(\alpha) = |F_M(\alpha;P)^2 f(m_j^k \alpha; Q - \operatorname{ord} m_j, R)^{2s}|$$

and

$$Y_j(\alpha) = |F_N(\alpha;P)^2 f(n_j^k \alpha; Q - \operatorname{ord} n_j, R)^{2s}|.$$

Then it is apparent from (7.23) that

$$S_4 \ll \sum_{\boldsymbol{m},\boldsymbol{n}} \int_{\mathbb{T}} \prod_{j=1}^{s} \big(X_j(\alpha)\, Y_j(\alpha)\big)^{1/(2s)}\, d\alpha,$$

so that by Hölder's inequality,

$$S_4 \ll \sum_{\boldsymbol{m},\boldsymbol{n}} \prod_{j=1}^{s} \left(\int_{\mathbb{T}} X_j(\alpha)\, d\alpha \right)^{1/(2s)} \left(\int_{\mathbb{T}} Y_j(\alpha)\, d\alpha \right)^{1/(2s)}. \tag{7.24}$$

Now observe that

$$\int_{\mathbb{T}} X_j(\alpha)\, d\alpha \leqq W(P,Q,R;m_j) \quad \text{and} \quad \int_{\mathbb{T}} Y_j(\alpha)\, d\alpha \leqq W(P,Q,R;n_j),$$

where we write $W(P,Q,R;m)$ for the number of solutions of the equation

$$\Psi(z;\boldsymbol{b}) + m^k(u_1^k + \cdots + u_s^k) = \Psi(w;\boldsymbol{c}) + m^k(v_1^k + \cdots + v_s^k), \tag{7.25}$$

with z, w, $\boldsymbol{b}$, $\boldsymbol{c}$ subject to (7.6), and with $u_j, v_j \in \mathscr{A}(Q - \theta P, R)$ $(1 \leqq j \leqq s)$ and $\big(\Psi'(z;\boldsymbol{b}), m\big) = \big(\Psi'(w;\boldsymbol{c}), m\big) = 1$. Then, on applying Hölder's inequality on the right-hand side of (7.24), we obtain the estimate

$$\begin{aligned} S_4 &\ll \left(\sum_{\boldsymbol{m},\boldsymbol{n}} 1 \right)^{1-1/(2s)} \left(\sum_{\boldsymbol{m},\boldsymbol{n}} \prod_{j=1}^{s} \big(W(P,Q,R;m_j)\, W(P,Q,R;n_j)\big) \right)^{1/(2s)} \\ &\ll (\hat{\boldsymbol{P}}^{\theta}\hat{\boldsymbol{R}})^{2s-1}\, V(P,Q,R;\theta), \end{aligned} \tag{7.26}$$

where $V(P,Q,R;\theta)$ denotes the number of solutions of the equation (7.25) subject to (7.6), (7.8), (7.9) and the conditions $\big(\Psi'(z;\boldsymbol{b}), m\big) = \big(\Psi'(w;\boldsymbol{c}), m\big) = 1$. We now seek to establish that

$$V(P,Q,R;\theta) \ll \hat{\boldsymbol{P}}^{\varepsilon}\tilde{\boldsymbol{C}}_r T_s(P,Q,R;\theta), \tag{7.27}$$

for on substituting this bound into (7.26), we obtain

$$S_s(P,Q,R) \ll \hat{\boldsymbol{P}}^{\varepsilon}\tilde{\boldsymbol{C}}_r(\hat{\boldsymbol{P}}^{\theta}\hat{\boldsymbol{R}})^{2s-1}\, T_s(P,Q,R;\theta),$$

and this confirms (7.11) in the fourth and final case.

For a given polynomial m satisfying (7.8), let $\mathscr{E}(m;u;\boldsymbol{b})$ denote the set of solutions z of the congruence $\Psi(z;\boldsymbol{b}) \equiv u \pmod{m^k}$, with $\langle z\rangle < \langle m^k\rangle$ and $\big(\Psi'(z;\boldsymbol{b}), m\big) = 1$. Consider an irreducible factor ϖ of m, and suppose that $\varpi^h \,\|\, m^k$. An application of Hensel's Lemma (see, for example, [10], Lemma 5.21), shows that $\operatorname{card}\big(\mathscr{E}(\varpi^h;u;\boldsymbol{b})\big) \leqq \delta$, where δ is the degree of Ψ. Applying the Chinese Remainder Theorem and recalling Corollary 7.2, therefore, we deduce that

$$\operatorname{card}\big(\mathscr{E}(m;u;\boldsymbol{b})\big) \leqq \delta^{\omega(m)} \ll \langle m\rangle^{\varepsilon}. \tag{7.28}$$

Consider a solution of (7.25) counted by $W(P,Q,R;m)$. Motivated by the observation that $\Psi(z;\boldsymbol{b}) \equiv \Psi(w;\boldsymbol{c}) \pmod{m^k}$, we classify the set of solutions according to the residue class modulo m^k of $\Psi(z;\boldsymbol{b})$. Let

$$g_m(\alpha;\zeta;\boldsymbol{b}) = \sum_{\substack{\langle z\rangle \leqq \hat{\boldsymbol{P}} \\ z \equiv \zeta \pmod{m^k}}} e\big(\alpha\Psi(z;\boldsymbol{b})\big)$$

and

$$G_m(\alpha) = \sum_{\langle u\rangle < \langle m\rangle^k} \Big| \sum_{\boldsymbol{b}} \sum_{\zeta \in \mathscr{E}(m;u;\boldsymbol{b})} g_m(\alpha;\zeta;\boldsymbol{b}) \Big|^2,$$

in which here, and in what follows, the summation over $\boldsymbol{b}$ is subject to (7.6). Then on reviewing the definition of $V(P,Q,R;\theta)$, we find that

$$V(P,Q,R;\theta) \leqq \sum^{\dagger}_{\hat{\boldsymbol{P}}^{\theta} < \langle m\rangle \leqq \min\{\hat{\boldsymbol{Q}}, \hat{\boldsymbol{P}}^{\theta}\hat{\boldsymbol{R}}\}} V_m, \tag{7.29}$$

where

$$V_m = \int_{\mathbb{T}} G_m(\alpha) |f(m^k\alpha; Q - \theta P, R)|^{2s}\, d\alpha. \tag{7.30}$$

We now apply Cauchy's inequality in combination with (7.28), thereby obtaining the estimate

$$\begin{aligned} G_m(\alpha) &\ll \langle m\rangle^{\varepsilon} \tilde{\boldsymbol{C}}_r \sum_{\langle u\rangle < \langle m\rangle^k} \sum_{\boldsymbol{b}} \sum_{\zeta \in \mathscr{E}(m;u;\boldsymbol{b})} |g_m(\alpha;\zeta;\boldsymbol{b})|^2 \\ &\leqq \langle m\rangle^{\varepsilon} \tilde{\boldsymbol{C}}_r \sum_{\boldsymbol{b}} \sum_{\langle \zeta\rangle < \langle m\rangle^k} |g_m(\alpha;\zeta;\boldsymbol{b})|^2. \end{aligned}$$

On substituting this bound into (7.29) and (7.30), we consequently deduce that

$$V(P,Q,R;\theta) \ll \hat{\boldsymbol{P}}^{\varepsilon} \tilde{\boldsymbol{C}}_r \Upsilon,$$

where

$$\Upsilon = \sum^{\dagger}_{\hat{\boldsymbol{P}}^{\theta} < \langle m\rangle \leqq \min\{\hat{\boldsymbol{Q}}, \hat{\boldsymbol{P}}^{\theta}\hat{\boldsymbol{R}}\}} \sum_{\boldsymbol{b}} \sum_{\langle \zeta\rangle < \langle m\rangle^k} \int_{\mathbb{T}} |g_m(\alpha;\zeta;\boldsymbol{b})^2 f(m^k\alpha; Q - \theta P, R)^{2s}|\, d\alpha.$$

A comparison of the equation underlying the right-hand side of the last relation with (7.7) reveals that $\Upsilon \leqq T_s(P,Q,R;\theta)$. The desired bound (7.27) follows at once, and as we remarked earlier, the latter confirms (7.11) in the fourth case. This completes the proof of the lemma.

8. The efficient differencing process

The rôle of the fundamental lemma (Lemma 7.4) is to relate the mean value $S_s(P,Q,R)$ to the derived mean value $T_s(P,Q,R;\theta)$, the latter containing the relatively powerful congruence condition (7.10). We now exploit this condition by engineering a differencing process more efficient than that available via conventional Weyl differencing. In

order to discuss this efficient differencing process, we define the modified forward differencing operator Δ_1^* by

$$\Delta_1^*\big(f(z);h;m\big) = m^{-k}\big(f(z) - f(z - hm^k)\big),$$

and then define Δ_j^* recursively by

$$\Delta_{j+1}^*\big(f(z);h_1,\dots,h_{j+1};m_1,\dots,m_{j+1}\big) = \Delta_1^*\big(\Delta_j^*\big(f(z);h_1,\dots,h_j;m_1,\dots,m_j\big);h_{j+1};m_{j+1}\big).$$

It is convenient also to adopt the convention that $\Delta_0\big(f(z)\big) = f(z)$.

While in characteristic zero, the differencing process effectively decreases the degree of the polynomial argument by precisely one, the situation in positive characteristic is more subtle. It is therefore useful to define the *q-difference degree* of a polynomial $f(z)$ with coefficients in $\mathbb{F}_q[t]$ to be the largest natural number γ for which $\Delta_\gamma^*\big(f(z);\boldsymbol{h};\boldsymbol{m}\big)$ is not identically zero as a polynomial in z, $\boldsymbol{h}$, $\boldsymbol{m}$. We write $\gamma\big(f(z);q\big)$ for the q-difference degree of the polynomial $f(z)$. In addition, when confusion is easily avoided, we write $\gamma(k;q)$ for $\gamma(z^k;q)$. The following lemma shows that $\gamma(k;q)$ may be conveniently evaluated in terms of the sum of digits function $\gamma_q(k)$ defined in the preamble to the statement of Theorem 1.1.

Lemma 8.1. *When k is a natural number, one has $\gamma(k;q) = \gamma_q(k)$.*

Proof. Let the characteristic of $\mathbb{F}_q$ be p, and write k in base p in the shape $k = a_np^n + \cdots + a_1p + a_0$, where $0 \leqq a_i \leqq p-1$ $(0 \leqq i \leqq n)$ and $a_n \neq 0$. We seek to show that $\gamma(k;q) = a_0 + a_1 + \cdots + a_n$, and this we achieve by induction. Observe first that if $\gamma_q(k) = 1$, then $k = p^n$ for some non-negative integer n. In such circumstances one has

$$\Delta_1^*(z^{p^n};h;m) = m^{-k}\big(z^{p^n} - (z - hm^k)^{p^n}\big) = (-1)^{p+1}h^{p^n}m^{k(p^n-1)},$$

which is not identically zero as a polynomial in z, $\boldsymbol{h}$ and $\boldsymbol{m}$. Thus we see that $\gamma(k;q) = 1$ when $\gamma_q(k) = 1$, and so the basis for our induction is established.

Suppose next that $\gamma_q(k) \geqq 2$, and that $\gamma(l;q) = \gamma_q(l)$ for each natural number l with $l < k$. By the binomial expansion, one has

$$\Delta_1^*(z^k;h;m) = \sum_{j=0}^{k-1}(-1)^{k-j+1}f_j(h,m)z^j,$$

where we write $f_j(h,m) = \binom{k}{j}h^{k-j}m^{k(k-j-1)}$. When $0 \leqq j < k$, write $\tau = \tau(k,j)$ for the non-negative integer satisfying $p^\tau \Big\| \binom{k}{j}$. Then we have

$$\tau = \sum_{h=1}^{\infty}\left(\left[\frac{k}{p^h}\right] - \left[\frac{j}{p^h}\right] - \left[\frac{k-j}{p^h}\right]\right) = \sum_{h=1}^{\infty}\left(\left\{\frac{j}{p^h}\right\} + \left\{\frac{k-j}{p^h}\right\} - \left\{\frac{k}{p^h}\right\}\right),$$

where, as usual, we write $\{\beta\}$ for $\beta - [\beta]$. It follows that $\binom{k}{j}$ is coprime to p if and only if j has the shape $j = b_np^n + \cdots + b_1p + b_0$, with $0 \leqq b_i \leqq a_i$ for $0 \leqq i \leqq n$ (this in fact fol-

lows from Lucas' criterion). Writing $\mathscr{N}(k)$ for the set of integers j with $0 \leqq j \leqq k-1$ for which the latter condition is satisfied, we therefore deduce that

$$\Delta_1^*(z^k; h; m) = \sum_{j \in \mathscr{N}(k)} (-1)^{k-j+1} f_j(h,m) z^j.$$

Furthermore, each term in the latter sum is non-trivial as a polynomial in z, h and m. In view of our inductive hypothesis, therefore, one has

$$\gamma(k;q) = 1 + \max_{j \in \mathscr{N}(k)} \gamma(j;q) = 1 + \max_{j \in \mathscr{N}(k)} \gamma_q(j).$$

Moreover, since $\gamma_q(k) \geqq 2$, there is some element j of $\mathscr{N}(k)$ for which $\gamma_q(j) = \gamma_q(k) - 1$, and so we conclude that $\gamma(k;q) = 1 + \big(\gamma_q(k) - 1\big) = \gamma_q(k)$. This establishes the inductive step, and so the proof of the lemma is complete.

Before discussing the efficient differencing process itself, we pause to summarise Lemma 7.4 in a form tailored for the task we have in mind. When j is a non-negative integer, we define the polynomial $\Psi_j(z; \boldsymbol{h}; \boldsymbol{m}) = \Psi_{j,k}(z; h_1, \dots, h_j; m_1, \dots, m_j)$ by putting

$$\Psi_j(z; \boldsymbol{h}; \boldsymbol{m}) = \Delta_j^*(z^k; \boldsymbol{h}; \boldsymbol{m}).$$

For each integer j with $1 \leqq j \leqq \gamma_q(k)$, one may write $\Psi'_{j,k}(z; \boldsymbol{h}; \boldsymbol{m})$ in the form

$$\Psi'_{j,k}(z; \boldsymbol{h}; \boldsymbol{m}) = k h_1 \dots h_j \sum_{l=0}^{k-j-1} \psi_{l,j}(\boldsymbol{h}; \boldsymbol{m}) z^l, \tag{8.1}$$

where, for $0 \leqq l \leqq k-j-1$, the polynomials $\psi_{l,j}(\boldsymbol{h}; \boldsymbol{m}) = \psi_{l,j}^{(k)}(h_1, \dots, h_j; m_1, \dots, m_j)$ have coefficients in $\mathbb{F}_q[t]$, and are of degree $k-j-1-l$ in $\boldsymbol{h}$ and $\boldsymbol{m}$. We observe that $\psi_{l,j}(\boldsymbol{h}; \boldsymbol{m})$ may be written as a polynomial in $h_r m_r^k$ $(1 \leqq r \leqq j)$, say $\psi_{l,j}(\boldsymbol{h}; \boldsymbol{m}) = \chi_{l,j}(h_1 m_1^k, \dots, h_j m_j^k)$. When $0 \leqq r \leqq j$, let $\mathscr{I}_{j,k}^{(r)}$ denote the set of indices l for which $\chi_{l,j}(\boldsymbol{\xi})$ does not depend explicitly on $\xi_{r+1}, \dots, \xi_j$. Here, we adopt the convention that $\mathscr{I}_{j,k}^{(j)} = \{0, 1, \dots, k-j-1\}$. Thus, in particular, the indices $l \in \mathscr{I}_{j,k}^{(0)}$ make no contribution on the right-hand side of (8.1).

We now abbreviate $\gamma_q(k)$ simply to γ, and when $1 \leqq i \leqq \gamma$, we take $\phi_i = \phi_i(s,k)$ to be a parameter chosen in due course, but satisfying $0 < \phi_i \leqq 1/k$. When $1 \leqq j \leqq \gamma$, we then put

$$\Phi_j = \phi_1 + \cdots + \phi_j, \quad M_j = \phi_j P, \quad H_j = P - kM_j \quad \text{and} \quad Q_j = (1 - \Phi_j)P. \tag{8.2}$$

The parameter intervals $[C_i', C_i]$ $(1 \leqq i \leqq r)$ of §7 are now interpreted as $(M_i, M_i + R]$ and $[0, H_i]$ $(1 \leqq i \leqq j)$, with $r = 2j$. We write $\mathfrak{X}_j$ for the set of $2j$-tuples of polynomials $(\boldsymbol{m}, \boldsymbol{h})$ with $\hat{\boldsymbol{M}}_i < \langle m_i \rangle \leqq \hat{\boldsymbol{M}}_i \hat{\boldsymbol{R}}$ and $1 \leqq \langle h_i \rangle \leqq \hat{\boldsymbol{H}}_i$ $(1 \leqq i \leqq j)$. When $1 \leqq \mu \leqq \lambda \leqq k$, let $\Theta_{\mu,\lambda}$ denote the set of polynomials $\chi_{l,\lambda}(\boldsymbol{\xi})$ with $l \in \mathscr{I}_{\lambda,k}^{(\mu)} \backslash \mathscr{I}_{\lambda,k}^{(\mu-1)}$, and write $\Xi_\mu = \Theta_{\mu,\mu} \cup \cdots \cup \Theta_{\mu,k}$. Next define $\mathscr{D}_{\mu,j}$ to be the set of elements $(\boldsymbol{m}, \boldsymbol{h}) \in \mathfrak{X}_j$ satisfying the condition that $\chi(h_1 m_1^k, \dots, h_\mu m_\mu^k) = 0$ for some $\chi \in \Xi_\mu$. We then put $\mathscr{E}_j = \mathscr{D}_{1,j} \cup \mathscr{D}_{2,j} \cup \cdots \cup \mathscr{D}_{j,j}$, and define $\mathscr{C}_j = \mathfrak{X}_j \backslash \mathscr{E}_j$. In this way, we ensure that when $\Psi'_{j,k}(z; \boldsymbol{h}; \boldsymbol{m})$ is considered as a polynomial in z, then whenever $(\boldsymbol{m}, \boldsymbol{h})$ lies in $\mathscr{C}_j$, every coefficient of $\Psi'_{j,k}$ that could conceivably be non-zero is indeed non-zero.

