COMPOSITIO MATHEMATICA

Sub-Weyl subconvexity for Dirichlet L-functions to prime power moduli

Djordje Milićević

Compositio Math. **152** (2016), 825–875.

doi:10.1112/S0010437X15007381

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Compositio Math. 152 (2016) 825–875
doi:10.1112/S0010437X15007381

Sub-Weyl subconvexity for Dirichlet L-functions to prime power moduli

Djordje Milićević

Abstract

We prove a subconvexity bound for the central value $L(\frac{1}{2},\chi)$ of a Dirichlet L-function of a character χ to a prime power modulus $q=p^n$ of the form $L(\frac{1}{2},\chi)\ll p^r q^{\theta+\epsilon}$ with a fixed r and $\theta\approx 0.1645<\frac{1}{6}$, breaking the long-standing Weyl exponent barrier. In fact, we develop a general new theory of estimation of short exponential sums involving p-adically analytic phases, which can be naturally seen as a p-adic analogue of the method of exponent pairs. This new method is presented in a ready-to-use form and applies to a wide class of well-behaved phases including many that arise from a stationary phase analysis of hyper-Kloosterman and other complete exponential sums.

1. Introduction and statement of results

One of the principal questions about L-functions is the size of their critical values. In this paper, we address an instance of the subconvexity problem, which we describe below, and break a long-standing barrier known as the Weyl exponent for central values of certain Dirichlet L-functions.

In the case of the Riemann zeta-function, the distribution of values of $\zeta(\frac{1}{2}+it)$ for large t is of central interest; see Titchmarsh [Tit86]. From the functional equation and the Phragmén–Lindelöf principle, it follows that

$$|\zeta(\tfrac{1}{2}+it)|\ll(1+|t|)^{\theta+\epsilon} \tag{1}$$

with $\theta=\frac{1}{4}$. The Lindelöf hypothesis, the statement that (1) holds with $\theta=0$, is a consequence of the celebrated Riemann hypothesis and lies very much out of reach of current methods, but an estimate of the form (1) where $\theta<\frac{1}{4}$ has important implications. It was proved by Hardy and Littlewood, by using Weyl differencing, that (1) holds with $\theta=\frac{1}{6}$. This exponent was lowered by Walfisz [Wal24] in 1924 to $\theta=\frac{163}{988}\approx 0.1650$; many subsequent papers slowly improved the result to the current value $\theta=\frac{53}{342}\approx 0.1550$, due to Bourgain [Bou14] (see also [Hux05]).

For an automorphic representation π of $\mathrm{GL}(n)$, the statement that

$$|L(\tfrac{1}{2},\pi)|\ll C(\pi)^{\theta+\epsilon}, \tag{2}$$

where $C(\pi)$ is the analytic conductor of π as defined by Iwaniec and Sarnak [IS00] and $\theta=\frac{1}{4}$, is known as the convexity bound and follows from the basic analytic properties of $L(s,\pi)$. The *subconvexity conjecture* states that such a bound always holds for some $\theta<\frac{1}{4}$. Proving a

Received 20 July 2014, accepted in final form 2 October 2014, published online 3 November 2015.
2010 Mathematics Subject Classification 11L07, 11M06 (primary), 11L03, 11L26, 11L40, 11S80, 26E30 (secondary).
Keywords: L-functions, subconvexity, van der Corput's method, p-adic analysis, exponential sums, character sums, depth aspect, method of stationary phase, exponent pairs.

Project sponsored by the National Security Agency under Grant Number H98230-14-1-0139.

subconvex estimate for any given L-function requires deep arithmetic considerations and can have important arithmetic, geometric, or dynamical consequences; see surveys [IS00, Mic07]. Many cases of subconvexity on lower-dimensional groups have been proved, often with exponents θ very close to $\frac{1}{4}$. A breakthrough paper of Michel and Venkatesh [MV10] contains a fully general subconvexity estimate for GL(2) L-functions (with θ close to $\frac{1}{4}$) by a geometric method and references to previous results. In some cases, $\theta = \frac{1}{6}$ was proved, and such a result goes under the name of *Weyl exponent*.

In the case of a Dirichlet L-function of a character χ modulo q, the corresponding statement that

$$|L(\tfrac{1}{2},\chi)| \ll q^{\theta+\epsilon} \tag{3}$$

is known only with $\theta = \frac{3}{16} = 0.1875$, due to Burgess [Bur63]. That the Weyl exponent $\theta = \frac{1}{6}$ is not known for this family is a major source of frustration. However, building on the ideas of Postnikov [Pos55], Barban *et al.* [BLT64] proved estimates allowing them to take $\theta = \frac{1}{6}$ when considering Dirichlet L-functions $L(s,\chi)$ associated to characters χ modulo p^n, where p is a fixed prime and $n \to \infty$. This result was generalized by Heath-Brown [Hea78] to a hybrid bound that contains (3) with an exponent $\frac{1}{6} \leqslant \theta < \frac{1}{4}$ assuming that the modulus q has a divisor d in a suitable range, with $\theta = \frac{1}{6}$ for moduli q having a divisor $d \asymp q^{1/3+o(1)}$ (including all sufficiently powerful moduli). Using a very different approach, Conrey and Iwaniec [CI00] obtained the Weyl exponent $\theta = \frac{1}{6}$ in the case when χ is a real (that is, quadratic) character.

The first main result of this article is the following theorem.

Theorem 1. *Let $\theta > \theta_0 \approx 0.1645$ be given. There is an $r \geqslant 0$ such that*

$$L(\tfrac{1}{2},\chi) \ll p^r \cdot q^{\theta}(\log q)^{1/2}$$

holds for every Dirichlet character χ to any prime power modulus $q = p^n$.

In particular, we see that, for sufficiently large $n \geqslant n_0$, Theorem 1 yields the subconvexity bound (3) with $\theta < \frac{1}{6}$. We stress that, even though our method is p-adic, the implied constant and the values of r and n_0 in Theorem 1 depend only on the value of θ and are *universal across all primes* p and all prime powers $q = p^n$. This is the first family of L-functions since Walfisz's 1924 result for the Riemann zeta-function in which a better exponent than $\frac{1}{6}$ has been obtained.

As the principal device of this paper, we develop a theory of estimation of exponential sums of the form

$$\sum_{M<m\leqslant M+B} e\biggl(\frac{f(m)}{p^n}\biggr), \tag{4}$$

where $f(t)$ is an analytic function on the ring $\mathbb{Z}_p$ of p-adic integers satisfying certain conditions. Here, and throughout the paper, $e(x)$ denotes $e^{2\pi i x}$ and its obvious unique extension from $\bigcup_{k\in\mathbb{Z}} p^k\mathbb{Z}$ to a $\mathbb{Z}_p$-periodic function on $\mathbb{Q}_p$. In Definition 1 (§ 3, below), we specify a class of (p-adically analytic) power series $\mathbf{F}$, which includes multiples $a\log_p(1+p^\kappa t)$ of the p-adic logarithm, and to which our estimates apply. Roughly speaking, series f in $\mathbf{F}$ satisfy $f'(t) = p^w\omega'(1+p^\kappa\omega t)^{-y} + p^w\gamma_0 + p^{u+w}g(t)$ with suitable parameters (which vary and are suppressed in this introduction) and a power series g satisfying suitable conditions (ensuring it does not interfere with the first, leading term). We call a pair of non-negative real numbers (k,ℓ) a p-adic exponent pair if, roughly, for every $f \in \mathbf{F}$ as above, every sufficiently large n, and every $0 < B \leqslant p^{n-w-\kappa}$,

$$\sum_{M<m\leqslant M+B} e\biggl(\frac{f(m)}{p^n}\biggr) \ll p^r\biggl(\frac{p^{n-w-\kappa}}{B}\biggr)^k B^\ell(\log p^{n-w-\kappa})^\delta,$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

with some r, δ depending on the exponent pair and the parameters implied in f. We will only need $\delta \in [0,1]$ in the exponent pairs we construct. In fact, we will be rather more precise and talk about *p-adic exponent data* in order to track all dependencies explicitly; see Definition 2 (§ 3, below).

The heart of our method of estimating sums of the form (4) is contained in Theorems 4 and 5, which we term B- and A-processes, respectively. An immediate consequence of these results is the following compact statement.

Theorem 2. *If (k,ℓ) is a p-adic exponent pair, then so are*

$$A(k,\ell) = \left(\frac{k}{2(k+1)}, \frac{k+\ell+1}{2(k+1)}\right) \quad \textit{and} \quad B(k,\ell) = \left(\ell - \frac{1}{2}, k + \frac{1}{2}\right).$$

Starting from the 'trivial' p-adic exponent pair $(0,1)$, we obtain with use of Theorem 2 further pairs: $B(0,1) = (\frac{1}{2}, \frac{1}{2})$ (which corresponds to a variant of the Pólya–Vinogradov inequality), $AB(0,1) = (\frac{1}{6}, \frac{2}{3})$, and infinitely many more, including, for example, $ABA^3B(0,1) = (\frac{11}{82}, \frac{57}{82})$.

Section 3, among other things, also presents the intuition behind the class $\mathbf{F}$ and Theorem 2 and describes a typical use of our method as well as further examples of phases in $\mathbf{F}$ that naturally arise in analytic number theory.

We step back for a moment to reflect on the analogy with the Archimedean aspect. The parallel between the subconvexity problem (1) in the t-aspect and (3) in the *'depth' aspect* (level p^n, $n \to \infty$) is particularly natural from the adelic point of view: one focuses on ramification at a single Archimedean or non-Archimedean place (or at a few places at once in hybrid bounds). The best available improvements on the bound (1) are obtained by estimating the exponential sum $\sum_{N<n\leqslant N+M} n^{it}$ in short intervals ($M \ll (1+|t|)^{1/2+\epsilon}$). The method of exponent pairs of van der Corput [VdC22], Phillips [Phi33], and Rankin [Ran55], a fundamental tool in the theory of exponential sums, relies on the iteration of two 'processes', the ('Archimedean') A- and B-process, which exploit the arithmetic structure by transforming a given exponential sum into rather different sums with different ranges of summation. Graham and Kolesnik [GK91] give an excellent survey of the theory of exponential sums. Note that transformations of p-adic exponent pairs given by Theorem 2 formally coincide with those provided by the Archimedean A- and B-processes.

The 'q-analogues' of Weyl differencing allowed previous researchers to establish the Weyl exponent in the context of estimating $L(\frac{1}{2},\chi)$ with a character χ to a powerful modulus and the associated exponential sums [Pos55, BLT64, FGM76, Hea78]. In Theorem 5, which establishes the A-process as a recursive process relying on a q-analogue of the Weyl–van der Corput inequality (Lemma 11), we embrace a different paradigm of f as a p-adic analytic function rather than a finite (essentially cubic in the works just referenced) polynomial. This allows us to obtain more general results, leaves us flexibility for iterative estimates, and brings to the fore the analogy with the Archimedean situation, while also presenting some serious difficulties which we overcome in the proof. Vinogradov's method was also applied by Gallagher [Gal72] and Iwaniec [Iwa74] in the study of zero-free regions for $L(s,\chi)$ near the line $\operatorname{Re} s = 1$ and the prime number theorem in arithmetic progressions to powerful moduli. Note that iterations of the A-process alone yield exponent pairs (k,ℓ) in which k is very small and ℓ is very close to 1; such estimates are suitable in ranges relevant to the behavior close to the edge of the critical strip.

Theorem 4 establishes the analogue of the B-process. Along with Lemmas 9 and 10 and Theorem 3 which we develop in the course of proving it, this result appears to have no nontrivial precedents in the literature. Our approach involves a careful application of p-adic Poisson

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

summation, with the Fourier transform $\hat{\mathbf{e}}_f(s)$ given by a complete exponential sum as in (23). We analyze such a sum using the p-adic analogue of the method of stationary phase (Lemma 7), which expresses it as a sum of contributions over all approximate critical points. In Lemma 9, we show that all such points indeed arise from actual, non-singular p-adic critical points and develop a p-adic implicit function theorem to express the critical points through analytic functions. This analysis culminates with Lemma 10, in which we evaluate $\hat{\mathbf{e}}_f(s)$ in appropriate ranges. We show that contributions from all approximate critical points can be collected via the p-adic Gaussian, and find that, for any given $f \in \mathbf{F}$, $\hat{\mathbf{e}}_f(s)$ vanishes unless s lies in a certain arithmetic progression (roughly) of the form $a_0 + p^\kappa t$, in which case an extremely handsome formula

$$\hat{\mathbf{e}}_f(a_0 + p^\kappa t) = \epsilon p^{(n-w+\kappa)/2} e\biggl(\frac{\breve{f}(t)}{p^n}\biggr)$$

holds, with some $\breve{f} \in \mathbf{F}$. As a particularly pleasing application, we obtain, in Theorem 3, a summation formula in which an exponential sum involving f is related to its 'dual sum', an exponential sum involving $\breve{f}$, with a long original sum giving rise to a short dual sum and conversely. The statement of the B-process, Theorem 4, follows when the existing pair (k, ℓ) is applied to the dual sum. In fact, the summation formula turns out to be extremely versatile, and we use it in the proof of the A-process (Theorem 5) to obtain tighter estimates.

Exponential sums of the form (4) enter the estimation of the central value $L(\frac{1}{2}, \chi)$ via the approximate functional equation. As we will see in § 6, every character χ modulo p^n satisfies $\chi(1 + p^\kappa t) = e(a \log_p(1 + p^\kappa t)/p^n)$ for some $a \in \mathbb{Z}_p$, with $a \in \mathbb{Z}_p^\times$ corresponding to primitive characters (here, we can take $\kappa = 1$ for odd p). After splitting the Dirichlet polynomials according to classes modulo p^κ and applying a p-adic exponent pair (k, ℓ), the best value of the exponent θ which can be obtained in the estimate of Theorem 1 is given by $\frac{1}{2}(k + \ell) - \frac{1}{4}$; see Theorem 6. (In fact, while the factor $(\log q)^{1/2}$ in Theorem 1 is not needed with the present slick formulation, we keep it there so that the values of r and θ arising from the p-adic exponent data apply verbatim without modification.) In particular, the trivial pair $(0, 1)$ recovers the convexity bound $\theta = \frac{1}{4}$, the pair $(\frac{1}{6}, \frac{2}{3})$ gives the Weyl exponent $\theta = \frac{1}{6}$, while already the pair $(\frac{11}{82}, \frac{57}{82})$ gives $\theta = \frac{27}{164} \approx 0.1646$, breaking the Weyl exponent barrier in this family. In light of Theorem 2, the set of p-adic exponent pairs obtainable by the p-adic A- and B-processes coincides with the classical situation. Rankin [Ran55] found the infimum of $(k+\ell)$ over all exponent pairs obtainable by A- and B-processes; his result gives the value of $\theta_0 \approx 0.1645$ in Theorem 1.

With trivial modifications, our proof yields the bound $L(\frac{1}{2} + it, \chi) \ll (1 + |t|)^A p^r q^\theta (\log q)^{1/2}$ with $A = \frac{5}{4}$, applicable along the entire critical line; see the remark after the proof of Theorem 6 for details. A hybrid bound also subconvex in t or even of sub-Weyl strength in both t- and q-aspects would be very interesting, but we do not pursue it here.

In addition to its intrinsic interest and the context into which it puts the method of exponential sums, the importance of Theorem 1 lies in how it informs our understanding of the various aspects of the subconvexity problem (including the t-aspect, the 'depth' aspect with which we are concerned, and the q-aspect) and of the available methods. We prefer to think of our A- and B-processes not as static estimates but as dynamical ways to *transform* (possibly incurring inequalities) a sum into (possibly a number of) other sums, which can in turn be transformed time and again, exploiting and transcoding the arithmetic structure present in the original sum. In this light, the fact that the analogous steps can be used in the transformations of p-adic and Archimedean sums indicates a deep analogy of their built-in, 'genetic' arithmetic structures.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

From a generalist point of view (such as Selberg class), it is generally believed [MV10] that the analytic behavior of L-functions is controlled in a universal fashion by the conductors $C(\pi)$. Theorem 1 points at intrinsic features of the depth aspect and helps shed light on the structure that distinguishes between those families of L-functions in which the Weyl subconvexity exponent $\theta = \frac{1}{6}$ is available through current techniques from those in which the naturally obtained exponent is Burgess's $\theta = \frac{3}{16}$. The universality of these exponents and techniques which allow one to break them and obtain better estimates toward the Lindelöf hypothesis were principal research themes of a 2006 workshop at the American Institute of Mathematics [Ric06]. Subsequent to the current paper, in [BM15a], Blomer and the author consider the subconvexity problem $L(\frac{1}{2}, f\otimes\chi) \ll_f (q^2)^{\theta+\epsilon}$ for character twists of a $\mathrm{GL}(2)$ L-function, in which $\theta = \frac{3}{16}$ is currently the best known result in general, and develop further p-adic tools to obtain the Weyl exponent $\theta = \frac{1}{6}$ in depth aspect and corresponding estimates for twisted sums of Hecke eigenvalues. For other recent striking examples of the distinctive rôle played by the square-full direction in analytic number theory, see [Hia14, NPS14, Tem14, Vis13]. Strong results can also be obtained in a number of problems when the modulus is well-factorable or 'smooth'; see, for example, [BM15b], or [HMQ14] for a hybrid subconvexity bound (3) for Dirichlet L-functions to factorable moduli.

The close of this introduction is a good place to open several questions suggested by our work. A number of subconvexity, non-vanishing, and moments-related problems for L-functions have so far found stronger answers in the t-aspect than in the q-aspect. The results of the present paper and [BM15a] indicate that the analogy with the depth aspect carries over in some of them; it will be interesting to see further ways in which it intervenes and how far it goes. Quantitatively stronger or hybrid (adelic in a sense) versions of Theorem 1 would also appear seriously interesting; the author has obtained some positive results in the initial investigations in this direction. Finally, our results establish a theory of short exponential sums involving p-adically analytic fluctuations independent of the specific application to Theorem 1. There are many applications of the method of (Archimedean) exponential sums to problems other than estimates of L-functions (such as in the geometry of numbers), and our results are general enough to be appropriate analogues of the machinery that is needed to break the canonical exponents in most of the better known of these applications; it appears extremely intriguing to investigate whether some of these questions have appropriate p-adic analogues.

Several notations will be used throughout the paper. For a positive integer i, we write

$$(y)_i = y(y-1)\cdots(y-i+1).$$

For $y \in \mathbb{Q}^+$, let $\iota(y) = \max(0, \mathrm{ord}_p(y^{-1}))$ and $\iota'(y) = \max(0, \mathrm{ord}_p\, y)$, so that $\mathrm{ord}_p\, y = \iota'(y) - \iota(y)$. We also write ι and ι' for $\iota(y)$ and $\iota'(y)$, respectively, when the value of y is unambiguous from the context. We denote $\varepsilon(y) = 1$ if $\mathrm{ord}_p\, y \neq 0$ and $\varepsilon(y) = 0$ if $\mathrm{ord}_p\, y = 0$. We write $f \ll g$ or $f = \mathrm{O}(g)$ to denote that $|f| \leqslant Cg$ for some constant C, or, equivalently, that $\limsup(|f|/g) < +\infty$.