Next we define

$$F_j(\alpha) = \sum_{z,\boldsymbol{h},\boldsymbol{m}} e\big(\alpha\Psi_{j,k}(z;\boldsymbol{h};\boldsymbol{m})\big),$$

where the summation is over z, $\boldsymbol{h}$, $\boldsymbol{m}$ with $1 \leqq \langle z\rangle \leqq \hat{P}$ and $(\boldsymbol{m},\boldsymbol{h}) \in \mathscr{C}_j$. Finally, we write $S_s(P,Q,R;\Psi_j)$ for $S_s(P,Q,R;\Psi_{j,k};\mathscr{C}_j)$, and do likewise with the counting functions T_s and N_s.

Lemma 8.2. *Let η be a positive number with $\eta < 1$, and suppose that R is a parameter satisfying $P/\log(2P) < R \leqq \eta P$. Then whenever s is a non-negative integer and $0 \leqq j < \gamma$, one has*

$$S_s(P,Q_j,R;\Psi_j) \ll \hat{P}^{\varepsilon}\hat{R}^{2s-1+j}\tilde{H}_j\tilde{M}_j\hat{M}_{j+1}^{2s-1}T_s(P,Q_j,R;\phi_{j+1};\Psi_j). \tag{8.3}$$

Proof. Our strategy is to establish by induction that for each natural number s the upper bound (8.3) holds. For the sake of convenience, write $\theta = \phi_{j+1}$, so that $\hat{P}^{\theta} = \hat{M}_{j+1}$. We begin by establishing a basis for the induction with the case $s = 0$. Observe that $S_0(P,Q_j,R;\Psi_j)$ counts the number of solutions of the equation

$$\Psi_j(z;\boldsymbol{h};\boldsymbol{m}) = \Psi_j(w;\boldsymbol{g};\boldsymbol{n}), \tag{8.4}$$

with $\langle z\rangle, \langle w\rangle \leqq \hat{P}$, $(\boldsymbol{m},\boldsymbol{h}) \in \mathscr{C}_j$ and $(\boldsymbol{n},\boldsymbol{g}) \in \mathscr{C}_j$. By exchanging the order of differentiation and differencing, one sees that $\Psi'_{j,k}(z;\boldsymbol{h};\boldsymbol{m}) = k\Psi_{j,k-1}(z;\boldsymbol{h};\boldsymbol{m})$, and so it follows from the discussion in the preamble to this lemma that when $(\boldsymbol{m},\boldsymbol{h}) \in \mathscr{C}_j$, then $\Psi'_{j,k}(z;\boldsymbol{h};\boldsymbol{m})$ is a non-trivial polynomial in z, though possibly constant (i.e. a non-vanishing polynomial only in $\boldsymbol{h}$ and $\boldsymbol{m}$). But the latter implies that $\Psi_{j,k}(z;\boldsymbol{h};\boldsymbol{m})$ is also a non-trivial polynomial in z, and of degree at least one. Fixing choices of $(\boldsymbol{m},\boldsymbol{h}) \in \mathscr{C}_j$ and $(\boldsymbol{n},\boldsymbol{g}) \in \mathscr{C}_j$, therefore, we find that for each fixed choice of w there are at most $k-j$ possible choices for z satisfying (8.4). We consequently find that

$$S_0(P,Q_j,R;\Psi_j) \ll \hat{P}(\tilde{H}_j\tilde{M}_j\hat{R}^j)^2. \tag{8.5}$$

The quantity $T_0(P,Q_j,R;\theta;\Psi_j)$, on the other hand, counts the number of solutions of the equation

$$\Psi_j(z;\boldsymbol{h};\boldsymbol{m}) = \Psi_j(w;\boldsymbol{h};\boldsymbol{m}), \tag{8.6}$$

with $\langle z\rangle, \langle w\rangle \leqq \hat{P}$, $(\boldsymbol{m},\boldsymbol{h}) \in \mathscr{C}_j$, $\hat{M}_{j+1} < \langle m\rangle \leqq \min\{\hat{Q}_j, \hat{M}_{j+1}\hat{R}\}$ and $z \equiv w \pmod{m^k}$. Counting only the diagonal solutions of (8.6) with $z = w$, we find that

$$T_0(P,Q_j,R;\theta;\Psi_j) \gg \hat{P}\hat{M}_{j+1}\tilde{H}_j\tilde{M}_j\hat{R}^{j+1}. \tag{8.7}$$

A comparison of (8.5) and (8.7) reveals that

$$S_0(P,Q_j,R;\Psi_j) \ll \tilde{H}_j\tilde{M}_j\hat{R}^{j-1}\hat{M}_{j+1}^{-1}T_0(P,Q_j,R;\theta;\Psi_j),$$

and this confirms the estimate (8.3) in the case $s = 0$.

Next, we suppose that (8.3) has been established with s replaced by u, for each non-negative integer u with $u < s$, and we consider the conclusion of Lemma 7.4 with $\theta = \phi_{j+1}$.

First consider the term $S_s(P,\theta P,R;\Psi_j)$. Note that since $0<\phi_i\leqq 1/k$ $(1\leqq i\leqq j+1)$ and $j<\gamma\leqq k$, one has $1-(\phi_1+\cdots+\phi_j)\geqq 1-j/k\geqq\theta$. It therefore follows from (8.2) that $\theta P\leqq Q_j$, that $\hat{P}^\theta\leqq\hat{Q}_j$, and hence also that $\hat{P}^{2\theta}\leqq\hat{Q}_j\hat{M}_{j+1}$. Then on interpreting the equation underlying $S_v(P,\theta P,R;\Psi_j)$ $(v=s-1,s)$ in integral form, and applying a trivial estimate for the generating function $f(\alpha;\theta P,R)$, we obtain the bound

$$\begin{aligned}S_s(P,\theta P,R;\Psi_j)&=\int_{\mathbb{T}}|F_j(\alpha)^2f(\alpha;\theta P,R)^{2s}|\,d\alpha\\&\ll\hat{Q}_j\hat{M}_{j+1}S_{s-1}(P,\theta P,R;\Psi_j).\end{aligned}$$

But $S_{s-1}(P,\theta P,R;\Psi_j)\leqq S_{s-1}(P,Q_j,R;\Psi_j)$, and so it follows from our inductive hypothesis that

$$S_s(P,\theta P,R;\Psi_j)\ll\hat{P}^{\varepsilon}\hat{R}^{2s-3+j}\tilde{H}_j\tilde{M}_j\hat{M}_{j+1}^{2s-2}\hat{Q}_jT_{s-1}(P,Q_j,R;\theta;\Psi_j).\tag{8.8}$$

A consideration of the semi-diagonal solutions of (7.7) counted by $T_s(P,Q_j,R;\theta;\Psi_j)$, in which $u_s=v_s$, in combination with the conclusion of Lemma 7.3, consequently reveals that

$$T_s(P,Q_j,R;\theta;\Psi_j)\gg\hat{Q}_{j+1}^{1-\varepsilon}T_{s-1}(P,Q_j,R;\theta;\Psi_j).\tag{8.9}$$

Now combining (8.8) and (8.9), and noting that $\hat{Q}_{j+1}\hat{M}_{j+1}=\hat{Q}_j$, we arrive at the upper bound

$$S_s(P,\theta P,R;\Psi_j)\ll\hat{P}^{2\varepsilon}\hat{R}^{2s-3+j}\tilde{H}_j\tilde{M}_j\hat{M}_{j+1}^{2s-1}T_s(P,Q_j,R;\theta;\Psi_j).\tag{8.10}$$

Next we consider $N_s(P,Q_j,R;\Psi_j)$. If z, w, $\boldsymbol{h}$, $\boldsymbol{g}$, $\boldsymbol{m}$, $\boldsymbol{n}$, $\boldsymbol{x}$, $\boldsymbol{y}$ is a solution of the equation

$$\Psi_j(z;\boldsymbol{h};\boldsymbol{m})-\Psi_j(w;\boldsymbol{g};\boldsymbol{n})=\sum_{i=1}^{s}(x_i^k-y_i^k)$$

counted by $N_s(P,Q_j,R;\Psi_j)$, then one has $\Psi_j'(z;\boldsymbol{h};\boldsymbol{m})=\Psi_j'(w;\boldsymbol{g};\boldsymbol{n})=0$, and $(\boldsymbol{m},\boldsymbol{h})\in\mathscr{C}_j$ and $(\boldsymbol{n},\boldsymbol{g})\in\mathscr{C}_j$. As in the discussion above concerning the equation (8.4), the polynomials $\Psi_j'(z;\boldsymbol{h};\boldsymbol{m})$ and $\Psi_j'(w;\boldsymbol{g};\boldsymbol{n})$ are non-trivial in z and w respectively. In particular, if either is a constant polynomial in terms of the respective variables z and w, then that constant is non-zero. It follows that for fixed choices of $(\boldsymbol{m},\boldsymbol{h})\in\mathscr{C}_j$ and $(\boldsymbol{n},\boldsymbol{g})\in\mathscr{C}_j$, there are at most $O(1)$ possible choices of z and w. On interpreting the number of solutions of the underlying equation in integral form and applying the triangle inequality, we therefore conclude that

$$N_s(P,Q_j,R;\Psi_j)\ll(\tilde{H}_j\tilde{M}_j\hat{R}^j)^2\int_{\mathbb{T}}|f(\alpha;Q_j,R)|^{2s}\,d\alpha.\tag{8.11}$$

If $x\in\mathscr{A}(Q_j,R)$, then either $\langle x\rangle<\hat{P}^\theta$, or else x has a divisor m with $\hat{P}^\theta<\langle m\rangle\leqq\hat{P}^\theta\hat{R}$. On considering the associated equations, one therefore finds that

$$\int_{\mathbb{T}}|f(\alpha;Q_{j+1},R)|^{2s}\,d\alpha\leqq\int_{\mathbb{T}}|\mathfrak{f}(\alpha)|^{2s}\,d\alpha,\tag{8.12}$$

where we write

$$\mathfrak{f}(\alpha)=f(\alpha;M_{j+1},R)+\sum_{\hat{M}_{j+1}<\langle m\rangle\leqq\hat{M}_{j+1}\hat{R}}f(\alpha m^k;Q_{j+1},R).$$

On considering the underlying equation, a change of variable yields the estimate

$$\sum_{\hat{\boldsymbol{M}}_{j+1}<\langle m\rangle\leqq\hat{\boldsymbol{M}}_{j+1}\hat{\boldsymbol{R}}}\int_{\mathbb{T}}|f(\alpha m^k;Q_{j+1},R)|^{2s}\,d\alpha\ll\hat{\boldsymbol{M}}_{j+1}\hat{\boldsymbol{R}}S_s(Q_{j+1},R),$$

and so a trivial estimate for $|f(\alpha;M_{j+1},R)|$, in combination with an application of Hölder's inequality, leads from (8.12) to the bound

$$\int_{\mathbb{T}}|f(\alpha;Q_j,R)|^{2s}\,d\alpha\ll\hat{\boldsymbol{M}}_{j+1}^{2s}+(\hat{\boldsymbol{M}}_{j+1}\hat{\boldsymbol{R}})^{2s}S_s(Q_{j+1},R).$$

On recalling (8.11), we therefore arrive at the relation

$$N_s(P,Q_j,R;\Psi_j)\ll(\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_j\hat{\boldsymbol{R}}^j)^2(\hat{\boldsymbol{M}}_{j+1}\hat{\boldsymbol{R}})^{2s}S_s(Q_{j+1},R). \tag{8.13}$$

Next, on considering the semi-diagonal solutions counted by $T_s(P,Q_j,R;\theta;\Psi_j)$ in which $z=w$, we obtain the lower bound

$$T_s(P,Q_j,R;\theta;\Psi_j)\gg\hat{\boldsymbol{P}}\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_{j+1}\hat{\boldsymbol{R}}^{j+1}S_s(Q_{j+1},R).$$

A comparison with (8.13) consequently leads to the upper bound

$$N_s(P,Q_j,R;\Psi_j)\ll\hat{\boldsymbol{P}}^{-1}\hat{\boldsymbol{R}}^{2s-1+j}\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_j\hat{\boldsymbol{M}}_{j+1}^{2s-1}T_s(P,Q_j,R;\theta;\Psi_j). \tag{8.14}$$

We now come to the third term on the right-hand side of (7.11). On recalling the inductive hypothesis, it follows from (8.9) together with the relation $\hat{\boldsymbol{Q}}_{j+1}\hat{\boldsymbol{M}}_{j+1}=\hat{\boldsymbol{Q}}_j$ that

$$\hat{\boldsymbol{Q}}_j\hat{\boldsymbol{P}}^{\theta+\varepsilon}S_{s-1}(P,Q_j,R;\Psi_j)\ll\hat{\boldsymbol{P}}^{3\varepsilon}\hat{\boldsymbol{R}}^{2s-3+j}\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_j\hat{\boldsymbol{M}}_{j+1}^{2s-1}T_s(P,Q_j,R;\theta;\Psi_j). \tag{8.15}$$

We therefore conclude from Lemma 7.4 in combination with (8.10), (8.14) and (8.15) that

$$S_s(P,Q_j,R;\Psi_j)\ll\hat{\boldsymbol{P}}^{3\varepsilon}\hat{\boldsymbol{R}}^{2s-1+j}\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_j\hat{\boldsymbol{M}}_{j+1}^{2s-1}T_s(P,Q_j,R;\theta;\Psi_j),$$

and this suffices to establish the inductive step. The desired conclusion (8.3) now follows for every non-negative integer s, and this completes the proof of the lemma.

The conclusion of Lemma 8.2 enables us to bound the mean value $S_s(P,Q_j,R;\Psi_j)$ in terms of $T_s(P,Q_j,R;\phi_{j+1};\Psi_j)$. We now complete the efficient differencing step by relating $T_s(P,Q_j,R;\phi_{j+1};\Psi_j)$ to $S_s(P,Q_{j+1},R;\Psi_{j+1})$.

Lemma 8.3. *Let η be a positive number with $\eta<1$, and suppose that R is a parameter satisfying $P/\log(2P)<R\leqq\eta P$. Then whenever s is a positive integer and $0\leqq j<\gamma$, one has*

$$\begin{aligned}T_s(P,Q_j,R;\phi_{j+1};\Psi_j)\ll{}&\hat{\boldsymbol{P}}^{1+\varepsilon}\hat{\boldsymbol{R}}^{j+1}\tilde{\boldsymbol{H}}_j\tilde{\boldsymbol{M}}_{j+1}S_s(Q_{j+1},R)\\&+\big(S_s(Q_{j+1},R)\big)^{1/2}\big(S_s(P,Q_{j+1},R;\Psi_{j+1})\big)^{1/2}.\end{aligned} \tag{8.16}$$

Proof. We begin by noting that $T_s(P,Q_j,R;\phi_{j+1};\Psi_j)$ counts the number of solutions of the equation

$$\Psi_j(z;\boldsymbol{h};\boldsymbol{m})-\Psi_j(w;\boldsymbol{h};\boldsymbol{m})=m^k\sum_{i=1}^{s}(u_i^k-v_i^k), \tag{8.17}$$

with

$$\langle z\rangle, \langle w\rangle \leqq \hat{P}, \quad (\boldsymbol{m}, \boldsymbol{h}) \in \mathscr{C}_j, \tag{8.18}$$

and with

$$m \text{ monic}, \quad \hat{M}_{j+1} < \langle m\rangle \leqq \min\{\hat{Q}_j, \hat{M}_{j+1}\hat{R}\}, \tag{8.19}$$

$$u_i, v_i \in \mathscr{A}(Q_{j+1}, R) \quad (1 \leqq i \leqq s) \quad \text{and} \quad z \equiv w \pmod{m^k}. \tag{8.20}$$

The last condition may be interpreted by writing $w = z - hm^k$ for some $h \in \mathbb{F}_q[t]$ with $\langle h\rangle \leqq \max\{\langle z\rangle, \langle w\rangle\}\langle m\rangle^{-k} \leqq \hat{H}_{j+1}$. Let U_0 denote the number of solutions of (8.17) with (8.18), (8.19) and (8.20), where in addition one has $z = w$, and let U_1 denote the corresponding number of solutions for which $w = z - hm^k$ with $(\boldsymbol{m}, m; \boldsymbol{h}, h) \in \mathscr{E}_{j+1}$. Also, let U_2 denote the number of solutions of the equation

$$\Psi_j(z; \boldsymbol{h}; \boldsymbol{m}) - \Psi_j(z - hm^k; \boldsymbol{h}; \boldsymbol{m}) = m^k \sum_{i=1}^{s} (u_i^k - v_i^k), \tag{8.21}$$

with z, $\boldsymbol{h}$, $\boldsymbol{m}$, m, $\boldsymbol{u}$, $\boldsymbol{v}$ subject to (8.18), (8.19) and (8.20), and subject also to the condition that $(\boldsymbol{m}, m; \boldsymbol{h}, h) \in \mathscr{C}_{j+1}$. Then it follows from the above discussion that one has the upper bound

$$T_s(P, Q_j, R; \phi_{j+1}; \Psi_j) \leqq U_0 + U_1 + U_2. \tag{8.22}$$

In view of the definition of U_0, the estimate

$$U_0 \ll \hat{P}\tilde{H}_j\tilde{M}_{j+1}\hat{R}^{j+1} S_s(Q_{j+1}, R) \tag{8.23}$$

is immediate from (8.17)–(8.20). Next we consider U_1. For a fixed choice of $\boldsymbol{m}$ and $\boldsymbol{h}$ with $(\boldsymbol{m}, \boldsymbol{h}) \in \mathscr{C}_j$, any polynomials m and h with $(\boldsymbol{m}, m, \boldsymbol{h}, h) \in \mathscr{E}_{j+1}$ necessarily satisfy the condition that $\chi(h_1 m_1^k, \dots, h_j m_j^k, hm^k) = 0$ for some $\chi \in \Xi_{j+1}$, and further that $\nu(h_1 m_1^k, \dots, h_j m_j^k) \neq 0$ whenever $\nu \in \Xi_j$. A consideration of the relative degrees of terms involving $\boldsymbol{m}$ and $\boldsymbol{h}$, and m and h, reveals that whenever $(\boldsymbol{m}, m, \boldsymbol{h}, h) \in \mathscr{E}_{j+1}$, then for each fixed $(\boldsymbol{m}, \boldsymbol{h}) \in \mathscr{C}_j$, the polynomial hm^k must be a zero of some one of $O(1)$ polynomials of degree at most k. There are consequently at most $O(1)$ possible such choices for hm^k for each fixed choice of $(\boldsymbol{m}, \boldsymbol{h}) \in \mathscr{C}_j$. For each fixed choice of the non-zero polynomial hm^k, moreover, it follows from Corollary 7.2 that the number of available choices for h and m is $O(\hat{P}^{\varepsilon})$. Given a fixed choice of w, it is a consequence of the foregoing discussion that there are at most $O(1)$ choices for z with $w = z - hm^k$ counted by U_1. Interpreting the equation (8.17) in terms of an associated integral and applying the triangle inequality, we thus conclude that

$$\begin{aligned} U_1 &\ll \hat{P}^{1+\varepsilon}\tilde{H}_j\tilde{M}_j\hat{R}^j \max_{\hat{M}_{j+1} < \langle m\rangle \leqq \hat{M}_{j+1}\hat{R}} \int_{\mathbb{T}} |f(\alpha m^k; Q_{j+1}, R)|^{2s}\, d\alpha \\ &= \hat{P}^{1+\varepsilon}\tilde{H}_j\tilde{M}_j\hat{R}^j S_s(Q_{j+1}, R). \end{aligned} \tag{8.24}$$