2. Preliminaries on p-adic analysis

In this section, we collect facts about p-adic exponential, logarithmic, and power series and prove several auxiliary results related to these p-adic series which will be useful in our later capstone estimates. The reader is encouraged to postpone details of proofs for the second reading. Much of the pain in this section comes from the occasional need, inherent in the method of exponent pairs, to deal with power series of the form $(1 + p^\kappa t)^y$, even when $\mathrm{ord}_p\, y \neq 0$, and our desire to minimize losses while doing so.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Throughout this section, all formal power series have coefficients in $\mathbb{Q}_p$ unless specified otherwise. For such a series $a(t)=\sum_{k=0}^{\infty}a_kt^k$, we follow the notation of [Rob00] and denote its radius of convergence by

$$r_a=\sup\{r\geqslant 0:\lim|a_k|_pr^k=0\}=\bigl(\limsup|a_k|_p^{1/k}\bigr)^{-1}\tag{5}$$

and its growth modulus by

$$M_ra=M_r(a)=\max|a_k|_pr^k\quad(0\leqslant r<r_a).$$

Note that we may very well have $\log_p r_a\in\mathbb{R}\backslash\mathbb{Z}$ even though each $\log_p|a_k|_p$ is an integer. We will write $M_ra\doteq|a_{k_0}|_pr^{k_0}$ if there is a unique $k_0\in\mathbb{N}$ achieving the maximum and the value of k_0 is clear from the context; such radii r are said to be regular.

We record the following standard fact.

Lemma 1. *Let $f(t)=\sum_{k=0}^{\infty}a_kt^k=a_0+tf_1(t)$ be a formal power series with $a_1\neq 0$, and let $0<r<r_f$ be such that $M_rf_1\doteq|a_1|_p$. Then, for every x,y with $|x|_p,|y|_p\leqslant r$, we have $|f(x)-f(y)|_p=|a_1|_p|x-y|_p$. In other words, for every x, y with $|x|_p,|y|_p\leqslant r$,*

$$f(x)\equiv f(y)\pmod{p^j|a_1|_p^{-1}}\iff x\equiv y\pmod{p^j}.$$

Proof. The proof is simple. We have that, for every $k\geqslant 2$,

$$\begin{aligned}|a_k(x^k-y^k)|_p&=|a_k(x-y)(x^{k-1}+x^{k-2}y+\cdots+y^{k-1})|_p\\&\leqslant|a_k|_pr^{k-1}\cdot|x-y|_p<|a_1|_p|x-y|_p.\end{aligned}$$

Therefore,

$$|f(x)-f(y)|_p=\biggl|\sum_{k=1}^{\infty}a_k(x^k-y^k)\biggr|_p=|a_1|_p|x-y|_p.\qquad\square$$

For two power series $f(t)$ and $g(t)$ such that $g(0)=0$, one can define purely formally the power series $(f\circ g)(t)=f(g(t))$ obtained by formal substitution. On the other hand, for any power series $a(t)=\sum_{k=0}^{\infty}a_kt^k$, we can define its derivative series $Da(t)=a'(t)=\sum_{k=1}^{\infty}ka_kt^{k-1}$. The usual rules for differentiation hold, including the sum and product rules, as well as the chain rule,

$$D(f\circ g)(t)=Df(g(t))Dg(t),\tag{6}$$

valid for any two power series f and g with $g(0)=0$ [Rob00, p. 289].

We will repeatedly use the following standard proposition, which gives a sufficient condition for this substitution to correspond to numerical substitution in convergent p-adic power series.

Lemma 2. *Let f and g be two convergent power series with $g(0)=0$. If $|x|<r_g$ and $M_{|x|}(g)<r_f$, then $r_{f\circ g}>|x|$ and the numerical evaluation of the composite $f\circ g$ can be made according to*

$$(f\circ g)(x)=f(g(x)).$$

Proof. This statement is from [Rob00, p. 294]. □

In particular, consider the power series

$$\varepsilon(x)=\exp_p(x)=\sum_{k=0}^{\infty}\frac{1}{k!}x^k=1+\varepsilon_0(x),\quad\lambda(x)=\log_p(1+x)=\sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{k}x^k.$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Recall that

$$\operatorname{ord}_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots < \frac{k}{p-1}, \quad \text{and so} \quad \operatorname{ord}_p(k!) \leqslant \frac{k-1}{p-1}.$$

It is therefore seen that

$$\begin{array}{lll} r_\varepsilon = r_{\varepsilon_0} = r_p, & M_r\varepsilon_0 \doteq r & \text{for all } r < r_p, \\ r_\lambda = 1, & M_r\lambda \doteq r & \text{for all } r < r_p, \end{array}$$

where $r_p = p^{-\rho_p}$, $\rho_p = 1/(p-1)$. Moreover, if $\mathcal{O}$ is any complete valuation ring extension of $\mathbb{Z}_p$ (possibly $\mathcal{O} = \mathbb{Z}_p$) and K is the field of fractions of $\mathcal{O}$, and if $B_r = \{t \in \mathcal{O} : |t|_p < r\}$, then $\varepsilon_0, \lambda : B_{r_p} \to B_{r_p}$ are isometries such that, according to Lemma 2, $\varepsilon_0 \circ \lambda = \lambda \circ \varepsilon_0 = \mathrm{id}_{B_{r_p}}$.

Of particular interest to us will be the power series $\pi^y(x)$, defined for $y \in K^\times$ as

$$\pi^y(x) = 1 + \pi_0^y(x) = \varepsilon(y\lambda(x)) = \sum_{k=0}^{\infty} \binom{y}{k} x^k.$$

It is easy to see that the radius of convergence $r_{\pi^y} = r_{\pi_0^y}$ equals ∞ if $y \in \mathbb{N}_0$, 1 if $\iota(y) = 0$ and $y \notin \mathbb{N}_0$, and $r_p p^{-\iota(y)}$ if $\iota(y) > 0$. In any case, for $r < r_p p^{-\iota(y)}$, the above composition is also valid as a numerical evaluation by Lemma 2, and $M_r\pi_0^y \doteq |y|_p r$. Moreover, $\pi_0^y : B_{r_p p^{-\iota(y)}} \to B_{r_p p^{-\iota'(y)}}$ is an isometry such that $\pi_0^{1/y} \circ \pi_0^y = \mathrm{id}_{B_{r_p p^{-\iota(y)}}}$. We write $\pi^y(x) = (1+x)^y$. We have that

$$\big((1+x_1)(1+x_2)\big)^y = (1+x_1)^y(1+x_2)^y \tag{7}$$

for all $x_1, x_2 \in B_{r_p p^{-\iota(y)}}$.

In particular, the equation $(1+x)^y = 1+t$ has a solution $x \in B_{r_p p^{-\iota(y)}}$ if and only if $t \in B_{r_p p^{-\iota'(y)}}$, in which case the solution is unique and given by $1 + x = (1+t)^{1/y}$.

Among all power series $a(t) = \sum_{k=0}^{\infty} a_k t^k$ with coefficients $a_k \in \mathbb{Z}_p$, we consider the following subsets:

$$\begin{aligned} \mathbf{I}_0(\mathbb{Z}_p) &= \{a(t) : a_k \in \mathbb{Z}_p \, (k \geqslant 0), \ \lim |a_k|_p = 0\}, \\ \mathbf{I}(\mathbb{Z}_p) &= \mathbb{Z}_p + pt\mathbf{I}_0(\mathbb{Z}_p) = \{a(t) : a_0 \in \mathbb{Z}_p, \ a_k \in p\mathbb{Z}_p \, (k \geqslant 1), \ \lim |a_k|_p = 0\}, \\ \mathbf{I}^\times(\mathbb{Z}_p) &= \mathbb{Z}_p^\times + pt\mathbf{I}_0(\mathbb{Z}_p) = \{a(t) : a_0 \in \mathbb{Z}_p^\times, \ a_k \in p\mathbb{Z}_p \, (k \geqslant 1), \ \lim |a_k|_p = 0\}, \\ \mathbf{I}^1(\mathbb{Z}_p) &= (1 + p\mathbb{Z}_p) + pt\mathbf{I}_0(\mathbb{Z}_p) = 1 + p\mathbf{I}_0(\mathbb{Z}_p), \\ \mathbf{I}_\kappa^1(\mathbb{Z}_p) &= (1 + p^\kappa\mathbb{Z}_p) + p^\kappa t\mathbf{I}_0(\mathbb{Z}_p) = 1 + p^\kappa\mathbf{I}_0(\mathbb{Z}_p). \end{aligned}$$

We see that all power series in the ring $\mathbf{I}_0(\mathbb{Z}_p)$ define analytic functions $\mathbb{Z}_p \to \mathbb{Z}_p$, that $\mathbf{I}(\mathbb{Z}_p)$ is a subring of $\mathbf{I}_0(\mathbb{Z}_p)$, and that $\mathbf{I}^\times(\mathbb{Z}_p)$ is the group of invertible elements of $\mathbf{I}(\mathbb{Z}_p)$. We note for reference that obviously

$$\begin{array}{ll} r_a \geqslant 1 & \text{for all } a \in \mathbf{I}_0(\mathbb{Z}_p), \\ M_r(a) \leqslant 1 & \text{for all } r \leqslant 1, \ a \in \mathbf{I}_0(\mathbb{Z}_p), \\ M_r(a) \doteq 1 & \text{for all } r \leqslant 1, \ a \in \mathbf{I}^\times(\mathbb{Z}_p). \end{array}$$

Let $y \in \mathbb{Q}_p^\times$ and an integer $\kappa \geqslant 1 + \iota'(2)$ be arbitrary, and let $\iota = \iota(y)$, $\iota' = \iota'(y)$, so that $\kappa + \iota' = \kappa + \iota + \operatorname{ord}_p y$. Then the power series $\pi_{[\kappa+\iota]}^y(x) = 1 + \pi_{[\kappa+\iota]0}^y(x) = (1 + p^{\kappa+\iota}x)^y$ satisfies

$$M_r\pi_{[\kappa+\iota]0}^y \doteq |y|_p p^{-\kappa-\iota} r = p^{-\kappa-\iota'} r$$

for every $r < p^\kappa r_p$ (in particular for $r = 1$), and $\pi_{[\kappa+\iota]}^y$ belongs to $\mathbf{I}_{\kappa+\iota'}^1(\mathbb{Z}_p)$.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

We will also consider, for any given $\lambda \in \mathbb{R}_{\geqslant 0}$, the following subspaces of $\mathbf{I}_0(\mathbb{Z}_p)$:

$$\begin{aligned} \mathbf{I}_0[\lambda](\mathbb{Z}_p) &= \{a(t) \in \mathbf{I}_0(\mathbb{Z}_p) : \operatorname{ord}_p a_k \geqslant \lceil k\lambda \rceil \ (k \in \mathbb{N}_0)\}, \\ \mathbf{I}_0^n[\lambda](\mathbb{Z}_p) &= t\mathbf{I}_0[\lambda](\mathbb{Z}_p), \\ \mathbf{I}_\kappa^1[\lambda](\mathbb{Z}_p) &= (1 + p^\kappa \mathbb{Z}_p) + p^\kappa \mathbf{I}_0^n[\lambda](\mathbb{Z}_p). \end{aligned} \tag{8}$$

For example, if $\lambda \in \mathbb{N}_0$, then $\mathbf{I}_0[\lambda](\mathbb{Z}_p)$ consists of power series of the form $a(t) = a_1(p^\lambda t)$ for some $a_1(t) \in \mathbf{I}_0(\mathbb{Z}_p)$. It is clear that each $\mathbf{I}_0[\lambda](\mathbb{Z}_p)$ is a ring, that $\mathbf{I}_0^n[\lambda](\mathbb{Z}_p)$ is an $\mathbf{I}_0[\lambda](\mathbb{Z}_p)$-module, and that, when $\kappa \geqslant \lambda$, $\mathbf{I}_\kappa^1[\lambda](\mathbb{Z}_p)$ is a subgroup of $\mathbf{I}_0[\lambda](\mathbb{Z}_p)^\times$. It is also clear that $r_a \geqslant p^\lambda$ for every $a(t) \in \mathbf{I}_0[\lambda](\mathbb{Z}_p)$.

The relevance of these classes for us stems from the fact that, as is easily verified,

$$\pi_{[\kappa+\iota]}^y \in \begin{cases} \mathbf{I}_{\kappa+\iota'}^1[\kappa - \rho_p](\mathbb{Z}_p), & \operatorname{ord}_p y \neq 0, \\ \mathbf{I}_{\kappa+\iota'}^1[\kappa](\mathbb{Z}_p), & \operatorname{ord}_p y = 0. \end{cases}$$

We can write $\pi_{[\kappa+\iota]}^y \in \mathbf{I}_{\kappa+\iota'}^1[\kappa - \rho_p(y)](\mathbb{Z}_p)$, where $\rho_p(y)$ equals ρ_p if $\operatorname{ord}_p y \neq 0$ and 0 otherwise.

For every $a(t) \in \mathbf{I}_{\kappa+\iota}^1(\mathbb{Z}_p)$, $a(t) = a_0 + p^{\kappa+\iota} t a_1(t)$, $a_0 \in (1 + p^{\kappa+\iota}\mathbb{Z}_p)$, $a_1(t) \in \mathbf{I}_0(\mathbb{Z}_p)$, we can consider $a(t)^y = a_0^y(1 + p^{\kappa+\iota} a_0^{-1} t a_1(t))^y$, with the latter power defined by formal substitution. This power series $a(t)^y$ belongs to $\mathbf{I}_{\kappa+\iota'}^1(\mathbb{Z}_p)$. According to Lemma 2, the values $a(t)^y$ can be numerically evaluated as compositions for $t \in \mathbb{Z}_p$. In particular, for every two $a(t), b(t) \in \mathbf{I}_{\kappa+\iota}^1(\mathbb{Z}_p)$, we have, according to (7), the equality of values

$$(a(t)b(t))^y = a(t)^y b(t)^y$$

for every $t \in \mathbb{Z}_p$. Consequently, both sides of this equation must also agree as power series in $\mathbf{I}_{\kappa+\iota'}^1(\mathbb{Z}_p)$. Similarly, let $a(t) \in \mathbf{I}_{\kappa+\iota}^1(\mathbb{Z}_p)$, and let $b(t) = a(t)^y \in \mathbf{I}_{\kappa+\iota'}^1(\mathbb{Z}_p)$. For every $t \in \mathbb{Z}_p$, we have an equality of values $a(t)^y = b(t)$ in $1 + p^{\kappa+\iota'}\mathbb{Z}_p$. Therefore, we must also have

$$a(t) = b(t)^{1/y}$$

as an equality of values $a(t) = b(t)^{1/y}$ in $1 + p^{\kappa+\iota}\mathbb{Z}_p$ for every $t \in \mathbb{Z}_p$, and therefore also as an equality of series in $\mathbf{I}_{\kappa+\iota}^1(\mathbb{Z}_p)$.

Finally, we comment on the compositions of series of the form (8). Suppose that $a(t) = \sum_{k=0}^\infty a_k t^k \in \mathbf{I}_0[\lambda_a](\mathbb{Z}_p)$ and $b(t) = t\sum_{k=0}^\infty b_k t^k \in \mathbf{I}_0^n[\lambda_b](\mathbb{Z}_p)$, where $\lambda_a > 0$. For every $r < p^{\lambda_b}$, $M_r(b) \leqslant r$, so that numerical substitution in $a(b(t))$ is allowed for all $r < \min(p^{\lambda_a}, p^{\lambda_b})$ according to Lemma 2. Moreover, from the formal substitution

$$a(b(t)) = \sum_{k=0}^\infty a_k t^k \bigg(\sum_{\ell=0}^\infty b_\ell t^\ell\bigg)^k = \sum_{k=0}^\infty \bigg(\sum_{k=k_0+\ell_1+\cdots+\ell_{k_0}} a_{k_0} b_{\ell_1} \ldots b_{\ell_{k_0}}\bigg) t^k,$$

it is clear that $(a \circ b) \in \mathbf{I}_0[\min(\lambda_a, \lambda_b)](\mathbb{Z}_p)$. If, in addition, $a(t) \in \mathbf{I}_\kappa^1[\lambda_a](\mathbb{Z}_p)$ for some $\kappa \geqslant \lambda_a$, then it follows from above that $(a \circ b)(t) \in \mathbf{I}_\kappa^1[\min(\lambda_a, \lambda_b)](\mathbb{Z}_p)$. In particular, if $a(t) \in \mathbf{I}_{\kappa+\iota}^1[\lambda](\mathbb{Z}_p)$, then $a(t)^y \in \mathbf{I}_{\kappa+\iota'}^1[\min(\kappa - \rho_p(y), \lambda)](\mathbb{Z}_p)$.

The following two Lemmas 3 and 4 will be useful in obtaining successive convergents to the solution of an implicit function problem in Lemma 9.

Lemma 3. *Let $y \in \mathbb{Q}_p^\times$ and $\kappa \in \mathbb{N}$ be arbitrary, and let $\iota = \iota(y)$, $\iota' = \iota'(y)$. Further, let $a(t)$ and $b(t)$ be two power series with $a(t) \in \mathbf{I}_{\kappa+\iota}^1[\lambda_a](\mathbb{Z}_p)$ and $b(t) \in \mathbf{I}_0^n[\lambda_b](\mathbb{Z}_p)$, $\lambda_a, \lambda_b \geqslant 0$. Then there exists a power series $\tilde{b}(t) \in \mathbf{I}_0^n[\min(\kappa - \rho_p(y), \lambda_a, \lambda_b)](\mathbb{Z}_p)$ such that*

$$(a(t) + p^{\kappa+\iota} b(t))^y = a(t)^y + p^{\kappa+\iota'} \tilde{b}(t).$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Proof. We may assume that $\lambda_a \leqslant \kappa+\iota$. Note that

$$(a(t)+p^{\kappa+\iota}b(t))^y = \big[a(t)\big(1+p^{\kappa+\iota}a(t)^{-1}b(t)\big)\big]^y = a(t)^y\big(1+p^{\kappa+\iota}a(t)^{-1}b(t)\big)^y.$$

As indicated above, we have that $a(t)^y \in \mathbf{I}^1_{\kappa+\iota'}[\min(\kappa-\rho_p(y),\lambda_a)](\mathbb{Z}_p)$, as well as $a(t)^{-1} \in \mathbf{I}^1_{\kappa+\iota}[\lambda_a](\mathbb{Z}_p)$, $a(t)^{-1}b(t) \in \mathbf{I}^n_0[\min(\lambda_a,\lambda_b)](\mathbb{Z}_p)$, and so

$$\big(1+p^{\kappa+\iota}a(t)^{-1}b(t)\big)^y \in \mathbf{I}^1_{\kappa+\iota'}[\min(\kappa-\rho_p(y),\lambda_a,\lambda_b)](\mathbb{Z}_p).$$

We can thus take

$$\tilde{b}(t) = a(t)^y\,\frac{\big(1+p^{\kappa+\iota}a(t)^{-1}b(t)\big)^y-1}{p^{\kappa+\iota'}}. \qquad \square$$

We continue with a discussion regarding formal substitution in Taylor series. We start with an easy observation [Rob00, Corollary on p. 76] that if $b_{ik} \in \mathbb{Q}_p$ $(i,k \in \mathbb{N}_0)$ are such that $\lim_{\max(i,k)\to\infty} |b_{ik}|_p = 0$, then $\sum_{i=0}^{\infty}(\sum_{k=0}^{\infty} b_{ik}) = \sum_{k=0}^{\infty}(\sum_{i=0}^{\infty} b_{ik})$.