Next we observe that

$$m^{-k}\big(\Psi_j(z; \boldsymbol{h}; \boldsymbol{m}) - \Psi_j(z - hm^k; \boldsymbol{h}; \boldsymbol{m})\big) = \Psi_{j+1}(z; \boldsymbol{h}, h; \boldsymbol{m}, m).$$

On interpreting the equation underlying (8.21) in integral form, we therefore deduce that

$$U_2 \ll \int_{\mathbb{T}} F_{j+1}(\alpha)|f(\alpha; Q_{j+1}, R)|^{2s}\, d\alpha.$$

By Schwarz's inequality, we thus arrive at the upper bound

$$\begin{aligned} U_2 &\ll \left(\int_{\mathbb{T}} |f(\alpha; Q_{j+1}, R)|^{2s}\, d\alpha\right)^{1/2} \left(\int_{\mathbb{T}} |F_{j+1}(\alpha)^2 f(\alpha; Q_{j+1}, R)^{2s}|\, d\alpha\right)^{1/2} \\ &= \big(S_s(Q_{j+1}, R)\big)^{1/2} \big(S_s(P, Q_{j+1}, R; \Psi_{j+1})\big)^{1/2}. \end{aligned} \tag{8.25}$$

The desired conclusion (8.16) follows on combining (8.22), (8.23), (8.24) and (8.25).

9. Permissible exponents

The application of Lemmata 8.2 and 8.3 in sequence permits us to estimate $S_s(P, Q_j, R; \Psi_j)$ in terms of $S_s(P, Q_{j+1}, R; \Psi_{j+1})$, and thereby a kind of differencing operation is executed inside the associated mean value. On recalling that $\Psi_0(z) = z^k$, it is evident from a comparison of (7.2) and (7.4) that $S_{s+1}(P, R) \leqq S_s(P, P, R; \Psi_0)$, and so we are able to apply the aforementioned differencing argument to obtain estimates for $S_u(P, R)$ for successive values of u. The goal of this section is to obtain estimates of the shape $S_s(P, R) \ll \hat{P}^{\lambda_s+\varepsilon}$, valid for suitable exponents λ_s when R is suitably small. In this context, and in what occurs henceforth, it is useful to introduce the following convention concerning the numbers ε and R. Whenever ε or R appear in a statement, either implicitly or explicitly, we assert that for each $\varepsilon > 0$, there exists a positive number $\eta_0(\varepsilon, s, k)$ such that the statement holds whenever $R = \eta P$, with $0 < \eta \leqq \eta_0(\varepsilon, s, k)$. Note that the "value" of ε, and η_0, may change from statement to statement, and hence also the dependency of implicit constants on ε and η. Notice that since our iterative methods will involve only a finite number of statements (depending at most on k, s and ε), there is no danger of losing control of implicit constants through the successive changes implicit in our arguments. Finally, we use the symbol $\approx$ to indicate that constants and powers of R and P^{ε} are to be ignored.

We say that the exponent $\Delta_s = \Delta_{s,k}(q)$ is *permissible* whenever, with the convention described above, one has $S_s(P, R) \ll \hat{P}^{\lambda_s+\varepsilon}$, wherein we write $\lambda_s = 2s - k + \Delta_s$. We may interpret what it means for the exponent Δ_s to be permissible as follows. Whenever $\varepsilon > 0$ and η_0 is a positive number sufficiently small in terms of ε, then for all positive numbers P sufficiently large in terms of q, ε, η, s and k, one has

$$\int_{\mathbb{T}} |f(\alpha; P, R)|^{2s}\, d\alpha \ll \hat{P}^{2s-k+\Delta_s+\varepsilon}.$$

Notice that by making use of a trivial estimate for $f(\alpha; P, R)$, it follows easily from the latter bound that permissible exponents Δ_s may always be assumed to satisfy the inequality $\Delta_s \leqq k$. In addition, the sequence of inequalities

$$\hat{P}^{2s} \ll \sum_{\langle h\rangle \leqq \hat{P}^k} \int_{\mathbb{T}} |f(\alpha; P, R)|^{2s} e(-\alpha h)\, d\alpha \ll \hat{P}^k \int_{\mathbb{T}} |f(\alpha; P, R)|^{2s}\, d\alpha$$

ensures that Δ_s is necessarily non-negative. The next lemma supplies permissible exponents when s is 1 or 2.

Lemma 9.1. *One has* $S_1(P,P) \ll \hat{P}$ *and* $S_2(P,P) \ll \hat{P}^{2+\varepsilon}$.

Proof. The first inequality claimed in the statement of the lemma is trivial from orthogonality. For the second, we observe that $S_2(P,P)$ is bounded above by the number of solutions of the equation

$$(x_1 - y_1)(x_1^{k-1} + x_1^{k-2}y_1 + \cdots + y_1^{k-1}) = x_2^k - y_2^k, \tag{9.1}$$

with $\langle x_i \rangle, \langle y_i \rangle \leqq \hat{P}$ $(i = 1,2)$. For each fixed choice of x_2 and y_2 with $x_2^k \neq y_2^k$, both $x_1 - y_1$ and $x_1^{k-1} + x_1^{k-2}y_1 + \cdots + y_1^{k-1}$ are divisors of the non-zero element of $\mathbb{F}_q[t]$ given by $x_2^k - y_2^k$. Fixing any one of the $O(\hat{P}^{\varepsilon})$ possible choices of these divisors, say d_1 and d_2 respectively, one finds that $x_1 = y_1 + d_1$, whence

$$(y_1 + d_1)^{k-1} + (y_1 + d_1)^{k-2}y_1 + \cdots + y_1^{k-1} = d_2.$$

The latter polynomial equation contains the leading term ky_1^{k-1}, and since throughout we assume that the characteristic of $\mathbb{F}_q$ does not divide k, we find that y_1 is determined by a non-trivial polynomial of degree $k-1$. Consequently, there are at most $k-1$ possible choices for y_1 and hence also for x_1. There are therefore at most $O(\hat{P}^{2+\varepsilon})$ solutions of (9.1) counted by $S_2(P,P)$ in which $x_2^k \neq y_2^k$.

When $x_2^k = y_2^k$, meanwhile, one has also $x_1^k = y_1^k$. In this situation, given a fixed choice of y_1 and y_2, there are at most k choices each for x_1 and x_2. The number of solutions of this type counted by $S_2(P,P)$ is therefore at most $O(\hat{P}^2)$. The upper bound $S_2(P,P) \ll \hat{P}^{2+\varepsilon}$ follows at once on combining this contribution with the one bounded in the previous paragraph.

It follows from Lemma 9.1 that one may take $\Delta_1 = k-1$ and $\Delta_2 = k-2$ as permissible exponents. We note that it is reasonable to conjecture that the exponent $\Delta_u = \max\{k-u, 0\}$ is permissible for each positive integer u. The next lemma delivers a bound for permissible Δ_u obtained through our efficient differencing process.

Lemma 9.2. *Write* $\gamma = \gamma_q(k)$, *and let* r *be a fixed natural number. Define the real numbers* θ_s, Δ_s *and* λ_s *inductively by defining* $\theta_2 = 0$, $\Delta_2 = k-2$, $\lambda_2 = 2$, *and when* $s > 2$ *by taking*

$$\theta_s = \frac{1}{k + \Delta_{s-1}} + \left(\frac{1}{k} - \frac{1}{k + \Delta_{s-1}}\right)\left(\frac{k - \Delta_{s-1}}{2k}\right)^{\gamma - 1},$$

$$\Delta_s = \Delta_{s-1}(1 - \theta_s) + k\theta_s - 1,$$

and

$$\lambda_s = 2s - k + \Delta_s.$$

Then the exponent Δ_s *is permissible for* $2 \leqq s \leqq r$. *In particular, given* $\varepsilon > 0$, *there is a positive number* $\eta_0 = \eta_0(\varepsilon, r, k)$ *with the property that whenever* $0 < \eta < \eta_0$, *one has* $S_s(P, \eta P) \ll \hat{P}^{\lambda_s + \varepsilon}$.

Proof. We establish the desired conclusion by induction on s. The conclusion of the lemma for $s = 2$ follows at once from Lemma 9.1. Suppose then that the conclusion of the lemma has been confirmed when $2 \leqq s \leqq u$. We apply Lemmata 8.2 and 8.3 to bound $S_{u+1}(P, \eta P)$ by making use of the trivial upper bound $S_{u+1}(P, \eta P) \leqq S_u(P, Q_0, R; \Psi_0)$, with $R = \eta P$, $Q_0 = P$ and $\Psi_0 = z^k$. With each application of Lemma 8.3, we make a choice for the associated parameter ϕ_{j+1} in such a manner that the two terms on the right-hand side are of similar order of magnitude, thereby optimising the ensuing upper bound for $T_u(P, Q_j, R; \phi_{j+1}; \Psi_j)$. In view of the inductive hypothesis and our conventions concerning ε and R, this choice for ϕ_{j+1} supplies the bound

$$T_u(P, Q_j, R; \phi_{j+1}; \Psi_j) \ll \hat{P}^{1+\varepsilon} \tilde{H}_j \tilde{M}_{j+1} \hat{Q}_{j+1}^{\lambda_u}. \tag{9.2}$$

We begin this process with $j = \gamma - 1$, and in this way successively define ϕ_j for $j = \gamma, \gamma - 1, \dots, 1$. At the final stage we are able to extract the desired upper bound for $S_u(P, Q_0, R; \Psi_0)$.

We begin by considering the mean value associated with the equation (7.4), and observe that by making a trivial estimate, one obtains

$$S_u(P, Q_\gamma, R; \Psi_\gamma) \ll \hat{P}^{2+\varepsilon} \tilde{H}_\gamma^2 \tilde{M}_\gamma^2 S_u(Q_\gamma, R).$$

An application of Lemma 8.3 now reveals that

$$T_u(P, Q_{\gamma-1}, R; \phi_\gamma; \Psi_{\gamma-1}) \ll T_1 + T_2, \tag{9.3}$$

where

$$T_1 = \hat{P}^{1+\varepsilon} \tilde{H}_{\gamma-1} \tilde{M}_\gamma S_u(Q_\gamma, R)$$

and

$$T_2 = \big(S_u(Q_\gamma, R)\big)^{1/2} \big(\hat{P}^{2+\varepsilon} \tilde{H}_\gamma^2 \tilde{M}_\gamma^2 S_u(Q_\gamma, R)\big)^{1/2}.$$

In order to minimise our estimate for $T_u(P, Q_{\gamma-1}, R; \phi_\gamma; \Psi_{\gamma-1})$, we make a choice for ϕ_γ in such a way that $T_1 \approx T_2$, that is

$$\hat{P} \tilde{H}_{\gamma-1} \tilde{M}_\gamma S_u(Q_\gamma, R) \approx \hat{P} \tilde{H}_\gamma \tilde{M}_\gamma S_u(Q_\gamma, R).$$

We therefore choose ϕ_γ so that $H_\gamma = 1$, which is to say $\phi_\gamma = 1/k$. Applying the inductive hypothesis for $S_u(Q_\gamma, R)$, we deduce from (9.3) that

$$T_u(P, Q_{\gamma-1}, R; \phi_\gamma; \Psi_{\gamma-1}) \ll \hat{P}^{1+\varepsilon} \tilde{H}_{\gamma-1} \tilde{M}_\gamma \hat{Q}_\gamma^{\lambda_u},$$

which confirms the estimate (9.2) in the case $j = \gamma - 1$.

Suppose next that $j \geqq 0$, and that we have fixed choices for ϕ_i when $\gamma \geqq i \geqq j + 1$, and further that we have established the bound (9.2). The conclusion of the previous para-

graph establishes such when $j = \gamma - 1$. On substituting (9.2) into the conclusion of Lemma 8.2, we obtain the upper bound

$$S_u(P, Q_j, R; \Psi_j) \ll \hat{P}^{1+\varepsilon} \hat{M}_{j+1}^{2u} \tilde{H}_j^2 \tilde{M}_j^2 \hat{Q}_{j+1}^{\lambda_u}.$$

Substituting this bound into the conclusion of Lemma 8.3, and applying the inductive hypothesis for $S_u(Q_j, R)$, we deduce that

$$T_u(P, Q_{j-1}, R; \phi_j; \Psi_{j-1}) \ll \hat{P}^{\varepsilon}(T_3 + T_4), \tag{9.4}$$

where

$$T_3 = \hat{P} \tilde{H}_{j-1} \tilde{M}_j \hat{Q}_j^{\lambda_u},$$

and

$$T_4 = (\hat{P} \hat{M}_{j+1}^{2u} \tilde{H}_j^2 \tilde{M}_j^2 \hat{Q}_{j+1}^{\lambda_u})^{1/2} (\hat{Q}_j^{\lambda_u})^{1/2}.$$

We minimise our estimate for $T_u(P, Q_{j-1}, R; \phi_j; \Psi_{j-1})$ by choosing ϕ_j in such a manner that $T_3 \approx T_4$, that is

$$(\hat{P} \tilde{H}_{j-1} \tilde{M}_j \hat{Q}_j^{\lambda_u})^2 \approx \hat{P} \hat{M}_{j+1}^{2u} \tilde{H}_j^2 \tilde{M}_j^2 \hat{Q}_{j+1}^{\lambda_u} \hat{Q}_j^{\lambda_u}.$$

We choose ϕ_j so that

$$1 + \lambda_u(1 - \Phi_j) = 2 - 2k\phi_j + 2u\phi_{j+1} + \lambda_u(1 - \Phi_j - \phi_{j+1}),$$

or equivalently,

$$\phi_j = \frac{1 + (k - \Delta_u)\phi_{j+1}}{2k}.$$

With this choice of ϕ_j, it follows from (9.4) that the estimate (9.2) holds with $j - 1$ in place of j, and this completes the inductive step.

Thus far we have fixed choices for ϕ_j ($\gamma \geqq j \geqq 1$) via the relations

$$\phi_\gamma = \frac{1}{k} \quad \text{and} \quad \phi_j = \frac{1 + (k - \Delta_u)\phi_{j+1}}{2k} \quad (1 \leqq j \leqq \gamma - 1).$$

It follows that for $j = 1, 2, \ldots, \gamma$, one has

$$\phi_j = \frac{1}{k + \Delta_u} + \left(\frac{1}{k} - \frac{1}{k + \Delta_u}\right)\left(\frac{k - \Delta_u}{2k}\right)^{\gamma - j}.$$

In particular, we have

$$\phi_1 = \frac{1}{k + \Delta_u} + \left(\frac{1}{k} - \frac{1}{k + \Delta_u}\right)\left(\frac{k - \Delta_u}{2k}\right)^{\gamma - 1}.$$

With this choice of ϕ_j $(1 \leqq j \leqq \gamma)$, it follows from (9.2) that

$$T_u(P, Q_0, R; \phi_1; \Psi_0) \ll \hat{P}^{1+\varepsilon} \hat{M}_1 \hat{Q}_1^{\lambda_u}.$$

We therefore deduce from Lemma 8.2 that

$$S_u(P, Q_0, R; \Psi_0) \ll \hat{P}^{1+\varepsilon} \hat{M}_1^{2u} \hat{Q}_1^{\lambda_u}, \tag{9.5}$$

and it follows that

$$S_{u+1}(P, R) \ll \hat{P}^{\lambda_{u+1}+\varepsilon}, \tag{9.6}$$

with $\lambda_{u+1} = \lambda_u(1 - \phi_1) + 1 + 2u\phi_1$. Thus, if we write θ_{u+1} in place of ϕ_1, we find that the exponent Δ_{u+1} is permissible, where $\Delta_{u+1} = \Delta_u(1 - \theta_{u+1}) + k\theta_{u+1} - 1$. The conclusion of the lemma now follows in all details.

We record a further consequence of the argument employed in the proof of Lemma 9.2 as an associated lemma.

Lemma 9.3. *Define the exponents λ_s $(2 \leqq s \leqq r)$ as in the statement of Lemma 9.2. Then one has*

$$\int_{\mathbb{T}} |F(\alpha; P)^2 f(\alpha; P, R)^{2s}| \, d\alpha \ll \hat{P}^{\lambda_{s+1}+\varepsilon} \quad (1 \leqq s < r).$$

Proof. We have only to observe that the upper bound (9.6) is extracted from (9.5), so that in fact one has $S_s(P, Q_0, R; \Psi_0) \ll \hat{P}^{\lambda_{s+1}+\varepsilon}$. But the latter supplies the conclusion of the present lemma.