For a power series $a(t)=\sum_{k=0}^{\infty} a_k t^k$, we can also consider its ith derivative $D_i a(t) = a^{(i)}(t) = i!\sum_{k=i}^{\infty}\binom{k}{i}a_k t^{k-i}$. The series for $D_i a$ converges on the disk of convergence D of a, and its sum agrees with the (analytic) ith derivative of a on D; in fact, it is immediate from (5) that $r_{a^{(i)}} = r_a$. Moreover, for every $x, b \in D$, we have an equality of values

$$f(x) = \sum_{i=0}^{\infty} \frac{f^{(i)}(b)}{i!}(x-b)^i, \tag{9}$$

since the order of summation can be exchanged with $b_{ik} = \binom{k}{i}a_k b^{k-i}(x-b)^i$ $(k \geqslant i)$ [Kat07, Proposition 3.22, p. 87].

On the other hand, suppose that $f_0, f_1, f_2, \ldots$ is a sequence of formal power series in $\mathbf{I}_0(\mathbb{Z}_p)$, with $f_i(t) = \sum_{k=0}^{\infty} a_{ik}t^k$. If, for every fixed $k \in \mathbb{N}_0$, $\lim |a_{ik}|_p = 0$, then we can define the formal sum $f(t) = \sum_{k=0}^{\infty}(\sum_{i=0}^{\infty} a_{ik})t^k$. If $x \in \mathbb{Q}_p$ is such that

$$\lim_{\max(i,k)\to\infty} |a_{ik}|_p|x|_p^k = 0, \tag{10}$$

then all $f_i(x)$ and $f(x)$ converge, and in fact we have an equality of values $f(x) = \sum_{i=0}^{\infty} f_i(x)$.

Finally, we will also consider, for an $i \in \mathbb{N}_0$, the class

$$\mathbf{I}_{0,i}[\lambda](\mathbb{Z}_p) = \{a(t) \in \mathbf{I}_0(\mathbb{Z}_p) : \mathrm{ord}_p\, a_k \geqslant \lceil (k+i)\lambda \rceil\ (k \in \mathbb{N}_0)\},$$

and, analogously, $\mathbf{I}^n_{0,i}[\lambda](\mathbb{Z}_p) = t\mathbf{I}_{0,i}[\lambda](\mathbb{Z}_p)$. It is easy to see that if $a(t) \in \mathbf{I}_0[\lambda](\mathbb{Z}_p)$, then $a^{(i)}(t)/i! \in \mathbf{I}_{0,i}[\lambda](\mathbb{Z}_p)$. It is also easy to see that if $a(t) \in \mathbf{I}_{0,i_a}[\lambda_a](\mathbb{Z}_p)$ and $b(t) \in \mathbf{I}^n_{0,i_b}[\lambda_b](\mathbb{Z}_p)$, then $(a \circ b) \in a(0) + \mathbf{I}_{0,i_a+i_b}[\min(\lambda_a,\lambda_b)](\mathbb{Z}_p)$ (and the term $a(0)$ may be omitted if $i_b = 0$). Also, if $a(t) \in \mathbf{I}_{0,i}[\lambda_a](\mathbb{Z}_p)$ and $b(t) \in t^j\mathbf{I}_0[\lambda_b](\mathbb{Z}_p)$, then $a(t)b(t) \in t^{\max(j-i,0)}\mathbf{I}_{0,\max(i-j,0)}[\min(\lambda_a,\lambda_b)](\mathbb{Z}_p)$.

We use these observations in the proof of the final lemma of this section.

Lemma 4. *Let $f \in \mathbf{I}_0(\mathbb{Z}_p)$, $g, h \in \mathbf{I}^n_0(\mathbb{Z}_p)$, $u \in \mathbb{N}_0$. Then*

$$f(g(t)+p^u h(t)) = \sum_{i=0}^{\infty} \frac{f^{(i)}(g(t))}{i!} p^{ui} h(t)^i.$$

In particular, if $f \in \mathbf{I}_0[\lambda_f](\mathbb{Z}_p)$, $g \in \mathbf{I}^n_0[\lambda_g](\mathbb{Z}_p)$, $h \in \mathbf{I}^n_0[\lambda_h](\mathbb{Z}_p)$, then

$$f(g(t)+p^u h(t)) = f(g(t)) + p^u f_1(t)$$

for some $f_1 \in \mathbf{I}^n_{0,1}[\min(\lambda_f,\lambda_g,\lambda_h)](\mathbb{Z}_p)$.

Proof. We have seen that if $a(t) \in \mathbf{I}_0(\mathbb{Z}_p)$ and $b(t) \in \mathbf{I}_0^n(\mathbb{Z}_p)$, then $(a \circ b) \in \mathbf{I}_0(\mathbb{Z}_p)$. From the discussion above, both sides of the first equality exist as formal power series in $\mathbf{I}_0(\mathbb{Z}_p)$, numerical substitution is allowed in all terms for $t \in p\mathbb{Z}_p$, and the values of both sides agree for all $t \in p\mathbb{Z}_p$ (in fact for all t for which $g(t), h(t) \in \mathbb{Z}_p$ and numerical substitution is allowed); therefore, they must agree as power series.

Suppose additionally that $f \in \mathbf{I}_0[\lambda_f](\mathbb{Z}_p)$, $g \in \mathbf{I}_0^n[\lambda_g](\mathbb{Z}_p)$, and $h \in \mathbf{I}_0^n[\lambda_h](\mathbb{Z}_p)$. Since $f^{(i)}(t)/i! \in \mathbf{I}_{0,i}[\lambda_f](\mathbb{Z}_p)$, we have that $f^{(i)}(g(t))/i! \in \mathbf{I}_{0,i}[\min(\lambda_f, \lambda_g)](\mathbb{Z}_p)$, and so

$$f_1(t) = \sum_{i=1}^{\infty} \frac{f^{(i)}(g(t))}{i!} p^{u(i-1)} h(t)^i \in \mathbf{I}_{0,1}^n[\min(\lambda_f, \lambda_g, \lambda_h)](\mathbb{Z}_p),$$

since $p^{u(i-1)} h(t)^i / t \in t^{i-1} \mathbf{I}_0[\lambda_h](\mathbb{Z}_p)$. □

3. p-adic exponent data and pairs

Exponential sums of the shape (4) cannot, of course, be non-trivially estimated entirely independently of the arithmetic structure of f. In this section, we define a class of functions to which our method suitably applies as well as the principal parameters of our estimates, p-adic exponent data and p-adic exponent pairs, derive some of their general properties, and give examples illustrating our definitions and their typical uses. Occasionally, and for illustrative purposes only, we reference in this section statements and equations from later sections, but, of course, all actual definitions and propositions are independent of the later material. Additional useful intuition, examples, and explanations can be found in § 6.

We may, in light of (9), think of $f(t)$ as a power series in t. Of particular interest to us will be the case when $f(t)$ is a constant multiple of the p-adic logarithm $\log_p(1 + pt)$ and B is relatively short compared with p^n. The method we develop, however, applies to estimation of sums of type (4) with a rather general f, as we discuss below. This is a very pleasing aspect of our method, although it is not entirely a matter of choice, for our recursive process produces many other f, in addition to the p-adic logarithm, which we need to be able to handle. Definition 1 gives a universe of power series in which we find it convenient to formulate our results.

Definition 1. Let $w \in \mathbb{Z}$, $u, \kappa \in \mathbb{N}$ with $\kappa \geqslant 1 + \iota'(2)$, $\lambda \in \rho_p\mathbb{N}$, $y \in \mathbb{Q}^+$, and let $\iota = \iota(y)$, $\iota' = \iota'(y)$, $\omega, \omega' \in \mathbb{Z}_p^\times$. We say that a power series $f \in \mathbb{Q}_p^\times \mathbf{I}_0(\mathbb{Z}_p)$ belongs to class $\mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$ if

$$f'(t) = p^w \omega' (1 + p^{\iota+\kappa} \omega t)^{-y} + p^w \gamma_0 + p^{u+w} g(t) \tag{11}$$

for some $\gamma_0 \in \mathbb{Z}_p$ and $g \in \mathbf{I}_0[\lambda](\mathbb{Z}_p)$. We say that f belongs to class $\mathbf{F}(w, y, \kappa, \lambda, u)$ if $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$ for some $\omega, \omega' \in \mathbb{Z}_p^\times$.

The condition $\lambda \in \rho_p\mathbb{N}$ (rather than simply $\lambda \in \mathbb{R}^+$) is used only to obtain sharper estimates in the proof of Lemma 10 and could easily be dispensed with, but the values of λ naturally obtained from our iterative method lie in this discrete set anyway. We will sometimes use the symbol ∞ in place of λ and u and say that f belongs to the class $\mathbf{F}(w, y, \kappa, \infty, \infty, \omega, \omega')$ if f satisfies Definition 1 for arbitrarily large values of λ and u, which is to say that (11) holds with $g = 0$.

The class $\mathbf{F}(w, y, \kappa, \lambda, u)$ is wholly unnecessarily restrictive. In fact, for each particular application of our method to an exponential sum involving a power series, say, in $\mathbf{I}_0(\mathbb{Z}_p)$, we really only need a finite list of non-vanishing conditions of the kind that are discussed, for example,

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

in [Hux05]. Such non-vanishing conditions are tedious but straightforward to write down in each particular instance. However, writing these conditions out in full generality appears very involved, and the class of functions we consider amply suffices for the subconvexity application. Our Definitions 1 and 2 should be compared with their Archimedean counterparts in [GK91, pp. 30–31].

Note that, for every series $f \in \mathbf{F}(w, y, \kappa, \lambda, u)$ and every $n \geqslant w$,

$$\mathbf{e}_f(m) = e\biggl(\frac{f(m)}{p^n}\biggr)$$

defines a function $\mathbf{e}_f : \mathbb{Z} \to \mathbb{C}$ which is periodic with period p^{n-w}. Indeed, by (9), we have, for every $q \in \mathbb{Z}$, an equality of values

$$f(m + p^{n-w}q) = f(m) + f'(m)p^{n-w}q + \sum_{r=2}^{\infty} \frac{f^{(r)}(m)}{r!} p^{(n-w)r} q^r.$$

Since $f'(m) \in p^w\mathbb{Z}_p$, while $\operatorname{ord}_p r! \leqslant \lfloor (r-1)\rho_p \rfloor$ and

$$\operatorname{ord}_p f^{(r)}(m) \geqslant w + \min\bigl((r-1)\kappa, u + \lceil (r-1)\lambda \rceil\bigr)$$

for every $r \geqslant 2$, we conclude that $f(m + p^{n-w}q) - f(m) \in p^n\mathbb{Z}_p$, from which the periodicity of $\mathbf{e}_f$ follows.

In this paper, we develop machinery to estimate sums of the form (4) whose general term $\mathbf{e}_f(m) = e(f(m)/p^n)$ is a periodic function arising from some $f \in \mathbf{F}(w, y, \kappa, \lambda, u)$. We give several examples illustrating varied situations in which such arithmetic sums arise as well as the rôle of various parameters in Definition 1.

Character sums

$$S_\chi(M, B) = \sum_{M < m \leqslant M+B} \chi(m)$$

for a Dirichlet character χ modulo $q = p^n$ are of classical interest and of direct relevance to our subconvexity application; we discuss them in § 6. For definiteness, suppose that χ is primitive. According to Lemma 13, there is an $a_0 \in \mathbb{Z}_p^\times$ such that

$$\chi(1 + p^{\kappa_1}t) = e\biggl(\frac{a_0 \log_p(1 + p^{\kappa_1}t)}{p^n}\biggr)$$

for every $t \in \mathbb{Z}$, where $\kappa_1 = 1 + \iota'(2)$. Splitting our character sum into classes modulo p^κ for a suitable $\kappa \geqslant \kappa_1$ and fixing, for every $1 \leqslant c \leqslant p^\kappa$ such that $p \nmid c$, an integer c' with $cc' \equiv 1 \pmod{p^n}$, we have that

$$S_\chi(M, B) = \sum_{1 \leqslant c \leqslant p^\kappa,\, p \nmid c} \chi(c) \sum_{(M-c)/p^\kappa < t \leqslant (M+B-c)/p^\kappa} e\biggl(\frac{a_0 \log_p(1 + p^\kappa c' t)}{p^n}\biggr). \tag{12}$$

Note that, for any $\omega \in \mathbb{Z}_p^\times$, since $\log_p(1+p^\kappa\omega t) \in p^\kappa\mathbf{I}_0(\mathbb{Z}_p)$ and $[\log_p(1+p^\kappa\omega t)]' = p^\kappa\omega(1+p^\kappa\omega t)^{-1}$, we have that $\log_p(1+p^\kappa\omega t) \in \mathbf{F}(\kappa, 1, \kappa, \infty, \infty, \omega, \omega)$. In particular, we have that the phase $f_c(t) = a_0 \log_p(1 + p^\kappa c' t)$ satisfies

$$f_c \in \mathbf{F}(\kappa, 1, \kappa, \infty, \infty, c', a_0c'), \tag{13}$$

so the inner sum above can be treated using our techniques.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

We see already in this example the need for the parameter κ in (11). A given arithmetic summand, such as $\chi(m)$ in this example, may exhibit its true local behavior as the exponential with a phase expressed by a well-behaved p-adic power series when restricted to a suitable p-adic neighborhood, such as the arithmetic progression $c+p^{\kappa}m$ with $\kappa \geqslant \kappa_1 = 1+\iota'(2)$. On the other hand, the phase of our exponential is also properly a polynomial in t, and sometimes it can be convenient to take a larger value of κ to obtain a lower-degree polynomial. In our case, the choices $\kappa > n/2+\mathrm{O}(1)$ and $\kappa > n/3+\mathrm{O}(1)$ produce exponential sums with a linear and quadratic phase, respectively, but of course they also require the splitting of the original sum into more pieces; we postpone the discussion of the relative utility of such choices to § 6. This first example also showcases the flexibility given by the extra parameters w, ω, and ω' in (11). As the discussion of periodicity of $\mathbf{e}_f$ indicates, changing the value of w is effectively equivalent to changing the modulus to p^{n-w}, so, while this flexibility could just as well be achieved by adjusting n, and while the value of w does change through the application of A- and B-processes, we find it convenient to keep n as a fixed parameter and track the changes in w separately. Finally the inclusion of ι in the exponent to $p^{\iota+\kappa}$ is simply a natural normalization in light of the properties of the p-adic power function $\pi^{y}(x)$ discussed in § 2 and is responsible for the elegant statement of Lemma 9.

Throughout our method, we think of the term $p^{w}\omega'(1+p^{\iota+\kappa}\omega t)^{-y}$ as the main term in (11), and we track the remaining terms to ensure that they do not interfere with the leading term. The extra flexibility afforded by allowing these smaller terms is both pleasing for the scope of our method and essential; we proceed to explain one of their sources and the rôle of parameters u and λ in controlling them. Our A-process relies on a version of Weyl differencing and reduces estimation of the sum (4) with $f \in \mathbf{F}(w,y,\kappa,\lambda,u)$ to sums involving a phase of the form

$$f_{\chi,h}(t) = f(t+p^{\chi}h) - f(t) = p^{\chi}hf'(t) + p^{2\chi}h^{2}\sum_{r=2}^{\infty} p^{(r-2)\chi}h^{r-2}\frac{f^{(r)}(t)}{r!};$$

see Lemma 12. For example, if $f(t) = f_c(t) = a_0\log_p(1+p^{\kappa}c't)$ as in the inner sum in (12), $(p^{\chi}hf'(t))' = a_0c'^2p^{\chi+2\kappa}h(1+p^{\kappa}c't)^{-2}$. The infinite sum contributes a secondary term (whose derivative is $p^{u+w}g(t)$ in (11)) which we must keep carrying while ensuring that it does not interfere with the main term, especially in light of the implicit function theorem (Lemma 9); this separation is the rôle of the parameter u. Moreover, the quantity $u+\lfloor\lambda\rfloor-\kappa-\iota'$ turns out to control both the new value of u for the phase $f_{\chi,h}$ in Lemma 12 and the success of Lemmas 9 and 10. The parameter λ is a measure of decay of coefficients of $g(t)$ (recall that, for $\lambda \in \mathbb{N}_0$, $g_0(p^{\lambda}t) \in \mathbf{I}_0[\lambda](\mathbb{Z}_p)$ for every $g_0 \in \mathbf{I}_0(\mathbb{Z}_p)$, and compare with the form of the leading term) and, in a sense, helps the secondary term keep pace with the extra factor of p^{κ} that the main term inherits with each differentiation.

As our third example, we consider sums of Kloosterman sums. According to Salié's classical evaluation (see [IK04, p. 322], [BM15a, § 7]), the Kloosterman sum $S(m_1,m_2,q)$, for an odd prime power $q=p^n$ ($n \geqslant 2$) and $p \nmid m_1m_2$, vanishes unless $\left(\frac{m_1m_2}{p}\right)=1$, in which case it is explicitly given as

$$S(m_1,m_2,q) = \sum_{x \bmod q}^{*} e\left(\frac{m_1\bar{x}+m_2x}{q}\right) = q^{1/2}\sum_{\pm}\epsilon(\pm\ell,q)e\left(\pm\frac{2\ell}{q}\right),$$

where $\pm\ell$ are the two points satisfying the stationary phase condition $\ell^2 \equiv m_1m_2 \pmod{q}$ (cf. Lemma 7), and $\epsilon(a,p^n)$ is the explicit unit factor as in Lemma 8, which depends only on p, the class of $a \bmod p$, and the parity of n. We refer the reader to [BM15a] for a more refined discussion of p-adic square roots and content ourselves here with the observation that

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

if $\pm\ell=\pm\ell(c)$ are the solutions to $\ell^2\equiv c\pmod{p^n}$, then $\ell(c+p^\kappa t)\equiv\pm\ell(c)(1+p^\kappa c't)^{1/2}\pmod{p^n}$ for every $\kappa\geqslant 1$, $t\in\mathbb{Z}$. We thus have, for example,

$$\sum_{M<m\leqslant M+B}S(1,m,q)=q^{1/2}\sum_{\pm}\sum_{1\leqslant c\leqslant p^\kappa,\,p\nmid c}\epsilon(\pm\ell(c),q)\sum_{(M-c)/p^\kappa<t\leqslant(M+B-c)/p^\kappa}e\biggl(\pm\frac{f_{c,1/2}(t)}{p^n}\biggr),$$

with the phase $f_{c,1/2}(t)=2\ell(c)(1+p^\kappa c't)^{1/2}$ in the class $\mathbf{F}(\kappa,\frac{1}{2},\kappa,\infty,\infty,c',\pm2\ell(c)c')$ of Definition 1. We remark that the good analytic behavior of derivatives of solutions to the stationary phase equation is not accidental and is instead genetic to the corresponding implicit function problem.