The bound supplied by Lemma 9.3 has value in that two classical Weyl sums are present in the mean value, yet the estimate available for this mean value is not diminished in quality. Since classical Weyl sums are a valuable resource in analysing the major arc contribution, this simple observation has considerable utility. By modifying the argument of the proof of [28], Theorem 2.1, we are able to convert the conclusion of Lemma 9.2 into a convenient form of essentially the same strength.

Theorem 9.4. *Write $\gamma = \gamma_q(k)$, and let r be a fixed natural number. For each $s \in \mathbb{N}$ with $2 \leqq s \leqq r$, define the positive number $\delta_{s,k}$ by means of the equation*

$$\delta_{s,k} + \log \delta_{s,k} = \begin{cases} 1 - 2s/k, & \text{when } k \leqq 2^{\gamma-2}, \\ 1 - (2 - 2^{1-\gamma})s/k, & \text{when } k > 2^{\gamma-2}. \end{cases} \tag{9.7}$$

Then the exponent $\Delta_{s,k} = k\delta_{s,k}$ is permissible for $2 \leqq s \leqq r$. In particular, if we define

$$\lambda_s = \begin{cases} 2s - k + ke^{1-2s/k}, & \text{when } k \leqq 2^{\gamma-2}, \\ 2s - k + ke^{1-(2-2^{1-\gamma})s/k}, & \text{when } k > 2^{\gamma-2}, \end{cases}$$

then one has $S_s(P, R) \ll \hat{P}^{\lambda_s+\varepsilon}$ $(2 \leqq s \leqq r)$.

Proof. We prove the theorem by induction. We begin by noting that for each natural number s, the exponent $\delta_{s,k}$ satisfies the inequality $0 < \delta_{s,k} < 1$. In addition, it is apparent

that $\delta + \log\delta$ is an increasing function of δ when $\delta > 0$. In order to establish the conclusion of the theorem, therefore, it suffices to prove for each fixed s that

$$S_s(P,R) \ll \hat{P}^{2s-k+k\delta^*+\varepsilon}, \tag{9.8}$$

with δ^* a positive number satisfying the condition $\delta^* + \log\delta^* \leqq \delta_{s,k} + \log\delta_{s,k}$.

Consider first the case in which $s = 2$. Lemma 9.1 supplies the bound $S_2(P,R) \ll \hat{P}^{2+\varepsilon}$, so that $\Delta_{2,k} = k - 2$ is a permissible exponent. Moreover, one has

$$1 - 2/k + \log(1 - 2/k) < 1 - 4/k \leqq \delta_{2,k} + \log\delta_{2,k},$$

and so when $s = 2$ the upper bound (9.8) holds with $\delta^* \leqq \delta_{2,k}$. This confirms the desired conclusion when $s = 2$.

Suppose next that the first conclusion of the theorem holds for the index s, and write $\delta = \delta_{s,k}$. In addition, write $\lambda = 2s + 2 - k + \Delta$ with

$$\Delta = k\delta(1 - \phi_1) + k\phi_1 - 1, \tag{9.9}$$

and

$$k\phi_1 = \frac{1}{1+\delta} + \left(1 - \frac{1}{1+\delta}\right)\left(\frac{1-\delta}{2}\right)^{\gamma-1}. \tag{9.10}$$

Then it follows from Lemma 9.2 that $\Delta_{s+1,k} = \Delta$ is a permissible exponent and that $S_{s+1}(P,R) \ll \hat{P}^{\lambda+\varepsilon}$. We therefore seek to prove that

$$\Delta/k + \log(\Delta/k) \leqq \delta_{s+1,k} + \log\delta_{s+1,k}, \tag{9.11}$$

and from here the bound (9.8) follows with s replaced by $s + 1$, and with $\delta^* = \delta_{s+1,k}$. In view of our opening remarks, the first conclusion of the theorem will then follow by induction.

On substituting (9.10) into (9.9), we deduce that

$$\Delta = k\delta + k\phi_1(1-\delta) - 1 = k\delta + \frac{1-\delta}{1+\delta} + \frac{\delta(1-\delta)}{1+\delta}\left(\frac{1-\delta}{2}\right)^{\gamma-1} - 1.$$

On writing $w = (1-\delta)^{\gamma}2^{1-\gamma}$, we therefore see that

$$\begin{aligned}\frac{\Delta}{k} + \log\left(\frac{\Delta}{k}\right) &= \delta\left(1 - \frac{2-w}{k(1+\delta)}\right) + \log\delta + \log\left(1 - \frac{2-w}{k(1+\delta)}\right)\\ &\leqq \delta + \log\delta - \frac{(2-w)\delta}{k(1+\delta)} - \frac{2-w}{k(1+\delta)} - \frac{(2-w)^2}{2k^2(1+\delta)^2}\\ &\leqq \delta + \log\delta - \frac{2-w}{k} - \frac{(2-w)^2}{2k^2(1+\delta)^2}.\end{aligned}$$

We now recall that $0 < \delta < 1$, whence $w < 2^{1-\gamma}$. Also, since $\gamma \geqq 2$, one has

$$2 - w = 2 - (1-\delta)^{\gamma} 2^{1-\gamma} \geqq 2 - (1-\delta)^2/2 = \frac{1}{2}(1+\delta)(3-\delta).$$

Thus we deduce that

$$\frac{\Delta}{k} + \log\left(\frac{\Delta}{k}\right) \leqq \delta + \log\delta - \frac{2-w}{k} - \frac{(3-\delta)^2}{8k^2}.$$

It follows that for all values of γ, one has

$$\Delta/k + \log(\Delta/k) \leqq \delta + \log\delta - (2 - 2^{1-\gamma})/k, \tag{9.12}$$

and that whenever γ satisfies the condition $2^{\gamma-2} \geqq k$, then

$$\Delta/k + \log(\Delta/k) \leqq \delta + \log\delta - 2/k. \tag{9.13}$$

We now recall that $\delta = \delta_{s,k}$, so that from (9.7) and (9.13), one obtains

$$\Delta/k + \log(\Delta/k) \leqq 1 - (2s+2)/k = \delta_{s+1,k} + \log\delta_{s+1,k},$$

when $k \leqq 2^{\gamma-2}$, whilst for $k > 2^{\gamma-2}$, it follows from (9.7) and (9.12) that

$$\Delta/k + \log(\Delta/k) \leqq 1 - (2 - 2^{1-\gamma})(s+1)/k = \delta_{s+1,k} + \log\delta_{s+1,k}.$$

We have therefore confirmed the bound (9.11), whence the exponent $\Delta_{s+1,k} = k\delta_{s+1,k}$ is permissible whenever $\Delta_{s,k} = k\delta_{s,k}$ is permissible. This establishes the inductive step, and so the first conclusion of the theorem follows by induction. In order to complete the proof of the theorem, we have merely to note that from the first part, the exponent $\Delta_{s,k}$ is permissible whenever $\Delta_{s,k}$ is a positive number satisfying

$$\Delta_{s,k} e^{\Delta_{s,k}/k} = \begin{cases} ke^{1-2s/k}, & \text{when } k \leqq 2^{\gamma-2}, \\ ke^{1-(2-2^{1-\gamma})s/k}, & \text{when } k > 2^{\gamma-2}. \end{cases} \tag{9.14}$$

But then $0 \leqq \Delta_{s,k} \leqq k$, and so the right-hand side of (9.14) provides an upper bound for $\Delta_{s,k}$.

10. Estimates for smooth Weyl sums: preliminaries

The goal of this and the following three sections is to convert our newly obtained mean value estimates for smooth Weyl sums into estimates for individual smooth Weyl sums on the set of minor arcs $\mathfrak{p}$. In order to derive such estimates we adapt the argument of [29], involving the use of the large sieve inequality, to the setting of $\mathbb{F}_q[t]$. Before advancing in the next section to the pursuit of useable estimates, we begin in this section with some preliminary manoeuvres.

Lemma 10.1. *When $\theta \in \mathbb{K}_\infty$ and m is a non-negative integer, one has*

$$\sum_{\langle x\rangle<\hat{m}} e(\theta x) = \begin{cases} \hat{m}, & \text{when } \operatorname{ord}\|\theta\| < -m, \\ 0, & \text{when } \operatorname{ord}\|\theta\| \geqq -m. \end{cases}$$

Proof. This is [14], Lemma 7.

When Q is a natural number, and $\pi \in \mathbb{F}_q[t]$ is irreducible, define

$$\mathscr{A}^*(Q,\pi) = \{x \in \mathbb{F}_q[t] : \langle x\rangle \leqq \hat{Q},\ \varpi \,|\, x \Rightarrow \varpi \trianglelefteqq \pi\},$$

in which the relation $\trianglelefteqq$ is that defined in the preamble to Lemma 3.1. Notice that $\mathscr{A}^*(Q,\pi) \subseteqq \mathscr{A}(Q, \operatorname{ord}\pi)$. The next lemma is an analogue of [22], Lemma 10.1.

Lemma 10.2. *Suppose that R, M and Q are positive numbers, that $y \in \mathscr{A}(Q,R)$, and in addition $1 \leqq R \leqq M < \operatorname{ord} y \leqq Q$. Then there is a unique triple (π,u,v), with π irreducible and v monic, satisfying the following conditions*:

(i) $y = uv$,

(ii) $u \in \mathscr{A}^*(Q - \operatorname{ord} v, \pi)$,

(iii) $M < \operatorname{ord} v \leqq M + \operatorname{ord}\pi$,

(iv) $\pi \,|\, v$,

(v) *whenever ϖ is a monic irreducible polynomial with $\varpi \,|\, v$, one has $\pi \trianglelefteqq \varpi$ and* $\operatorname{ord}\varpi \leqq R$.

Proof. Consider natural numbers R, M, Q and an element $y \in \mathscr{A}(Q,R)$ satisfying the hypotheses of the statement of the lemma. We begin by establishing the existence of a triple (π,u,v) with π irreducible and v monic, and satisfying the conditions (i)–(v). Observe first that when $y \in \mathscr{A}(Q,R)$, then in view of (2.2) we may write $y = c\varpi_1\varpi_2\dots\varpi_\sigma$ with $c \in \mathbb{F}_q^\times$, and with ϖ_i $(1 \leqq i \leqq \sigma)$ monic irreducible polynomials satisfying $\varpi_1 \trianglerighteqq \varpi_2 \trianglerighteqq \cdots \trianglerighteqq \varpi_\sigma$ and $\operatorname{ord}\varpi_1 \leqq R$. Let

$$d_0 = 1 \quad \text{and} \quad d_j = \prod_{1\leqq i\leqq j} \varpi_i \quad (1 \leqq j \leqq \sigma).$$

Then

$$0 = \operatorname{ord} d_0 < \operatorname{ord} d_1 < \cdots < \operatorname{ord} d_\sigma = \operatorname{ord} y.$$

Since $\operatorname{ord} y > R$ and $y \in \mathscr{A}(Q,R)$, one necessarily has $\sigma \geqq 2$. But $0 < M < \operatorname{ord} y$, and so there exists a natural number τ with $\operatorname{ord} d_\tau \leqq M < \operatorname{ord} d_{\tau+1}$. Moreover, since $R \leqq M < \operatorname{ord} y$, it is apparent that $1 \leqq \tau < \sigma$. Consequently,

$$M < \operatorname{ord} d_{\tau+1} = \operatorname{ord}(d_\tau\varpi_{\tau+1}) \leqq M + \operatorname{ord}\varpi_{\tau+1}.$$

We now take $\pi = \varpi_{\tau+1}$, $v = d_{\tau+1}$ and $u = y/v$, and observe that (π,u,v) satisfies all of the conditions imposed on the triple in the statement of the lemma.

Next we establish the uniqueness of the triple (π, u, v). Suppose that the triples (π_i, u_i, v_i) $(i = 1, 2)$ both satisfy the conditions imposed on (π, u, v) in the statement of the lemma, save that subscripts are applied to the variables in the obvious manner. If the two triples are distinct, there is plainly no loss of generality in supposing that either $\pi_1 \prec \pi_2$, or else that $\pi_1 = \pi_2$ and $v_1 \succ v_2$. For $i = 1, 2$, let w_i denote the product of all the monic irreducible factors ϖ of y with $\varpi \succ \pi_i$. Then for $i = 1, 2$, it is apparent that $v_i = \pi_i^{h_i} w_i$ for some exponent h_i with $h_i \geqq 1$. If $\pi_1 \prec \pi_2$, then $v_2 \mid w_1$, and so it follows from the condition (iii) that

$$\operatorname{ord} v_1 \geqq \operatorname{ord} \pi_1 + \operatorname{ord} v_2 > \operatorname{ord} \pi_1 + M. \tag{10.1}$$

But, also in view of the condition (iii), one has $\operatorname{ord} v_1 \leqq M + \operatorname{ord} \pi_1$. We therefore arrive at a contradiction, and so we are forced instead to assume that $\pi_1 = \pi_2$ and $v_1 \succ v_2$. The first of the latter two conditions implies that $w_1 = w_2$, whence the second leads us to the condition $h_1 > h_2$. But then we once again obtain the inequality (10.1), contradicting condition (iii) as before. We therefore conclude that the triples (π_i, u_i, v_i) $(i = 1, 2)$ are identical, and so the triple (π, u, v), whose existence is asserted in the statement of the lemma, is in fact unique. This completes the proof of the lemma.

We next employ this combinatorial decomposition of the set $\mathscr{A}(Q, R)$ so as to rewrite smooth Weyl sums in a potentially bilinear form. In order to assist in this endeavour, when M and R are positive numbers with $1 \leqq R \leqq M$, and π is a monic irreducible polynomial with $\operatorname{ord} \pi \leqq R$, we define $\mathscr{B}(M, \pi, R)$ to be the set of monic polynomials $v \in \mathbb{F}_q[t]$ for which $M < \operatorname{ord} v \leqq M + \operatorname{ord} \pi$, $\pi \mid v$, and such that whenever ϖ is a monic irreducible polynomial dividing v, then $\varpi \geqq \pi$ and $\operatorname{ord} \varpi \leqq R$.

Lemma 10.3. *Let $\alpha \in \mathbb{K}_\infty$. Then whenever R, M and Q are positive numbers with $1 \leqq R \leqq M < Q$ and $r \in \mathbb{F}_q[t] \backslash \{0\}$, one has*

$$\sum_{\substack{x \in \mathscr{A}(Q,R) \\ (x,r)=1}} e(\alpha x^k) \ll \hat{R} \max_{\substack{\pi \text{ irreducible} \\ \operatorname{ord} \pi \leqq R}} \sup_{\theta \in \mathbb{T}} V_r(\alpha; Q, M, R; \pi; \theta) + \hat{M},$$

where

$$V_r(\alpha; Q, M, R; \pi; \theta) = \sum_{\substack{v \in \mathscr{B}(M,\pi,R) \\ (v,r)=1}} \Big| \sum_{\substack{u \in \mathscr{A}^*(Q-M,\pi) \\ (u,r)=1}} e\big(\alpha(uv)^k + \theta u\big) \Big|.$$

Proof. We make use of Lemma 10.2 to decompose the smooth Weyl sum in question in the form

$$\begin{aligned} \sum_{\substack{x \in \mathscr{A}(Q,R) \\ (x,r)=1}} e(\alpha x^k) &= \sum_{\substack{x \in \mathscr{A}(Q,R) \\ \operatorname{ord} x \leqq M \\ (x,r)=1}} e(\alpha x^k) + \sum_{\substack{x \in \mathscr{A}(Q,R) \\ \operatorname{ord} x > M \\ (x,r)=1}} e(\alpha x^k) \\ &\ll \hat{M} + \sum_{\substack{\pi \\ \operatorname{ord} \pi \leqq R \\ (\pi,r)=1}}^{\dagger} |W_{r,\pi}(\alpha; Q, R)|, \end{aligned} \tag{10.2}$$

where we have written

$$W_{r,\pi}(\alpha; Q, R) = \sum_{\substack{v \in \mathscr{B}(M,\pi,R) \\ (v,r)=1}} \sum_{\substack{u \in \mathscr{A}^*(Q-\operatorname{ord} v,\pi) \\ (u,r)=1}} e\big(\alpha(uv)^k\big).$$

But if we write

$$W^+_{r,\pi}(\alpha,\theta;Q,M,R)=\sum_{\substack{v\in\mathscr{B}(M,\pi,R)\\(v,r)=1}}\sum_{\substack{u\in\mathscr{A}^*(Q-M,\pi)\\(u,r)=1}}e\big(\alpha(uv)^k+\theta u\big),$$

then it follows that

$$W_{r,\pi}(\alpha;Q,R)=\int_{\mathbb{T}}W^+_{r,\pi}(\alpha,\theta;Q,M,R)\sum_{\langle x\rangle\leqq\hat{Q}\langle v\rangle^{-1}}e(-\theta x)\,d\theta.$$

We next observe that by Lemma 10.1, provided that $\langle v\rangle\leqq\hat{Q}$, one has

$$\int_{\mathbb{T}}\Big|\sum_{\langle x\rangle\leqq\hat{Q}\langle v\rangle^{-1}}e(\theta x)\Big|\,d\theta=\int_{\langle\theta\rangle<q^{-1}\hat{Q}^{-1}\langle v\rangle}q\hat{Q}\langle v\rangle^{-1}\,d\theta=1.$$

Thus we conclude that

$$W_{r,\pi}(\alpha;Q,R)\leqq\sup_{\theta\in\mathbb{T}}|W^+_{r,\pi}(\alpha,\theta;Q,M,R)|. \tag{10.3}$$

On substituting (10.3) into (10.2), the conclusion of the lemma now follows on summing trivially over π and applying the triangle inequality.