Many other cases of complete exponential sums to prime power moduli, for example hyper-Kloosterman sums, similarly give rise to exponentials with p-adically analytic phases satisfying the conditions of Definition 1. This involves an explicit evaluation of stationary points, which leads to an implicit function problem that can, under rather general conditions, be solved within the class $\mathbf{F}$; see Lemma 9. In particular, this procedure also ultimately powers the duality approach in the proof of the B-process in § 4. Solution of the implicit function problem is another important source of the secondary term in (11) in applications. For another involved and hands-on example, in which the phase $f\in\mathbf{F}$ arises from a repeated explicit evaluation by the p-adic method of stationary phase, see [BM15a].

Finally, we discuss translational invariance in the classes $\mathbf{F}(w,y,\kappa,\lambda,u)$. For a power series $f\in\mathbb{Q}_p^\times\mathbf{I}_0(\mathbb{Z}_p)$ and any $t,M\in\mathbb{Z}_p$, we have by (9) an equality of values

$$f(M+t)=\sum_{i=0}^{\infty}\frac{f^{(i)}(M)}{i!}t^i.$$

We may therefore consider $f(M+t)$ as a power series, which we denote by $f_M(t)$. Note that the formal derivative of f_M agrees with the translation of the derivative f', that is, $(f_M)'(t)=(f')_M(t)=f'(M+t)$. The following lemma is a simple but important verification.

Lemma 5. *Each of the classes $\mathbf{I}_0(\mathbb{Z}_p)$, $\mathbf{I}_{0,j}[\lambda](\mathbb{Z}_p)$, and $\mathbf{F}(w,y,\kappa,\lambda,u)$ is invariant under translations, that is, if f belongs to one of these classes $\mathbf{C}$, then $f_M\in\mathbf{C}$ for every $M\in\mathbb{Z}_p$.*

Proof. Suppose that $f=\sum_{k=0}^\infty c_kt^k\in\mathbf{I}_0(\mathbb{Z}_p)$, so that $\lim|c_k|_p=0$, and $M\in\mathbb{Z}_p$. Then $f^{(i)}(M)/i!=\sum_{k=0}^\infty\binom{k+i}{i}c_{k+i}M^k$, and so

$$\biggl|\frac{f^{(i)}(M)}{i!}\biggr|_p\leqslant\sup_{k\geqslant0}\biggl|\binom{k+i}{i}c_{k+i}M^k\biggr|_p\leqslant\sup_{k\geqslant i}|c_k|_p\to0\quad(i\to\infty).$$

This shows that f_M is a power series with integral coefficients and that, in fact, $f_M\in\mathbf{I}_0(\mathbb{Z}_p)$. If, moreover, $f\in\mathbf{I}_{0,j}[\lambda](\mathbb{Z}_p)$, then the above estimate shows that

$$\mathrm{ord}_p(f^{(i)}(M)/i!)\geqslant\inf_{k\geqslant i}\mathrm{ord}_p\,c_k\geqslant\inf_{k\geqslant i}\lceil\lambda(k+j)\rceil=\lceil\lambda(i+j)\rceil,$$

so $f_M\in\mathbf{I}_{0,j}[\lambda](\mathbb{Z}_p)$ too.

Now, let $f\in\mathbf{F}(w,y,\kappa,\lambda,u,\omega,\omega')$, so that f' satisfies (11) with $g\in\mathbf{I}_0[\lambda](\mathbb{Z}_p)$. Then, using (7), we have for every $t\in B_{p^{-\kappa}}$ an equality of values

$$\begin{aligned}f'(M+t)&=p^w\omega'\bigl(1+p^{\iota+\kappa}\omega(M+t)\bigr)^{-y}+p^w\gamma_0+p^{u+w}g(M+t)\\&=p^w\omega'(1+p^{\iota+\kappa}\omega M)^{-y}\bigl[1+p^{\iota+\kappa}\omega(1+p^{\iota+\kappa}\omega M)^{-1}t\bigr]^{-y}+p^w\gamma_0+p^{u+w}g_M(t).\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

The right-hand side of this equality is a power series which must coincide with $(f_M)'$. We have already proved that $f_M \in \mathbb{Q}_p^\times \mathbf{I}_0(\mathbb{Z}_p)$ and that $g_M \in \mathbf{I}_0[\lambda](\mathbb{Z}_p)$, so $f_M \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega(1 + p^{\iota+\kappa}\omega M)^{-1}, \omega'(1 + p^{\iota+\kappa}\omega M)^{-y})$. □

We now define p-adic exponent data and pairs. Let P denote the set of prime numbers. For any sets X, Y, and any family of subsets $X_p \subset X$ $(p \in P)$, let $\mathbf{J}(X_p; Y)$ be the set of all functions $g : \mathbb{Q}^+ \times \bigsqcup_{p\in P}(\{p\} \times X_p) \to Y$ such that, for every $y \in \mathbb{Q}^+$, there is a finite subset $P_0(y) \subset P$ and a function $g_0 : (P \backslash P_0(y)) \times X \to Y$ such that $g(y, p, x) = g_0(p, x)$ for every $p \in P \backslash P_0(y)$ and every $x \in X_p$.

In particular, write $\mathbf{J}(Y) := \mathbf{J}(\emptyset; Y)$ for the set of functions $g(y, p) : \mathbb{Q}^+ \times P \to Y$ with the above properties, and $\mathbf{J}_1(Y) := \mathbf{J}(\mathbb{N}_p' \times \rho_p\mathbb{N}; Y)$ (with $X = \mathbb{R}^+$ and $\mathbb{N}_p' = \iota'(2) + \mathbb{N}$) for the set of such functions $g(y, p, \kappa, \lambda) : \mathbb{Q}^+ \times \bigsqcup_{p\in P}(\{p\} \times \mathbb{N}_p' \times \rho_p\mathbb{N}) \to Y$.

Classes $\mathbf{J}(Y)$ and $\mathbf{J}_1(Y)$ for appropriate Y are suitable universes for certain components of p-adic exponent data in Definition 2. For example, with variables keeping their meaning from Definition 1, $\kappa_0(y, p) \in \mathbf{J}(\mathbb{N})$ is the smallest value of κ to which our datum applies, and it may well differ from its generic value for some exceptional (y, p). For example, if a datum is obtained using our A- and B-processes, and if one of the iterations involves the power series $\pi_{[\kappa]}^{7y+2}(x)$, then it may be necessary to require a higher value of κ for those pairs (y, p) for which $\mathrm{ord}_p(7y+2) \neq 0$; when estimating (4), this simply corresponds to a finer initial splitting as in (12). We require p-adic exponent data to be universal in that they ultimately apply to all values of y and p. However, as our examples demonstrate, in a typical application we need to estimate a sum involving a phase with one specific value of y. What really matters, then, is that our method applies in a uniform (tightest possible) way for all primes outside a finite exceptional set (which may depend on y) and with a possible finite adjustment of initial conditions at the exceptional primes; this is precisely the content of our definitions, with Y denoting the universe of assumed values and with $\mathbf{J}_1(Y)$ also taking into account the possible dependence of other parameters on specific values of κ and λ. The reader interested in applications may treat quantities in classes $\mathbf{J}(Y)$ and $\mathbf{J}_1(Y)$ simply as explicit 'expressions' in terms of other parameters y, p, κ, λ, knowing that their form suffices for the purpose of estimating any given exponential sum to which our method applies.

We note on the side that, in all p-adic exponent data we produce, the functions in corresponding classes $\mathbf{J}(X_p; Y)$ actually satisfy the following stronger uniformity condition in y and p: there is a finite set $P_0 \subset P$, a finite set of non-vanishing linear forms $l_i(y) = a_i y + b_i$ $(1 \leqslant i \leqslant I)$, and functions $g_0 : \mathbb{Z}^I \times P \times X \to Y$ and $g_0' : \mathbb{Z}^I \times X \to Y$ such that $f(y, p, x) = g_0((\mathrm{ord}_p\, l_i(y))_{i=1}^I, p, x)$ for every $y \in \mathbb{Q}^+$, $p \in P$, and $x \in X_p$, as well as $g_0(z, p, x) = g_0'(z, x)$ for every $z \in \mathbb{Z}^I$, $p \in P \backslash P_0$, and $x \in X_p$.

We are now ready for the main definition.

Definition 2. Let $\mathbf{Q}$ be the set of all quintuples

$$q = (k, \ell, r, \delta, (n_0, u_0, \kappa_0, \lambda_0)) \tag{14}$$

where $k, \ell \in \mathbb{R}$, $0 \leqslant k \leqslant \frac{1}{2} \leqslant \ell \leqslant 1$, $r \in \mathbf{J}_1(\mathbb{R})$, $\delta \in \mathbb{R}_0^+$, $n_0, u_0 \in \mathbf{J}_1(\mathbb{N})$, $\kappa_0 \in \mathbf{J}(\mathbb{N})$, $\lambda_0 \in \mathbf{J}(\mathbb{R}_0^+)$, and $n_0(y, p, \kappa, \lambda) > \kappa + \iota'(y)$.