11. Estimates for smooth Weyl sums: large moduli

The argument that we apply to estimate the smooth Weyl sum $f(\alpha;P,R)$ proceeds in two phases. In one stage we apply the large sieve inequality to estimate $f(\alpha;P,R)$. This treatment provides a satisfactory bound whenever α is well approximated by a ratio a/g of polynomials with $\langle g\rangle$ small. In the second stage one applies a treatment employing bilinear sums that yields viable estimates in the complementary situation in which α is well-approximated only by ratios a/g in which $\langle g\rangle$ is necessarily large. In this section we tackle the latter situation, beginning with an auxiliary lemma on bilinear sums.

Lemma 11.1. *Suppose that $\alpha\in\mathbb{K}_\infty$, and that a and g are elements of $\mathbb{F}_q[t]$ with g monic, $(a,g)=1$ and $\langle g\alpha-a\rangle<\langle g\rangle^{-1}$. Then whenever $C,D\in\mathbb{N}$, one has*

$$\sum_{\langle c\rangle<\hat{C}}\Big|\sum_{\langle d\rangle<\hat{D}}e(\alpha cd)\Big|\ll\hat{C}\hat{D}\big(\langle g\rangle^{-1}+\hat{C}^{-1}+\hat{D}^{-1}+\langle g\rangle(\hat{C}\hat{D})^{-1}\big). \tag{11.1}$$

Proof. We begin by observing that, in view of the conclusion of Lemma 10.1, the inner sum on the left-hand side of (11.1) is either $\hat{D}$ or 0, depending on whether $\operatorname{ord}\|\alpha c\|<-D$ or $\operatorname{ord}\|\alpha c\|\geqq-D$. Suppose that α, a and g satisfy the hypotheses of the statement of the lemma. Then by dividing the range of summation for c into arithmetic progressions modulo g, we deduce that

$$\sum_{\langle c\rangle<\hat{C}}\Big|\sum_{\langle d\rangle<\hat{D}}e(\alpha cd)\Big|\leqq\hat{D}\sum_{\langle w\rangle<\hat{C}\langle g\rangle^{-1}}\sum_{\substack{\langle r\rangle<\langle g\rangle\\ \operatorname{ord}\|\alpha(r+gw)\|<-D}}1. \tag{11.2}$$

Consider a fixed choice of $w\in\mathbb{F}_q[t]$, and, if one exists, a fixed choice of r satisfying the conditions imposed by the inner summation on the right-hand side of (11.2). If r' is any

other polynomial with $\langle r' \rangle < \langle g \rangle$ that also satisfies $\operatorname{ord}\|\alpha(r' + gw)\| < -D$, then necessarily $\operatorname{ord}\|\alpha(r - r')\| < -D$. Write $\alpha = a/g + \beta$, and observe that

$$\operatorname{ord}\|\alpha(r - r')\| \leqq \operatorname{ord}\|a(r - r')/g\| + \operatorname{ord}\|\beta(r - r')\|.$$

Since by hypothesis, one has $\langle \beta \rangle < \langle g \rangle^{-2}$, we see that

$$\operatorname{ord}\|\beta(r - r')\| = \operatorname{ord}\beta + \operatorname{ord}(r - r') < -2(\operatorname{ord} g) + \operatorname{ord} g = -\operatorname{ord} g.$$

Meanwhile, when $r \neq r'$, we have $a(r - r') \not\equiv 0 \pmod{g}$, whence $\operatorname{ord}\|a(r - r')/g\| \geqq -\operatorname{ord} g$. We therefore deduce that, whether or not $r \neq r'$, one has $\operatorname{ord}\|\alpha(r - r')\| = \operatorname{ord}\|a(r - r')/g\|$, and that whenever r and r' both occur in the inner summation on the right-hand side of (11.2), then necessarily $\operatorname{ord}\|a(r - r')/g\| < -D$. By rearranging the latter summation, we therefore conclude that

$$\sum_{\langle c \rangle < \hat{C}} \left| \sum_{\langle d \rangle < \hat{D}} e(\alpha cd) \right| \leqq \hat{D} \sum_{\langle w \rangle < \hat{C}\langle g \rangle^{-1}} \sum_{\substack{\langle h \rangle < \langle g \rangle \\ \operatorname{ord}\|ah/g\| < -D}} 1. \tag{11.3}$$

Since $(a, g) = 1$, it follows that as h runs over a complete residue system modulo g, then so does ah. Suppose now that $y \in \mathbb{F}_q[t]$ satisfies $\langle y \rangle < \langle g \rangle$, and consider what it means for $\operatorname{ord}\|y/g\| < -D$. When $\langle g \rangle \leqq \hat{D}$, one has $\operatorname{ord}\|y/g\| < -D$ if and only if $g \mid y$. When $\langle g \rangle > \hat{D}$, meanwhile, one has $\operatorname{ord}\|y/g\| < -D$ if and only if $\langle y \rangle < \langle g \rangle \hat{D}^{-1}$. It follows that there are precisely $\max\{1, \langle g \rangle \hat{D}^{-1}\}$ residue classes y modulo g for which $\operatorname{ord}\|y/g\| < -D$, whence from (11.3),

$$\begin{aligned} \sum_{\langle c \rangle < \hat{C}} \left| \sum_{\langle d \rangle < \hat{D}} e(\alpha cd) \right| &\leqq \hat{D}(1 + \hat{C}\langle g \rangle^{-1})(1 + \langle g \rangle \hat{D}^{-1}) \\ &= \hat{C}\hat{D}\big(\langle g \rangle^{-1} + \hat{C}^{-1} + \hat{D}^{-1} + \langle g \rangle (\hat{C}\hat{D})^{-1}\big). \end{aligned}$$

This completes the proof of the lemma.

The next lemma, which provides upper bounds for $f(\alpha; P, R)$ of use when α is not well-approximated by ratios a/g with $\langle g \rangle$ small, is established via an analogue of the argument used to prove [29], Lemma 3.1.

Lemma 11.2. *Suppose that λ is a real number with $1/2 < \lambda < 1$, and write $M = \lambda P$. Let $\alpha \in \mathbb{K}_\infty$, and suppose that a and g are elements of $\mathbb{F}_q[t]$ with g monic, $(a, g) = 1$ and $\langle g\alpha - a \rangle < \langle g \rangle^{-1}$. Then whenever $l, w \in \mathbb{N}$, and Δ_l and Δ_w are permissible, one has*

$$f(\alpha; P, R) \ll \hat{P}^{1+\varepsilon}\big(\hat{M}^{\Delta_w}(\hat{P}/\hat{M})^{\Delta_l}\Xi_k(g; P, M)\big)^{1/(2lw)} + \hat{M},$$

where

$$\Xi_k(g; P, M) = \langle g \rangle^{-1} + \hat{M}^{-k} + (\hat{P}/\hat{M})^{-k} + \langle g \rangle \hat{P}^{-k}.$$

Proof. An application of Lemma 10.3 with $r = 1$ shows that there exists an irreducible polynomial π with $\operatorname{ord}\pi \leqq R$, and an element $\theta \in \mathbb{T}$, for which

$$f(\alpha; P, R) \ll \hat{R}\mathscr{H}(\alpha) + \hat{M}, \tag{11.4}$$

where we have written

$$\mathscr{H}(\alpha) = \sum_{v \in \mathscr{A}(M+R,R)} |h(\alpha; v, \theta)|,$$

with

$$h(\alpha; v, \theta) = \sum_{u \in \mathscr{A}^*(P-M,\pi)} e\big(\alpha(uv)^k + \theta u\big).$$

Define the complex numbers of unit modulus $\varepsilon(v,\theta)$ by means of the relation

$$|h(\alpha; v, \theta)|^l = \varepsilon(v,\theta) h(\alpha; v, \theta)^l.$$

Here we adopt the convention that when $h(\alpha; v, \theta) = 0$, then we take $\varepsilon(v,\theta) = 1$. Next, when $d \in \mathbb{F}_q[t]$, we take r_d to be the number of solutions of the equation $u_1^k + \cdots + u_l^k = d$, with $u_i \in \mathscr{A}^*(P-M,\pi)$ $(1 \leqq i \leqq l)$, in which each solution $\boldsymbol{u}$ is counted with weight $e\big(\theta(u_1 + \cdots + u_l)\big)$. Thus we find that

$$h(\alpha; v, \theta)^l = \sum_{\langle d \rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} r_d e(\alpha\, dv^k).$$

A swift application of Hölder's inequality consequently leads from here to the estimate

$$\begin{aligned} \mathscr{H}(\alpha)^l &\ll (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{l-1} \sum_{v \in \mathscr{A}(M+R,R)} |h(\alpha; v, \theta)|^l \\ &= (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{l-1} \sum_{\langle d \rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} r_d \mathfrak{h}(\alpha; d, \theta), \end{aligned} \tag{11.5}$$

where we have written

$$\mathfrak{h}(\alpha; d, \theta) = \sum_{v \in \mathscr{A}(M+R,R)} \varepsilon(v,\theta) e(\alpha\, dv^k).$$

Now let n_d denote the number of solutions of the equation $u_1^k + \cdots + u_l^k = d$, with $u_i \in \mathscr{A}(P-M, \operatorname{ord}\pi)$, counted without weights. Thus, in particular, for each polynomial d one has $|r_d| \leqq n_d$. A further application of Hölder's inequality leads from (11.5) to the bound

$$\mathscr{H}(\alpha)^{2lw} \leqq (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{2w(l-1)} \Big(\sum_d n_d \Big)^{2w-2} \Big(\sum_d n_d^2 \Big) J_w(\alpha),$$

in which the summations on the right-hand side are over all polynomials $d \in \mathbb{F}_q[t]$, and where we have written

$$J_w(\alpha) = \sum_{\langle d \rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} |\mathfrak{h}(\alpha; d, \theta)|^{2w}. \tag{11.6}$$

But by considering the underlying equations, it is apparent that

$$\sum_d n_d \leqq (q\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^l \quad \text{and} \quad \sum_d n_d^2 \leqq S_l(P-M,R),$$

and hence

$$\mathscr{H}(\alpha)^{2lw} \ll (\hat{\boldsymbol{P}}\hat{\boldsymbol{R}})^{2lw} (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-2l} (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-2w} S_l(P-M,R) J_w(\alpha). \tag{11.7}$$

Next we write

$$\tilde{n}_c = \int_{\mathbb{T}} |\mathfrak{h}(\beta; d, \theta)|^{2w} e(-\beta c d)\, d\beta.$$

Then it follows from orthogonality that $\tilde{n}_c$ is equal to the number of solutions of the equation

$$\sum_{i=1}^{w} (v_i^k - v_{w+i}^k) = c,$$

with $v_i \in \mathscr{A}(M+R, R)$ $(1 \leqq i \leqq 2w)$, wherein each solution $\boldsymbol{v}$ is counted with weight

$$\prod_{i=1}^{w} \varepsilon(v_i, \theta)\overline{\varepsilon(v_{w+i}, \theta)}.$$

Since $|\varepsilon(v, \theta)| = 1$ for each v, an application of the triangle inequality, combined with a consideration of the underlying equation, leads to the upper bound

$$\tilde{n}_c \leqq \tilde{n}_0 \leqq S_w(M+R, R).$$

Thus it follows from (11.6) that

$$J_w(\alpha) = \sum_{\langle d\rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} \sum_{\langle c\rangle \leqq (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^k} \tilde{n}_c e(\alpha c d) \ll S_w(M+R, R)\mathscr{R}(\alpha), \tag{11.8}$$

where

$$\mathscr{R}(\alpha) = \sum_{\langle c\rangle \leqq (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^k} \Big| \sum_{\langle d\rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} e(\alpha c d) \Big|.$$

Applying Lemma 11.1 with $C = k(M+R)+1$ and $D = k(P-M)+1$, we obtain the estimate

$$\mathscr{R}(\alpha) \ll (\hat{\boldsymbol{P}}\hat{\boldsymbol{R}})^k \big(\langle g\rangle^{-1} + (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-k} + (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-k} + \langle g\rangle (\hat{\boldsymbol{P}}\hat{\boldsymbol{R}})^{-k} \big). \tag{11.9}$$

On collecting together the upper bounds (11.7), (11.8) and (11.9), and noting that Δ_l and Δ_w are permissible exponents, we arrive at the upper bound

$$\begin{aligned} \mathscr{H}(\alpha) &\ll \hat{\boldsymbol{P}}\hat{\boldsymbol{R}} \big((\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-k+\Delta_l} (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-k+\Delta_w} \mathscr{R}(\alpha) \big)^{1/(2lw)} \\ &\ll \hat{\boldsymbol{P}}^{1+\varepsilon} \big((\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{\Delta_l} \hat{\boldsymbol{M}}^{\Delta_w} \Xi_k(g; P, M) \big)^{1/(2lw)}. \end{aligned}$$

The conclusion of the lemma now follows on substituting this bound into (11.4).

12. Estimates for smooth Weyl sums: small moduli

We now examine the smooth Weyl sum $f(\alpha; P, R)$ when α is well-approximated by a ratio a/g in which $\langle g\rangle$ is relatively small. Here we apply a variant of Vinogradov's method

modelled on the argument of [29], Lemma 4.1. We recall and emphasise at this point that we assume throughout that $\mathrm{ch}(\mathbb{F}_q) \nmid k$.

Lemma 12.1. *Suppose that λ is a real number with $1/2 < \lambda < 1$, and write $M = \lambda P$. Let $\alpha \in \mathbb{K}_\infty$, and suppose that a and g are elements of $\mathbb{F}_q[t]$ with g monic, $(a,g) = 1$ and $\langle g\alpha - a\rangle < (\hat{M}\hat{R})^{-k}$, $\langle g\rangle \leqq (\hat{M}\hat{R})^k$, and either $\langle g\alpha - a\rangle \geqq \hat{M}\hat{P}^{-k}$ or $\langle g\rangle > \hat{M}\hat{R}$. Then whenever s is a natural number satisfying $2s \geqq k+1$ and Δ_s is permissible, one has*

$$f(\alpha; P, R) \ll \hat{P}^\varepsilon \hat{M} + \hat{P}^{1+\varepsilon}\big(\hat{M}^{-1}(\hat{P}/\hat{M})^{\Delta_s}\big(1 + \langle g\rangle(\hat{P}/\hat{M})^{-k}\big)\big)^{1/(2s)}.$$

Proof. The bilinear decomposition that enables us to apply the large sieve in this instance is a little more delicate than that applied in the proof of Lemma 11.2. We begin by recalling the definition of the set $\mathscr{C}_g(L)$ from the preamble to Lemma 7.1. Suppose that α, a and g satisfy the hypotheses of the statement of the lemma. We observe that each element y in $\mathscr{A}(P,R)$ may be written uniquely in the form $y = xd$, with $d \in \mathscr{C}_g(P)$ and $x \in \mathscr{A}(P - \operatorname{ord} d, R)$ satisfying $(x,g) = 1$. The smooth Weyl sum $f(\alpha; P, R)$ defined in (2.3) may therefore be rewritten in the shape

$$f(\alpha; P, R) = \sum_{d \in \mathscr{C}_g(P) \cap \mathscr{A}(P,R)} \sum_{\substack{x \in \mathscr{A}(P - \operatorname{ord} d, R) \\ (x,g)=1}} e\big(\alpha(xd)^k\big).$$

An application of Lemma 7.1 now reveals that

$$\begin{aligned} f(\alpha; P, R) &\ll \sum_{d \in \mathscr{C}_g(P-M)} \Big| \sum_{\substack{x \in \mathscr{A}(P - \operatorname{ord} d, R) \\ (x,g)=1}} e\big(\alpha(xd)^k\big)\Big| + \sum_{\substack{d \in \mathscr{C}_g(P) \\ \operatorname{ord} d > P - M}} \hat{P}/\langle d\rangle \\ &\ll \hat{P}^\varepsilon \max_{d \in \mathscr{C}_g(P-M)} \Big| \sum_{\substack{x \in \mathscr{A}(P - \operatorname{ord} d, R) \\ (x,g)=1}} e\big(\alpha(xd)^k\big)\Big| + \hat{P}^\varepsilon \hat{M}. \end{aligned}$$

When $d \in \mathscr{C}_g(P-M)$, one has $M - \operatorname{ord} d \geqq M - (P-M) = (2\lambda - 1)P > 0$. It therefore follows from Lemma 10.3 that there exists a polynomial $d \in \mathscr{C}_g(P-M)$, an irreducible polynomial π with $\operatorname{ord}\pi \leqq R$, and an element $\theta \in \mathbb{T}$, such that

$$f(\alpha; P, R) \ll \hat{P}^\varepsilon \hat{M} + \hat{P}^\varepsilon \hat{R}\mathfrak{g}(\alpha; d, \pi, \theta), \tag{12.1}$$

where

$$\mathfrak{g}(\alpha; d, \pi, \theta) = \sum_{\substack{v \in \mathscr{B}(M - \operatorname{ord} d, \pi, R) \\ (v,g)=1}} \Big| \sum_{\substack{u \in \mathscr{A}^*(P-M, \pi) \\ (u,g)=1}} e\big(\alpha(uvd)^k + \theta u\big)\Big|. \tag{12.2}$$

Let $J(g,d,h)$ denote the number of solutions of the congruence $(xd)^k \equiv h \pmod g$ with $\langle x\rangle < \langle g\rangle$ and $(x,g) = 1$. When $(h,g) \nmid d^k$, one plainly has $J(g,d,h) = 0$. Suppose then that $(h,g) \mid d^k$, and write $h' = h/(h,g)$ and $g' = g/(h,g)$. Then $J(g,d,h)$ is equal to $\langle (h,g)\rangle$ multiplied by the number of solutions of the congruence

$$x^k d^k/(h,g) \equiv h' \pmod{g'}, \tag{12.3}$$

with $\langle x\rangle < \langle g'\rangle$. Since $(h', g') = 1$, the number of solutions of this congruence is at most $O(\langle g'\rangle^{\varepsilon})$. In order to verify this assertion, observe first that for each irreducible divisor ϖ of g', the number of solutions of the congruence $x^k d^k/(h,g) \equiv h' \pmod{\varpi}$ is at most k. Moreover, since any solution x of (12.3) necessarily satisfies $(x, g') = 1$, and $\mathrm{ch}(\mathbb{F}_q) \nmid k$, it follows from Hensel's Lemma that each solution of the latter congruence lifts uniquely to a corresponding solution x modulo ϖ^l, for each natural number l. The Chinese Remainder Theorem consequently ensures that the number of solutions of (12.3) with $\langle x\rangle < \langle g'\rangle$ is at most $k^{\omega(g')}$, and so the desired conclusion follows from Corollary 7.2. In this way, we deduce that

$$J(g,d,h) \ll \langle g\rangle^{\varepsilon}\langle (h,g)\rangle \ll \langle g\rangle^{\varepsilon}\langle d\rangle^{k}. \tag{12.4}$$

Let $\mathscr{V}$ denote the set of monic polynomials v with $\hat{\boldsymbol{M}}/\langle d\rangle < \langle v\rangle \leqq \hat{\boldsymbol{M}}\hat{\boldsymbol{R}}/\langle d\rangle$ and $(v, g) = 1$. Then in view of the estimate (12.4), there exists a natural number L, satisfying $L \ll \langle g\rangle^{\varepsilon}\langle d\rangle^{k}$, with the following property. The set $\mathscr{V}$ can be divided into L classes $\mathscr{V}_1, \dots, \mathscr{V}_L$ such that, for any two distinct elements v_1, v_2 in a given set $\mathscr{V}_j$, we have $(v_1 d)^k \equiv (v_2 d)^k \pmod{g}$ if and only if $v_1 \equiv v_2 \pmod{g}$. Let b_y denote the number of solutions of the equation $u_1^k + \cdots + u_s^k = y$ with $u_i \in \mathscr{A}^*(P - M, \pi)$ and $(u_i, g) = 1$ $(1 \leqq i \leqq s)$, in which each solution $\boldsymbol{u}$ is counted with weight $e\big(\theta(u_1 + \cdots + u_s)\big)$. Then an application of Hölder's inequality to (12.2) yields the estimate

$$\mathfrak{g}(\alpha; d, \pi, \theta)^{2s} \ll \hat{\boldsymbol{P}}^{\varepsilon}\langle d\rangle^{k}(\hat{\boldsymbol{M}}\hat{\boldsymbol{R}}/\langle d\rangle)^{2s-1} \max_{1\leqq j\leqq L} \sum_{v\in\mathscr{V}_j} \Big| \sum_{\langle y\rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} b_y e\big(\alpha(vd)^k y\big)\Big|^2.$$

The hypotheses of the statement of the lemma permit us to assume that $2s - 1 \geqq k$. It therefore follows that there is an integer j, with $1 \leqq j \leqq L$, for which

$$\mathfrak{g}(\alpha; d, \pi, \theta)^{2s} \ll \hat{\boldsymbol{P}}^{\varepsilon}(\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{2s-1} \sum_{v\in\mathscr{V}_j} \Big| \sum_{\langle y\rangle \leqq (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} b_y e\big(\alpha(vd)^k y\big)\Big|^2. \tag{12.5}$$

In preparation for the application of the large sieve inequality, we next consider the spacing of the elements $\alpha(vd)^k$ in $\mathbb{T}$ for distinct elements v of $\mathscr{V}_j$. Suppose that $v_1, v_2 \in \mathscr{V}_j$ satisfy $v_1 \not\equiv v_2 \pmod{g}$. Then in view of our construction of the set $\mathscr{V}_j$, one necessarily has $(v_1 d)^k \not\equiv (v_2 d)^k \pmod{g}$, and hence our hypothesis that $(a, g) = 1$ ensures that

$$\operatorname{ord}\big\|a\big((v_1 d)^k - (v_2 d)^k\big)/g\big\| \geqq -\operatorname{ord} g.$$

Moreover, if we write $\beta = \alpha - a/g$, then we may suppose that $\langle g\beta\rangle < (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-k}$. Since $d \in \mathscr{C}_g(P - M)$ and $v \in \mathscr{B}(M - \operatorname{ord} d, \pi, R)$, one obtains

$$\begin{aligned}\operatorname{ord}\big\|\beta\big((v_1 d)^k - (v_2 d)^k\big)\big\| &< \big(-k(M+R) - \operatorname{ord} g\big) + k(M+R)\\ &\leqq \operatorname{ord}\big\|a\big((v_1 d)^k - (v_2 d)^k\big)/g\big\|.\end{aligned}$$

We therefore deduce that

$$\operatorname{ord}\big\|(\beta + a/g)\big((v_1 d)^k - (v_2 d)^k\big)\big\| = \operatorname{ord}\big\|a\big((v_1 d)^k - (v_2 d)^k\big)/g\big\|,$$

whence

$$\text{ord}\big\|\alpha\big((v_1d)^k-(v_2d)^k\big)\big\| \geqq -\text{ord}\, g. \tag{12.6}$$

We now divide into cases, according to the size of $\langle g\rangle$. Suppose first that $\langle g\rangle > \hat{\boldsymbol{M}}\hat{\boldsymbol{R}}/\langle d\rangle$. Since for $v \in \mathscr{B}(M-\text{ord}\, d,\pi,R)$, one has $\langle v\rangle \leqq \hat{\boldsymbol{M}}\hat{\boldsymbol{R}}/\langle d\rangle$, it follows that in this case the elements of $\mathscr{V}_j$ are necessarily distinct modulo g. It therefore follows from (12.6) that the points $\alpha(vd)^k$ are spaced at least $\langle g\rangle^{-1}$ apart in $\mathbb{T}$.

Suppose next that $\langle g\rangle \leqq \hat{\boldsymbol{M}}\hat{\boldsymbol{R}}/\langle d\rangle$. In this case we plainly have $\langle g\rangle \leqq \hat{\boldsymbol{M}}\hat{\boldsymbol{R}}$, and so the hypotheses of the lemma permit us to suppose that $\langle g\alpha-a\rangle \geqq \hat{\boldsymbol{M}}\hat{\boldsymbol{P}}^{-k}$. On one hand, if $v_1, v_2 \in \mathscr{V}_j$ satisfy the condition $v_1 \not\equiv v_2 \pmod g$, then it follows from (12.6) that the points $\alpha(v_1d)^k$ and $\alpha(v_2d)^k$ are spaced at least $\langle g\rangle^{-1}$ apart in $\mathbb{T}$. If $v_1 \equiv v_2 \pmod g$ on the other hand, then on recalling that $\langle g\alpha-a\rangle < (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-k}$, we find that

$$\begin{aligned}\text{ord}\big\|\alpha\big((v_1d)^k-(v_2d)^k\big)\big\| &= \text{ord}\|(\alpha-a/g)d^k(v_1^k-v_2^k)\| \\ &\geqq M-kP-\text{ord}\, g+\text{ord}\big(d^k(v_1^k-v_2^k)\big).\end{aligned} \tag{12.7}$$

In order to obtain a lower bound for the final term appearing on the right-hand side of (12.7), we begin by noting that

$$\text{ord}\big(d^k(v_1^k-v_2^k)\big) \geqq \text{ord}(v_1-v_2)+\text{ord}\big(d^{k-1}(v_1^{k-1}+v_1^{k-2}v_2+\cdots+v_2^{k-1})\big). \tag{12.8}$$

If $v_1 \neq v_2$ and $v_1 \equiv v_2 \pmod g$, we have

$$\text{ord}(v_1-v_2) \geqq \text{ord}\, g. \tag{12.9}$$

Further, if $\text{ord}\, v_1 = \text{ord}\, v_2$, then since the elements of $\mathscr{V}_j$ are monic, each term $v_1^{k-1-l}v_2^l$ has the same degree and leading coefficient 1. Consequently, as an element of $\mathbb{F}_q[t]$, the expression $v_1^{k-1}+v_1^{k-2}v_2+\cdots+v_2^{k-1}$ has degree $(k-1)\,\text{ord}\, v_1$ with leading coefficient k (which is, of course, not divisible by $\text{ch}(\mathbb{F}_q)$). Whether or not $\text{ord}\, v_1 = \text{ord}\, v_2$, therefore, we find that when $v_1, v_2 \in \mathscr{V}_j$, one has

$$\begin{aligned}\text{ord}\big(d^{k-1}(v_1^{k-1}+v_1^{k-2}v_2+\cdots+v_2^{k-1})\big) &= \max\{\text{ord}(v_1d)^{k-1}, \text{ord}(v_2d)^{k-1}\} \\ &> (k-1)M.\end{aligned} \tag{12.10}$$

On substituting (12.9) and (12.10) into (12.8), we see that

$$\text{ord}\big(d^k(v_1^k-v_2^k)\big) \geqq (k-1)M+\text{ord}\, g,$$

whence by (12.7) we have

$$\text{ord}\big\|\alpha\big((v_1d)^k-(v_2d)^k\big)\big\| \geqq -k(P-M).$$

In this case, therefore, the points $\alpha(v_1d)^k$ and $\alpha(v_2d)^k$ are spaced at least $(\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-k}$ apart in $\mathbb{T}$.

The previous discussion shows that for $v \in \mathscr{V}_j$, the points $\alpha(vd)^k$ are spaced at least $\min\{\langle g\rangle^{-1}, (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-k}\}$ apart in $\mathbb{T}$. We now apply the large sieve inequality for function fields, as given by Hsu [12], Theorem 2.4, to deduce that

$$\sum_{v\in\mathscr{V}_j}\Big|\sum_{\langle y\rangle\leqq(\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} b_y e\big(\alpha(vd)^k y\big)\Big|^2 \ll \big(\langle g\rangle + (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k\big) \sum_{\langle y\rangle\leqq(\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} |b_y|^2. \tag{12.11}$$

But on considering the underlying equation, and recalling that Δ_s is a permissible exponent, one has

$$\sum_{\langle y\rangle\leqq(\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k} |b_y|^2 \leqq S_s(P-M,R) \ll (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{2s-k+\Delta_s+\varepsilon}.$$

On substituting the latter estimate into (12.11), and thence into (12.5) and (12.1), we deduce that

$$f(\alpha;P,R) \ll \hat{\boldsymbol{P}}^{\varepsilon}\hat{\boldsymbol{M}} + (\hat{\boldsymbol{P}}\hat{\boldsymbol{R}})^{1+\varepsilon}\big((\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{\Delta_s}\hat{\boldsymbol{M}}^{-1}\big(1+\langle g\rangle(\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^{-k}\big)\big)^{1/(2s)}.$$

The conclusion of the lemma is now immediate on recalling our conventions concerning ε and R.

13. Estimates for smooth Weyl sums: a uniform bound

The principal conclusions of the previous two sections can be combined to provide an estimate for smooth Weyl sums of use no matter what range the modulus g may lie in. In this section we derive such a bound, and also optimise parameters so as to obtain conclusions asymptotically as strong as are attainable via our methods.

Theorem 13.1. *Suppose that λ is a real number with $1/2 < \lambda < 1$. Let $\alpha \in \mathbb{K}_\infty$, and suppose that whenever a and g are elements of $\mathbb{F}_q[t]$ with g monic, $(a,g)=1$ and $\langle g\alpha - a\rangle \leqq \hat{\boldsymbol{P}}^{\lambda-k}$, then one has $\langle g\rangle > \hat{\boldsymbol{P}}^{\lambda}\hat{\boldsymbol{R}}$. Then provided that $l,s,w \in \mathbb{N}$ satisfy $2s \geqq k+1$, and Δ_l, Δ_s, Δ_w are permissible exponents, one has*

$$f(\alpha;P,R) \ll \hat{\boldsymbol{P}}^{\varepsilon}(\hat{\boldsymbol{P}}^{\lambda} + \hat{\boldsymbol{P}}^{1-\mu} + \hat{\boldsymbol{P}}^{1-\nu}),$$

where

$$\mu = \frac{k(1-\lambda) - \lambda\Delta_w - (1-\lambda)\Delta_l}{2lw} \quad \text{and} \quad \nu = \frac{\lambda - (1-\lambda)\Delta_s}{2s}.$$

Proof. For the sake of concision, let us write $M = \lambda P$. By the function field analogue of Dirichlet's theorem on diophantine approximation (see [14], Lemma 3), given $\alpha \in \mathbb{T}$, there exist polynomials a and g in $\mathbb{F}_q[t]$ with g monic, $(a,g)=1$, $\langle g\rangle \leqq (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^k$ and $\langle g\alpha - a\rangle < (\hat{\boldsymbol{M}}\hat{\boldsymbol{R}})^{-k}$. For the latter pair of polynomials, we have, in particular, the upper bound $\langle g\alpha - a\rangle < \langle g\rangle^{-1}$. Consequently, we may apply Lemma 11.2 to deduce that when $\langle g\rangle > (\hat{\boldsymbol{P}}/\hat{\boldsymbol{M}})^k$, one has

$$\begin{aligned} f(\alpha;P,R) &\ll \hat{\boldsymbol{P}}^{1+\varepsilon}\big(\hat{\boldsymbol{P}}^{\lambda\Delta_w+(1-\lambda)\Delta_l}(\hat{\boldsymbol{P}}^{-k(1-\lambda)} + \hat{\boldsymbol{P}}^{-k\lambda})\big)^{1/(2lw)} + \hat{\boldsymbol{P}}^{\lambda} \\ &\ll \hat{\boldsymbol{P}}^{\varepsilon}(\hat{\boldsymbol{P}}^{\lambda} + \hat{\boldsymbol{P}}^{1-\mu}). \end{aligned} \tag{13.1}$$

Suppose, on the other hand, that $\langle g\rangle \leqq (\hat{P}/\hat{M})^k$. If $\langle g\alpha - a\rangle \geqq \hat{M}\hat{P}^{-k}$, then the hypotheses of the statement of Lemma 12.1 are satisfied. If $\langle g\alpha - a\rangle < \hat{M}\hat{P}^{-k}$, meanwhile, the hypotheses of the present lemma ensure that $\langle g\rangle > \hat{M}\hat{R}$, and so the hypotheses of the statement of Lemma 12.1 are again satisfied. We therefore conclude from Lemma 12.1 that when $\langle g\rangle \leqq (\hat{P}/\hat{M})^k$, then one has

$$f(\alpha; P, R) \ll \hat{P}^{\varepsilon}\big(\hat{P}^{\lambda} + \hat{P}(\hat{P}^{-\lambda+(1-\lambda)\Delta_s})^{1/(2s)}\big) \ll \hat{P}^{\varepsilon}(\hat{P}^{\lambda} + \hat{P}^{1-\nu}). \tag{13.2}$$

The proof of the lemma follows on combining (13.1) and (13.2).

As is more or less apparent from the conclusion of Theorem 13.1, the optimal choice of λ is that satisfying the condition $\mu = \nu$. A modest calculation therefore leads to the following corollary.

Corollary 13.2. *Suppose that $l, s, w \in \mathbb{N}$ satisfy $2s \geqq k+1$, and Δ_l, Δ_s, Δ_w are permissible exponents. Define λ and σ by means of the relations*

$$\sigma = \frac{k - \Delta_l - \Delta_s\Delta_w}{2\big(s(k + \Delta_w - \Delta_l) + lw(1 + \Delta_s)\big)}$$

and

$$\lambda = \frac{s(k - \Delta_l) + lw\Delta_s}{s(k + \Delta_w - \Delta_l) + lw(1 + \Delta_s)}.$$

Suppose in addition that $1/2 < \lambda < 1 - \sigma$. Then one has

$$\sup_{\alpha \in \mathfrak{m}(\lambda P)} |f(\alpha; P, R)| \leqq \sup_{\alpha \in \mathfrak{m}(P)} |f(\alpha; P, R)| \ll \hat{P}^{1-\sigma+\varepsilon}.$$

Proof. The desired conclusion follows directly from Theorem 13.1 provided that one is able to show that whenever α lies in $\mathfrak{m}(P)$, then α satisfies the hypotheses of the statement of Theorem 13.1. Consider then a point α in $\mathfrak{m}(P)$. Suppose that a and g are elements of $\mathbb{F}_q[t]$ with g monic, $(a, g) = 1$ and $\langle g\alpha - a\rangle \leqq \hat{P}^{\lambda-k}$. If one were to have $\langle g\rangle \leqq \hat{P}$, then necessarily $\alpha \in \mathfrak{M}(P)$, contradicting our earlier assumption that $\alpha \in \mathfrak{m}(P)$. We are therefore forced to conclude that $\langle g\rangle > \hat{P} > \hat{P}^{\lambda}$. Consequently, whenever α lies in $\mathfrak{m}(P)$, then α satisfies the hypotheses of the statement of Theorem 13.1. The proof of the corollary is completed on verifying that with the choice of λ made in the statement, one has $\mu = \nu = \sigma$ in the conclusion of Lemma 13.1.

On making use of Theorem 9.4 to supply permissible exponents within this corollary, we obtain a conclusion simple enough to use directly in subsequent applications.

Corollary 13.3. *Suppose that k and q are natural numbers with $\mathrm{ch}(\mathbb{F}_q) \nmid k$. Define $\gamma = \gamma_q(k)$ as in the preamble to the statement of Theorem* 1.1, *and in addition define $B = B_q(k)$ by putting*

$$B_q(k) = \begin{cases} 1, & \text{when } k \leqq 2^{\gamma-2}, \\ (1 - 2^{-\gamma})^{-1}, & \text{when } k > 2^{\gamma-2}. \end{cases}$$

Then there is a positive absolute constant C_4 with the property that, with the exponent $\sigma(k)$ defined by means of the relation

$$\sigma(k)^{-1} = Bk(\operatorname{Log} k + B \operatorname{Log}\operatorname{Log} k + C_4\sqrt{\operatorname{Log}\operatorname{Log} k}),$$

there exists a positive number τ satisfying $\tau < 1/2$ for which

$$\sup_{\alpha \in \mathfrak{m}((1-\tau)P)} |f(\alpha; P, R)| \leqq \sup_{\alpha \in \mathfrak{m}(P)} |f(\alpha; P, R)| \ll \hat{P}^{1-\sigma(k)+\varepsilon}.$$

Proof. We begin by considering the situation in which k is large. Put

$$s = \left\lceil \frac{1}{2} Bk(\log k + \log\log\log k + 1) \right\rceil, \tag{13.3}$$

$$w = \left\lceil \frac{1}{2} Bk(\log\log k + 1) \right\rceil, \quad \text{and} \quad l = \lceil Bk/\sqrt{\log\log k} \rceil. \tag{13.4}$$

Then from Theorem 9.4, we find that the exponents Δ_s^* and Δ_w^* are permissible, where

$$\Delta_s^* = ke^{1-2s/(Bk)} \leqq 1/\log\log k \quad \text{and} \quad \Delta_w^* = ke^{1-2w/(Bk)} \leqq k/\log k.$$

We also see from Theorem 9.4 that the exponent Δ_l^* is permissible, where Δ_l^* satisfies the equation

$$(\Delta_l^*/k) + \log(\Delta_l^*/k) = 1 - 2l/(Bk).$$

But $\delta + \log\delta$ is an increasing function of δ, and so it follows that

$$\Delta_l^*/k < 1 - l/(Bk) + l^2/(B^2k^2).$$

We therefore deduce that the exponents

$$\Delta_s = 1/\log\log k, \quad \Delta_w = k/\log k \quad \text{and} \quad \Delta_l = k - l/B + l^2/(B^2k) \tag{13.5}$$

are permissible.

We next recall the conclusion of Corollary 13.2. Define the exponents $\lambda(k)$ and $\sigma(k)$ by

$$\lambda(k) = 1 - \frac{s\Delta_w + lw}{s(k + \Delta_w - \Delta_l) + lw(1 + \Delta_s)} \tag{13.6}$$

and

$$\sigma(k)^{-1} = 2s + \frac{2(s\Delta_w + lw)(1 + \Delta_s)}{k - \Delta_l - \Delta_s\Delta_w}. \tag{13.7}$$

Then whenever $1/2 < \lambda(k) < 1 - \sigma(k)$, and in addition α satisfies the hypotheses of Theorem 13.1, one has $f(\alpha; P, R) \ll \hat{P}^{1-\sigma(k)+\varepsilon}$. But for sufficiently large values of k, it follows

from (13.3), (13.4) and (13.5) that the permissible exponents in the previous paragraph yield the formulae

$$2(s\Delta_w + lw) = Blk\log\log k\big(1 + O(1/\sqrt{\log\log k})\big), \tag{13.8}$$

$$k - \Delta_l - \Delta_s\Delta_w = \frac{l}{B}\big(1 + O(1/\sqrt{\log\log k})\big) \tag{13.9}$$

and

$$s(k - \Delta_l) + lw(1 + \Delta_s) + s\Delta_w = \frac{sl}{B}\big(1 + O(1/\sqrt{\log\log k})\big). \tag{13.10}$$

On substituting (13.8) and (13.9) together with (13.3) and (13.5) into (13.7), we find that the exponent $\sigma(k)$ satisfies the upper bound

$$\sigma(k)^{-1} \leqq Bk\log k + B^2k\log\log k\big(1 + O(1/\sqrt{\log\log k})\big).$$

Thus, when k is sufficiently large, there is a positive absolute constant C_4 for which

$$\sigma(k)^{-1} \leqq Bk(\log k + B\log\log k + C_4\sqrt{\log\log k}). \tag{13.11}$$

Likewise, now making use also of (13.10), we deduce from (13.6) that

$$1 - \lambda(k) = B\frac{\log\log k}{\log k}\big(1 + O(1/\sqrt{\log\log k})\big).$$

When k is sufficiently large, therefore, it follows from (13.11) that $1/2 < \lambda(k) < 1 - \sigma(k)$. We may thus conclude that whenever k is sufficiently large, one has

$$\sup_{\alpha\in\mathfrak{m}(\lambda P)} |f(\alpha; P, R)| \leqq \sup_{\alpha\in\mathfrak{m}(P)} |f(\alpha; P, R)| \ll \hat{P}^{1-\sigma(k)+\varepsilon}, \tag{13.12}$$

where $\sigma(k)$ satisfies the upper bound (13.11).

The argument up to this point is applicable for sufficiently large values of k, say for $k > k_0$. We now seek to establish an estimate of the shape

$$\sup_{\alpha\in\mathfrak{m}(P)} |f(\alpha; P, R)| \ll \hat{P}^{1-\delta}, \tag{13.13}$$

for some positive number δ, for each exponent k with $k \leqq k_0$. By suitably increasing the size of the absolute constant C_4 in (13.11), it follows from (13.12) that the estimate (13.13) holds for all exponents k, and thus the conclusion of the corollary follows at once.

For simplicity, we now take D to be a sufficiently large, though fixed, positive number, and we set

$$s = \lceil 9BDk\log k + 1\rceil, \quad w = \lceil BDk\log k + 1\rceil \quad \text{and} \quad l = 2.$$

It follows from Theorem 9.4 that the exponents Δ_s^* and Δ_w^* are permissible, where

$$\Delta_s^* = ke^{1-2s/(Bk)} \leqq k^{-17D} \quad \text{and} \quad \Delta_w^* = ke^{1-2w/(Bk)} \leqq k^{-D}.$$

Thus, on recalling the conclusion of Lemma 9.1, we find that the exponents $\Delta_s = k^{-17D}$, $\Delta_w = k^{-D}$ and $\Delta_l = k-2$ are permissible. On substituting these exponents into (13.6) and (13.7), and noting that D has been chosen sufficiently large, we obtain

$$0 < 1 - \lambda(k) \leqq \frac{2BDk\log k + 5}{20BDk\log k} < \frac{1}{9}$$

and

$$\sigma(k)^{-1} \leqq 2s + lw + 1 < 21BDk\log k. \tag{13.14}$$

On noting that the exponent $\lambda(k)$ satisfies the condition $1/2 < \lambda(k) < 1 - \sigma(k)$, we may apply Corollary 13.2 to establish that (13.12) holds in the present situation, though now with the upper bound (13.14) in place of (13.11). This conclusion confirms the desired estimate (13.13), and the conclusion of the corollary now follows.

14. An upper bound for $G_q(k)$: the proof of Theorem 1.1

The conclusions of §13 enable us to establish minor arc estimates of the shape (6.1), and from there we are able to bound $G_q(k)$ by means of Lemma 6.4.

Lemma 14.1. *Let $\lambda(k)$ and $\sigma(k)$ be defined as in the statement of Corollary* 13.2, *and suppose that $1/2 < \lambda(k) < 1 - \sigma(k)$. Suppose also that v is a natural number with $v \geqq k-1$, and that Δ_{v+1} is a permissible exponent. Then whenever u is a natural number with $u > 2v + \Delta_{v+1}/\sigma(k)$, there exists a positive number δ for which*

$$\int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^u|\, d\alpha \ll \hat{P}^{u+2-k-\delta}.$$

Proof. We begin by recalling that $\mathfrak{p} = \mathfrak{m}(P)$, so that the hypotheses of the lemma lead from Corollary 13.2 to the upper bound

$$\sup_{\alpha\in\mathfrak{p}} |f(\alpha; P, R)| \ll \hat{P}^{1-\sigma(k)+\varepsilon}. \tag{14.1}$$

Let $w = [\Delta_{v+1}/\sigma(k)] + 1$. Then on combining (14.1) with the conclusion of Lemma 9.3, we deduce that

$$\begin{aligned}\int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^{2v+w}|\, d\alpha &\leqq \Big(\sup_{\alpha\in\mathfrak{p}} |f(\alpha)|\Big)^w \int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha \\ &\ll (\hat{P}^{1-\sigma(k)+\varepsilon})^w \hat{P}^{2v+2-k+\Delta_{v+1}+\varepsilon}.\end{aligned}$$

Since $w\sigma(k) > \Delta_{v+1}$, it follows that there is a positive number δ for which

$$\int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^{2v+w}|\, d\alpha \ll \hat{P}^{2v+w+2-k-\delta}.$$

The conclusion of the lemma now follows by making use of the trivial estimate $|f(\alpha)| \ll \hat{P}$.

Observe that Lemma 14.1 establishes that whenever $u > 2v + \Delta_{v+1}/\sigma(k)$, and $u > 2k - 2$, then u is accessible to the exponent k. It therefore follows from Lemma 6.4 that when s is an even integer with $s \geqq u + 2$, and $m \in \mathbb{J}_q^k[t]$, then $\mathscr{R}_s(m; \mathfrak{P}) \gg \hat{\boldsymbol{P}}^{s-k}$. But under the same hypotheses, one finds from (6.1) that there is a positive number δ with the property that

$$\int_{\mathfrak{p}} F(\alpha)^2 f(\alpha)^{s-2} e(-\alpha m)\, d\alpha \ll \hat{\boldsymbol{P}}^{s-u-2} \int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^u|\, d\alpha \ll \hat{\boldsymbol{P}}^{s-k-\delta}.$$

Consequently,

$$\mathscr{R}_s(m; \mathbb{T}) = \mathscr{R}_s(m; \mathfrak{P}) + \mathscr{R}_s(m; \mathfrak{p}) \gg \hat{\boldsymbol{P}}^{s-k} + O(\hat{\boldsymbol{P}}^{s-k-\delta}) \gg \hat{\boldsymbol{P}}^{s-k}.$$

We summarise this conclusion in the form of a theorem.

Theorem 14.2. *Let $\lambda(k)$ and $\sigma(k)$ be defined as in the statement of Corollary* 13.2, *and suppose that $1/2 < \lambda(k) < 1 - \sigma(k)$. Suppose also that v is a natural number with $v \geqq k - 1$ and that Δ_{v+1} is a permissible exponent. Then whenever s is an even integer with $s > 2v + 2 + \Delta_{v+1}/\sigma(k)$, and $m \in \mathbb{J}_q^k[t]$, one has $R(m) \gg \langle m \rangle^{s/k-1}$. In particular, when Δ_v $(v \geqq k - 1)$ are permissible exponents, one has $G_q(k) \leqq \mathfrak{G}_q(k)$, where we write*

$$\mathfrak{G}_q(k) = \min_{v \geqq k-1} \big(2v + 4 + 2\big[\Delta_{v+1}/\big(2\sigma(k)\big)\big]\big).$$

Corollary 14.3. *There is an absolute constant C_5 with the property that*

$$G_q(k) \leqq Bk\left(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k} + C_5\frac{\sqrt{\operatorname{Log}\operatorname{Log} k}}{\operatorname{Log} k}\right).$$

Proof. We apply the conclusions of Corollary 13.3 and Theorems 9.4 and 14.2 to deduce that

$$G_q(k) \leqq \min_{v \geqq k-1}\left(2v + 4 + 2\left[\frac{1}{2}Bk^2 e^{1-(2v+2)/(Bk)}\mathscr{L}(k)\operatorname{Log} k\right]\right), \tag{14.2}$$

where we write

$$\mathscr{L}(k) = 1 + B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k} + C_4\frac{\sqrt{\operatorname{Log}\operatorname{Log} k}}{\operatorname{Log} k},$$

and with C_4 chosen to be a suitably large positive absolute constant. On taking

$$v = \left\lceil \frac{1}{2}Bk\left(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 1 + B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k}\right)\right\rceil,$$

we find that

$$\begin{aligned} ke^{1-(2v+2)/(Bk)} &\leqq \frac{1}{\operatorname{Log} k}\exp\left(-B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k}\right) \\ &= \frac{1}{\operatorname{Log} k}\left(1 - B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k} + O\left(\frac{(\operatorname{Log}\operatorname{Log} k)^2}{(\operatorname{Log} k)^2}\right)\right). \end{aligned}$$

The upper bound for $G_q(k)$ provided by (14.2) therefore becomes

$$G_q(k) \leqq Bk(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 1 + B\operatorname{Log}\operatorname{Log} k/\operatorname{Log} k) + Bk\big(1 + O(\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k)\big).$$

The conclusion of the corollary follows on taking C_5 to be a sufficiently large positive absolute constant.

On comparing the definition of $B_q(k)$ with that of $A_q(k)$ given in (1.2), we see that when $k \geqq 4$, one has $B_q(k) = A_q(k)$ for $k > 2^{\gamma-2}$, and $B_q(k) \leqq A_q(k)$ for $k \leqq 2^{\gamma-2}$. The first conclusion of Theorem 1.1 consequently follows at once from that of Corollary 14.3. When $p = \operatorname{ch}(\mathbb{F}_q)$ divides k, on the other hand, the relation $G_q(k) = G_q\big(k/\operatorname{ch}(\mathbb{F}_q)\big)$ follows on noting that every sum of kth powers in $\mathbb{F}_q[t]$ belongs to $\mathbb{F}_q[t^p]$, and that when $m \in \mathbb{J}_q^k[t]$, the representation problem (1.1) may therefore be reduced to the simpler one

$$m_1 = x_1^{k/p} + x_2^{k/p} + \cdots + x_s^{k/p},$$

where $m_1(t^p) = m(t)$. This completes our proof of Theorem 1.1.

We finish this section by remarking that it should be possible to adapt the methods of [24] and [25] to the function field setting, at least when $\operatorname{ch}(\mathbb{F}_q) > k$. With sufficient effort, therefore, it should be feasible to establish under the latter condition that $G_q(5) \leqq 17$, $G_q(6) \leqq 24$, $G_q(7) \leqq 33$, $G_q(8) \leqq 42$, and so on.

15. An upper bound for $G_q^+(k)$: the proof of Theorem 1.2

A modification of the classical argument familiar from $\mathbb{Z}$ yields a straightforward proof of the upper bound for $G_q^+(k)$ recorded in Theorem 1.2. We therefore economise on details.

Lemma 15.1. *Suppose that k and q are natural numbers with $\operatorname{ch}(\mathbb{F}_q) \nmid k$. Let $\lambda(k)$ and $\sigma(k)$ be defined as in the statement of Corollary* 13.2, *and suppose that $1/2 < \lambda(k) < 1 - \sigma(k)$. Suppose also that v is a natural number with $v \geqq k - 1$, and that Δ_{v+1} is a permissible exponent. Then one has $G_q^+(k) \leqq \mathfrak{G}_q^+(k)$, where we write*

$$\mathfrak{G}_q^+(k) = \max\big\{2k + 1, v + 3 + \big[\Delta_{v+1}/\big(2\sigma(k)\big)\big]\big\}.$$

Proof. Let M be a large natural number, and suppose that v is a natural number satisfying the hypotheses of the lemma. We put $s = \mathfrak{G}_q^+(k)$, and let $\mathscr{Z}^*(M) = \mathscr{Z}_{s,k}^*(M)$ denote the set of non-exceptional polynomials m in $\mathbb{J}_q^k[t]$, with $\operatorname{ord} m = M$, that fail to admit a strict representation as a sum of s kth powers. The set of exceptional polynomials may be handled in like manner with trivial modifications to the argument, so we suppress additional discussion of this set. Next, defining $P = \lceil M/k \rceil$ as in the preamble to the statement of Theorem 1.1, we define $\mathscr{Z}(M) = \mathscr{Z}_{s,k}(M)$ to be the set of non-exceptional polynomials m in $\mathbb{J}_q^k[t]$, with $\operatorname{ord} m = M$, for which the equation (2.4) fails to possess a solution with $\langle x_i \rangle \leqq \hat{\boldsymbol{P}}$ $(i = 1, 2)$ and $y_j \in \mathscr{A}(P, R)$ $(1 \leqq j \leqq s - 2)$. For the sake of concision, we write $Z^*(M) = \operatorname{card}\big(\mathscr{Z}^*(M)\big)$ and $Z(M) = \operatorname{card}\big(\mathscr{Z}(M)\big)$. Note that $Z^*(M) \leqq Z(M)$, and

hence, in order to establish the conclusion of the lemma it suffices to show that $Z(M) = o(\hat{M})$ as $M \to \infty$.

Next we define the exponential sum

$$K(\alpha) = \sum_{m \in \mathscr{Z}(M)} e(-m\alpha).$$

Then as a consequence of Lemma 5.4, one has

$$\int_{\mathfrak{R}} F(\alpha)^2 f(\alpha)^{s-2} K(\alpha)\, d\alpha = \sum_{m \in \mathscr{Z}(M)} \mathscr{R}_s(m; \mathfrak{R}) \gg Z(M)\hat{P}^{s-k}.$$

But if $m \in \mathscr{Z}(M)$, then $\mathscr{R}_s(m; \mathbb{T}) = 0$, whence

$$\int_{\mathfrak{R}} F(\alpha)^2 f(\alpha)^{s-2} e(-m\alpha)\, d\alpha + \int_{\mathfrak{n}} F(\alpha)^2 f(\alpha)^{s-2} e(-m\alpha)\, d\alpha = 0.$$

Thus we see that

$$\left| \int_{\mathfrak{n}} F(\alpha)^2 f(\alpha)^{s-2} K(\alpha)\, d\alpha \right| = \int_{\mathfrak{R}} F(\alpha)^2 f(\alpha)^{s-2} K(\alpha)\, d\alpha \gg Z(M)\hat{P}^{s-k}.$$

An application of Schwarz's inequality now yields

$$Z(M)\hat{P}^{s-k} \ll \left(\int_{\mathbb{T}} |K(\alpha)|^2\, d\alpha \right)^{1/2} \left(\int_{\mathfrak{n}} |F(\alpha)^4 f(\alpha)^{2s-4}|\, d\alpha \right)^{1/2}. \tag{15.1}$$

In order to estimate the second integral on the right-hand side of (15.1), we begin by noting that Lemma 14.1 implies that whenever

$$2s - 4 > 2v + \Delta_{v+1}/\sigma(k), \tag{15.2}$$

then there is a positive number δ for which

$$\int_{\mathfrak{p}} |F(\alpha)^2 f(\alpha)^{2s-4}|\, d\alpha \ll \hat{P}^{2s-2-k-\delta}. \tag{15.3}$$

Under the same conditions, we therefore find that $2s - 4$ is accessible to the exponent k, whence Lemma 6.3 yields

$$\int_{\mathfrak{P}\setminus\mathfrak{N}} |F(\alpha)^2 f(\alpha)^{2s-4}|\, d\alpha \ll \hat{P}^{2s-2-k}\hat{V}^{-1/(ks)}. \tag{15.4}$$

Since $\mathfrak{n} = \mathfrak{p} \cup (\mathfrak{P}\setminus\mathfrak{N})$, the trivial estimate $F(\alpha) \ll \hat{P}$ leads from (15.3) and (15.4) to the upper bound

$$\int_{\mathfrak{n}} |F(\alpha)^4 f(\alpha)^{2s-4}|\, d\alpha \ll \hat{P}^2 \int_{\mathfrak{n}} |F(\alpha)^2 f(\alpha)^{2s-4}|\, d\alpha \ll \hat{P}^{2s-k}\hat{V}^{-1/(ks)}.$$

Finally, by orthogonality, the first integral on the right-hand side of (15.1) is equal to $Z(M)$. We therefore conclude from (15.1) that

$$Z(M)\hat{P}^{s-k} \ll Z(M)^{1/2}(\hat{P}^{2s-k}\hat{V}^{-1/(ks)})^{1/2},$$

whence

$$Z(M) \ll \hat{P}^k \hat{V}^{-1/(ks)} \ll \hat{M}(\log \hat{M})^{-1/(12ks)}.$$

We have shown in this way that $Z(M) = o(\hat{M})$ as $M \to \infty$, and from this, in view of our earlier comments concerning exceptional polynomials, it follows that $G_q^+(k) \leqq s$. The proof of the lemma is completed by reference to (15.2).

We note that one variable may be saved in the argument above with only modest additional effort. In our discussion we made use of two variables not restricted to be smooth in (2.4), where only one is required in our minor arc treatment. This expedience allowed us easy reference to Lemmata 5.4 and 6.3. However, by a straightforward modification of the arguments of §§5 and 6, the two classical Weyl sums may be replaced by one classical Weyl sum together with a smooth Weyl sum, and thereby a variable is saved.

A comparison of Lemma 15.1 with the conclusion of Theorem 14.2 reveals that the upper bounds $\mathfrak{G}_q^+(k)$ and $\mathfrak{G}_q(k)$ established by these lemmata for $G_q^+(k)$ and $G_q(k)$, respectively, are essentially related by the equation $\mathfrak{G}_q^+(k) = \frac{1}{2}\mathfrak{G}_q(k) + 1$. The argument of the proof of Corollary 14.3 therefore yields the following upper bound for $G_q^+(k)$.

Corollary 15.2. *There is an absolute constant C_6 with the property that*

$$G_q^+(k) \leqq \frac{1}{2}Bk\left(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + B\frac{\operatorname{Log}\operatorname{Log} k}{\operatorname{Log} k} + C_6\frac{\sqrt{\operatorname{Log}\operatorname{Log} k}}{\operatorname{Log} k}\right).$$

In view of the discussion completing §14, the conclusion of Theorem 1.2 now follows at once without additional complications.

16. The solubility of diagonal equations: the proof of Theorem 1.3

The application of the Hardy-Littlewood method to equations of the shape (1.4) over $\mathbb{F}_q[t]$ is essentially routine, and so we confine ourselves to an abbreviated discussion of the proof of Theorem 1.3. We consider an equation of the shape (1.4) satisfying the hypotheses of the statement of Theorem 1.3. Let P be a natural number sufficiently large in terms of s, k, q and $\boldsymbol{a}$. We seek to establish a lower bound for the number $N_s(P;\boldsymbol{a})$ of solutions $\boldsymbol{x} \in \mathbb{F}_q[t]^s$ with $\langle x_i \rangle \leqq \hat{P}$ $(1 \leqq i \leqq s)$ by means of the Hardy-Littlewood method. Recalling the notation introduced in (2.3), we now define $F_i = F_i(\alpha; P)$ and $f_i = f_i(\alpha; P, R)$ by

$$F_i(\alpha; P) = F(a_i\alpha; P) \quad \text{and} \quad f_i(\alpha; P, R) = f(a_i\alpha; P, R).$$

Then it follows from (2.1) that a lower bound for $N_s(P;\boldsymbol{a})$ is provided by the quantity $N_s^*(P, R;\boldsymbol{a})$, defined by

$$N_s^*(P, R;\boldsymbol{a}) = \int_{\mathbb{T}} F_1F_2f_3 \dots f_s \, d\alpha. \tag{16.1}$$

Next define $\sigma(k)$ as in the statement of Corollary 13.3, and let τ be the associated positive number satisfying $\tau < 1/2$. Suppose that $c \in \mathbb{F}_q[t]$, and that P is sufficiently

large in terms of $\operatorname{ord} c$. Then it is a straightforward exercise to verify that whenever $c\alpha \in \mathfrak{M}\big((1-\tau)P\big)$, then $\alpha \in \mathfrak{M}\big((1-\tau)P + \operatorname{ord} c\big) \subseteqq \mathfrak{M}(P)$. Consequently, whenever $\alpha \in \mathfrak{m}(P)$, then $c\alpha \in \mathfrak{m}\big((1-\tau)P\big)$. We therefore deduce that when P is sufficiently large in terms of the degrees of the coefficients $a_1, \dots, a_s$, then

$$\sup_{\alpha \in \mathfrak{p}} |f_i(\alpha)| = \sup_{\alpha \in \mathfrak{m}(P)} |f(a_i\alpha; P, R)| \leqq \sup_{\beta \in \mathfrak{m}((1-\tau)P)} |f(\beta; P, R)| \ll \hat{P}^{1-\sigma(k)+\varepsilon}.$$

A modification of the argument of the proof of Lemma 14.1 now shows that whenever v is a natural number with $v \geqq k-1$, and Δ_{v+1} is a permissible exponent, and provided that u is a natural number with $u > 2v + \Delta_{v+1}/\sigma(k)$, then there is a positive number δ with the property that

$$\int_{\mathfrak{p}} |F_i(\alpha)^2 f_j(\alpha)^u| \, d\alpha \ll \hat{P}^{u+2-k-\delta} \quad (1 \leqq i, j \leqq s). \tag{16.2}$$

In order to justify this assertion, one must note in particular that the efficient differencing arguments underlying §§7, 8 and 9 may be modified so as to incorporate non-zero coefficients in the underlying variables. Thus, when b and c are fixed non-zero polynomials, one finds that whenever Δ_{s+1} is a permissible exponent, then

$$\int_{\mathbb{T}} |F(b\alpha; P)^2 f(c\alpha; P, R)^{2s}| \, d\alpha \ll \hat{P}^{\lambda_{s+1}+\varepsilon},$$

where $\lambda_{s+1} = 2s + 2 - k + \Delta_{s+1}$.

Next, by a straightforward modification of the argument of the proof of Lemma 6.3, we deduce from (16.2) that when Δ_u $(u = 1, 2, \dots)$ are permissible exponents, and

$$s \geqq \min_{v \geqq k-1} \big\{2v + 4 + 2\big[\Delta_{v+1}/\big(2\sigma(k)\big)\big]\big\}, \tag{16.3}$$

then

$$\int_{\mathfrak{P}\setminus\mathfrak{N}} |F_i(\alpha)^2 f_j(\alpha)^{s-2}| \, d\alpha \ll \hat{P}^{s-k} \hat{V}^{-2/(ks)} \quad (1 \leqq i, j \leqq s).$$

On recalling that $\mathfrak{n} = \mathfrak{p} \cup (\mathfrak{P}\setminus\mathfrak{N})$, therefore, an application of Hölder's inequality in combination with (16.2) and the last estimate reveals that

$$\int_{\mathfrak{n}} |F_1 F_2 f_3 \dots f_s| \, d\alpha \ll \hat{P}^{s-k} \hat{V}^{-2/(ks)}. \tag{16.4}$$

Turning next to the analysis of the major arcs $\mathfrak{N}$, we may follow the arguments underlying the discussion of §5. Thus we find that

$$\int_{\mathfrak{N}} F_1 F_2 f_3 \dots f_s \, d\alpha - \rho(P/R)^{s-2} \mathfrak{S}_{s,k} J_{s,k} \ll \hat{P}^{s-k} \hat{V}^{-1/k}, \tag{16.5}$$

where

$$J_{s,k} = \int_{\langle\beta\rangle < (q\hat{P})^{1-k}} F(a_1\beta; P) \dots F(a_s\beta; P) \, d\beta, \tag{16.6}$$

and

$$\mathfrak{S}_{s,k} = \sum_{g \in \mathbb{F}_q[t]}^{\dagger} \mathfrak{A}_s(g),$$

with

$$\mathfrak{A}_s(g) = \langle g\rangle^{-s} \sum_{\substack{\langle b\rangle < \langle g\rangle \\ (b,g)=1}} S(g,a_1b)\dots S(g,a_sb).$$

Here, the exponential sums $S(g,a_ib)$ are defined via (4.1) for $1 \leqq i \leqq s$.

Defining next

$$\Omega_{\varpi,s} = 1 + \sum_{h=1}^{\infty} \mathfrak{A}_s(\varpi^h),$$

an argument paralleling that of the proof of Lemma 5.2 shows that $\prod_{\varpi} \Omega_{\varpi,s}$ converges absolutely to $\mathfrak{S}_{s,k}$. In addition, if we write $M_s(g)$ for the number of solutions of the congruence $a_1x_1^k + \dots + a_sx_s^k \equiv 0 \pmod g$, with $\langle x_i\rangle < \langle g\rangle$ $(1 \leqq i \leqq s)$, then

$$\Omega_{\varpi,s} = \lim_{h\to\infty} \langle \varpi\rangle^{h(1-s)} M_s(\varpi^h),$$

and

$$|\Omega_{\varpi,s} - 1| \ll \langle \varpi\rangle^{-1-1/k}.$$

But by the hypotheses of Theorem 1.3, the equation (1.4) possesses a non-trivial solution $\boldsymbol{x} = \boldsymbol{a}$ in $\mathbb{K}_{\varpi}$. Since $\mathrm{ch}(\mathbb{F}_q) \nmid k$, therefore, we may apply Hensel's Lemma to show that $M_s(\varpi^h) \gg \langle \varpi\rangle^{h(s-1)}$, whence $\Omega_{\varpi,s} > 0$ for each irreducible polynomial ϖ. We thus conclude that for some positive number $A = A(q,s,k;\boldsymbol{a})$, one has

$$\mathfrak{S}_{s,k} \gg \prod_{\varpi} (1 + A\langle \varpi\rangle^{-1-1/k})^{-1} \gg 1.$$

Moreover, by an argument paralleling that employed in the proof of Lemma 5.1, one has $\mathfrak{S}_{s,k} \ll 1$. Consequently, the hypotheses of Theorem 1.3 ensure that

$$1 \ll \mathfrak{S}_{s,k} \ll 1. \tag{16.7}$$

It remains only to estimate the singular integral $J_{s,k}$. Here we observe that the argument of the proof of [14], Lemma 15 leads from (16.6) to the relation

$$J_{s,k} = (q\hat{P})^{1-k} \mathscr{M}_{s,k}(P;\boldsymbol{a}), \tag{16.8}$$

where $\mathscr{M}_{s,k}(P;\boldsymbol{a})$ denotes the number of solutions of the inequality

$$\langle a_1x_1^k + \dots + a_sx_s^k\rangle < (q\hat{P})^{k-1},$$

with $\langle x_i\rangle \leqq \hat{P}$ $(1 \leqq i \leqq s)$. The existence of a solution $\boldsymbol{x} \in \mathbb{K}_{\infty}^s$ of the equation (1.4) ensures that $\mathscr{M}_{s,k}(P;\boldsymbol{a}) \geqq 1$ when P is sufficiently large. A variant of the argument of the proof of [14], Lemma 16 therefore shows that $\mathscr{M}_{s,k}(P;\boldsymbol{a}) \gg \hat{P}^{s-k}(q\hat{P})^{k-1}$, and thus we deduce from (16.8) that $J_{s,k} \gg \hat{P}^{s-k}$. The argument of the proof of Lemma 5.1 leading to (5.8), moreover, establishes that $J_{s,k} \ll \hat{P}^{s-k}$. The hypotheses of Theorem 1.3 therefore guarantee that

$$\hat{P}^{s-k} \ll J_{s,k} \ll \hat{P}^{s-k}. \tag{16.9}$$

On substituting (16.7) and (16.9) into (16.5), we are able to conclude that, under the hypotheses of the statement of Theorem 1.3, one has

$$\int_{\mathfrak{R}} F_1F_2f_3\dots f_s\,d\alpha \gg \hat{\boldsymbol{P}}^{s-k}.$$

In view of (16.1) and (16.4), therefore, provided that the lower bound (16.3) is satisfied, we arrive at the lower bound

$$\begin{aligned} N_s^*(P,R;\boldsymbol{a}) &= \int_{\mathfrak{R}} F_1F_2f_3\dots f_s\,d\alpha + \int_{\mathfrak{n}} F_1F_2f_3\dots f_s\,d\alpha \\ &\gg \hat{\boldsymbol{P}}^{s-k} + O(\hat{\boldsymbol{P}}^{s-k}\hat{\boldsymbol{V}}^{-2/(ks)}). \end{aligned}$$

The conclusion of Theorem 1.3 now follows on verifying that the argument of the proof of Corollary 14.3 leads from (16.3) to the upper bound

$$\min_{v\geqq k-1}\{2v+4+2[\Delta_{v+1}/(2\sigma(k))]\} \leqq \hat{\boldsymbol{G}}_q(k) + C_7k\sqrt{\operatorname{Log}\operatorname{Log}k}/\operatorname{Log}k,$$

for a suitable positive absolute constant C_7. This completes our discussion of the proof of Theorem 1.3.

References

[1] *M. Car*, Arithmétique additive dans l'anneau des polynômes á une indéterminée sur un corps fini, Thèse, Université de Provence, 1972.

[2] *M. Car*, Le problème de Waring pour l'anneau des polynômes sur un corps fini, Séminaire de Théorie des Nombres, 1972–1973 (Univ. Bordeaux I, Talence), Exp. No. 6, Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence (1973), 13pp.

[3] *M. Car*, Théorèmes de densité dans $\mathbb{F}_q[X]$, Acta Arith. **48** (1987), 145–165.

[4] *M. Car*, Waring's problem in function fields, Proc. London Math. Soc. (3) **68** (1994), 1–30.

[5] *M. Car* and *J. Cherly*, Sommes de cubes dans l'anneau $\mathbb{F}_{2^h}[X]$, Acta Arith. **65** (1993), 227–241.

[6] *M. Car* and *L. Gallardo*, Sums of cubes of polynomials, Acta Arith. **112** (2004), 41–50.

[7] *J. Cherly*, Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring, Journées Arithmétiques (Luminy 1989), Astérisque **198–200** (1991), 83–96.

[8] *G. W. Effinger* and *D. R. Hayes*, Additive number theory of polynomials over a finite field, Oxford University Press, Oxford 1991.

[9] *L. Gallardo*, On the restricted Waring problem over $\mathbb{F}_{2^n}[t]$, Acta Arith. **92** (2000), 109–113.

[10] *M. J. Greenberg*, Lectures on forms in many variables, W. A. Benjamin, New York 1969.

[11] *G. H. Hardy* and *E. M. Wright*, An introduction to the theory of numbers (5th edition), Oxford University Press, Oxford 1979.

[12] *C.-N. Hsu*, A large sieve inequality for rational function fields, J. Number Th. **58** (1996), 267–287.

[13] *R. M. Kubota*, Waring's problem for $\mathbb{F}_q[x]$, Ph.D. Thesis, University of Michigan, Ann Arbor 1971.

[14] *R. M. Kubota*, Waring's problem for $\mathbb{F}_q[x]$, Dissert. Math. (Rozprawy Mat.) **117** (1974), 60pp.

[15] *S. Lang*, On quasi-algebraic closure, Ann. Math. (2) **55** (1952), 373–390.

[16] *K. R. Matthews*, Waring's theorem for polynomials over a field, M.Sc. Thesis, University of Queensland, 1967.

[17] *R. E. A. C. Paley*, Theorems on polynomials in a Galois field, Quart. J. Math. **4** (1933), 52–63.

[18] *D. Panario*, *X. Gourdon* and *P. Flajolet*, An analytic approach to smooth polynomials over finite fields, Algorithmic Number Theory (Portland, OR, 1998), Lect. Notes Comput. Sci. **1423**, Springer, Berlin (1998), 226–236.

[19] *M. Rosen*, Number theory in function fields, Grad. Texts Math. **210**, Springer-Verlag, New York 2002.

[20] *K. Soundararajan*, Smooth polynomials: analysis and asymptotics, unpublished manuscript, 1993.

[21] *L. N. Vaserstein*, Waring's problem for algebras over fields, J. Number Th. **26** (1987), 286–298.
[22] *R. C. Vaughan*, A new iterative method in Waring's problem, Acta Math. **162** (1989), 1–71.
[23] *R. C. Vaughan*, The Hardy-Littlewood Method, second edition, Cambridge University Press, 1997.
[24] *R. C. Vaughan* and *T. D. Wooley*, Further improvements in Waring's problem, Acta Math. **174** (1995), 147–240.
[25] *R. C. Vaughan* and *T. D. Wooley*, Further improvements in Waring's problem, IV: higher powers, Acta Arith. **94** (2000), 203–285.
[26] *W. A. Webb*, Waring's problem in $GF[q, x]$, Acta Arith. **22** (1973), 207–220.
[27] *T. D. Wooley*, Large improvements in Waring's problem, Ann. Math. (2) **135** (1992), 131–164.
[28] *T. D. Wooley*, The application of a new mean value theorem to the fractional parts of polynomials, Acta Arith. **65** (1993), 163–179.
[29] *T. D. Wooley*, New estimates for smooth Weyl sums, J. London Math. Soc. (2) **51** (1995), 1–13.

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada N2L 3G1
e-mail: yrliu@math.uwaterloo.ca

School of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom
e-mail: matdw@bristol.ac.uk

Eingegangen 2. Januar 2007, in revidierter Fassung 29. Mai 2007