We call a quintuple $q \in \mathbf{Q}$ as in (14) a p-adic exponent datum if, for every $p \in P$, $y \in \mathbb{Q}^+$, $w \in \mathbb{Z}$, $\kappa \in \mathbb{N}$ with $\kappa \geqslant 1 + \iota'(2)$, $\lambda \in \rho_p\mathbb{N}$, $n, u \in \mathbb{N}$ such that

$$\kappa \geqslant \kappa_0(y, p), \quad \lambda \geqslant \lambda_0(y, p), \quad n \geqslant w + n_0(y, p, \kappa, \lambda), \quad u \geqslant u_0(y, p, \kappa, \lambda),$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

and for every $f \in \mathbf{F}(w, y, \kappa, \lambda, u)$, $M \in \mathbb{Z}$, and $0 < B \leqslant p^{n-w-\kappa-\iota'}$, we have the estimate

$$\sum_{M<m\leqslant M+B} e\left(\frac{f(m)}{p^n}\right) \ll p^r \left(\frac{p^{n-w-\kappa-\iota'}}{B}\right)^k B^\ell (\log p^{n-w-\kappa-\iota'})^\delta, \tag{15}$$

where $r = r(y, p, \kappa, \lambda)$, and the implied constant depends only on the datum q.

We call a pair

$$\pi = (k, \ell)$$

of non-negative numbers a p-adic exponent pair if $q = (k, \ell, r, \delta, (n_0, u_0, \kappa_0, \lambda_0))$ is a p-adic exponent datum for some $r \in \mathbf{J}_1(\mathbb{R})$, $\delta \in \mathbb{R}_0^+$, $n_0, u_0 \in \mathbf{J}_1(\mathbb{N})$, $\kappa_0 \in \mathbf{J}(\mathbb{N})$, $\lambda_0 \in \mathbf{J}(\mathbb{R}_0^+)$.

Every p-adic exponent datum q carries two kinds of quantities: the values of k, ℓ, r, and δ describe the upper bound (15), while $(n_0, u_0, \kappa_0, \lambda_0)$ can be thought of as 'initial conditions' that control the moduli p^n and the classes $\mathbf{F}(w, y, \kappa, \lambda, u)$ of phases f to which this estimate applies. We emphasize that, while the implied constant in (15) may be different from one p-adic exponent datum to another, it is, for a given datum q, absolute, and (15) holds uniformly across all other parameters, including p, y, w, κ, λ, n, u, f, M, and B.

Note that $(0, 1)$ is trivially a p-adic exponent pair, as $(0, 1, 0, 0, (\kappa + \iota' + 1, 1, 1 + \iota'(2), \rho_p))$ is a p-adic exponent datum. Further, note that the estimate on the right-hand side of (15) is an increasing function of B, and so, when applying this estimate, we may freely use an upper bound on B instead of its exact value. We also mention that any $\delta \in \mathbf{J}_1(\mathbb{R}_0^+)$ would suffice for applications; we ask for $\delta \in \mathbb{R}_0^+$ simply because this will be the case in all p-adic exponent data we construct.

We now describe a typical use of Definition 2. The estimate (15) holds uniformly in all parameters. In a typical application, p^n is the principal parameter, B is a certain power of p^n (depending on κ), and, upon choosing an allowable κ, the phase f and hence w, y, λ, u are all fixed. In a depth-aspect problem, the p-adic exponent pair (k, ℓ) controls the principal power dependence of our estimate on p^n, so, in practice, one first chooses the pair (k, ℓ) to optimize this dependence (for specific relative sizes of B and p^n and the desired type of result) and then considers the corresponding datum. For example, the pair $(\frac{1}{2}, \frac{1}{2})$, given by the p-adic exponent datum (36)

$$\omega_{1/2} = \Big(\tfrac{1}{2}, \tfrac{1}{2}, 0, 1, \big(\kappa + \iota' + 1 + \iota'(12), \max(\kappa - \lfloor\lambda\rfloor + \iota' + 1, 1), 1 + \iota'(4), \rho_p\big)\Big),$$

is well suited for very long sums (4), yielding in (15) the upper bound

$$\sum_{M<m\leqslant M+B} e\left(\frac{f(m)}{p^n}\right) \ll (p^{n-w-\kappa-\iota'})^{1/2} \log p^{n-w-\kappa-\iota'},$$

valid for all p^n and $f \in \mathbf{F}(w, y, \kappa, \lambda, u)$ with $\kappa \geqslant 1 + \iota'(4)$, $\lambda \geqslant \rho_p$, $n \geqslant w + \kappa + \iota' + 1 + \iota'(12)$, $u \geqslant \max(\kappa - \lfloor\lambda\rfloor + \iota' + 1, 1)$ and for all $M \in \mathbb{Z}$ and $0 < B \leqslant p^{n-w-\kappa-\iota'}$, which is uniform in B and can be seen as a variant of the Pólya–Vinogradov inequality. Section 6 contains a supply of explicit p-adic exponent data yielded by our method that one can choose from, as we do in the course of proving the sub-Weyl subconvex bound (60). Each of these p-adic exponent pairs arises from $(0, 1)$ by finitely many A- and B-processes, which in turn give rise to successive p-adic exponent data q. With each application, the quantities in q change and become fairly complicated (cf. the statement of Lemma 5), but they always take a dramatically simpler form away from finitely many p, such as for $p \notin \{2, 3\}$, $p \nmid y$ in the case of $\omega_{1/2}$. For such generic p, the original sum

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

is split as in (12) with $\kappa \geqslant \kappa_0$ (the latter being a constant for a fixed y and non-exceptional p), and, assuming that the (generally mild) 'separation' conditions $\lambda \geqslant \lambda_0$ and $u \geqslant u_0$ are met, the inner sum is estimated by (15). Since the p-adic exponent datum used ultimately applies to all p, this proof is then easily adjusted at the finitely many exceptional primes, without necessarily impacting the final result. We refer the reader to the proof of Theorem 6 and the discussion around (60) for a sample execution of this approach. Finally, all these calculations simplify even further if one is willing to simply treat constants in certain exponents of p (such as κ, n_0, u_0, r) as $\mathrm{O}(1)$, a shortcut that we do not take but that would be perfectly acceptable in a purely depth-aspect problem (when p is considered fixed).

We proceed to comment on why the conditions $0 \leqslant k \leqslant \frac{1}{2} \leqslant \ell \leqslant 1$ are included in Definition 2 and collect some additional useful information along the way. Consider $f(t) = p^{w-\kappa-\iota}(-y+1)^{-1}(1+p^{\kappa+\iota}t)^{-y+1}$ for $y \neq 1$, and $f(t) = p^{w-\kappa}\log_p(1+p^{\kappa}t)$ for $y=1$. Let

$$S(a) = \sum_{M<m\leqslant M+B} e\left(\frac{af(m)}{p^n}\right).$$

Note that, for $a \in \mathbb{Z}_p^\times$, $af(t) \in \mathbf{F}(w, y, \kappa, \infty, \infty, 1, a)$. We have that

$$\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} |S(a)|^2 = \sum_{M<m_1,m_2\leqslant M+B}\sum \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} e\left(\frac{a(f(m_1)-f(m_2))}{p^n}\right).$$

Recall from § 2 that $M_r\pi^0_{-y+1} \doteq |-y+1|_p r$ for all $r < r_p p^{-\iota}$ and $M_r\lambda \doteq r$ for all $r < r_p$. It follows easily that $\mathrm{ord}_p(f(m_1)-f(m_2)) = w + \mathrm{ord}_p(m_1-m_2)$ for every $m_1, m_2 \in \mathbb{Z}_p$. Therefore, if $B \leqslant p^{n-w-1}$ (and so certainly throughout the range $1 \leqslant B \leqslant p^{n-w-\kappa-\iota'}$), the inner sum vanishes unless $m_1 = m_2$, and so

$$\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} |S(a)|^2 = \varphi(p^n)\cdot B.$$

It follows that $|S(a)| \geqslant B^{1/2}$ for at least one $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, if an estimate of the form (15) is to hold for all B in some interval $I \subseteq [1, p^{n-w-\kappa-\iota'}]$, we must have

$$p^r\left(\frac{p^{n-w-\kappa-\iota'}}{B}\right)^k B^\ell(\log p^{n-w-\kappa-\iota'})^\delta \gg B^{1/2} \tag{16}$$

throughout the entire range $B \in I$. This conclusion ('no better than square root cancellation') will be used several times. In particular, with the choice $B=1$ and $n-w=n_0$, we have that $p^{r+(n_0-\kappa-\iota')k}(\log p^{n_0-\kappa-\iota'})^\delta \gg 1$. On the other hand, taking $B = p^{n-w-\kappa-\iota'}$, we see that the defining property (15) cannot hold with $\ell < \frac{1}{2}$.

Next, consider the behavior when $f(t)$ is as above, M and B are arbitrary but fixed, and $n \to \infty$. An elementary application of Dirichlet's box principle shows that we can find an $a \in (\mathbb{Z}/p^n\mathbb{Z})\backslash(p^n\mathbb{Z})$ such that

$$p^{-w}(af(M+1), af(M+2), \dots, af(M+B)) \in \mathbb{Q}_p^{/B/} + p^{n-w}\mathbb{Z}_p^B + ([0, p^{n-w}/\lfloor p^{n/B}\rfloor] \cap \mathbb{Z})^B,$$

where $\mathbb{Q}_p^{/B/} = \{(q, \dots, q) \in \mathbb{Q}_p^B : q \in \mathbb{Q}_p\}$. For this choice of a, we have that $|S(a)| = |B + \mathrm{O}(Bp^{-n/B})| \gg B$; on the other hand, $af(t) \in \mathbf{F}(\mathrm{ord}_p a + w, y, \kappa, \infty, \infty, 1, a|a|_p)$ and $\mathrm{ord}_p a \leqslant n - \lfloor n/B \rfloor$, and so $p^{n-(\mathrm{ord}_p a+w)-\kappa-\iota'} \geqslant p^{\lfloor n/B\rfloor-w-\kappa-\iota'}$ in (15). Taking $n \to \infty$, we see that no estimate of the form (15) can hold with $k < 0$.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

We have seen how, for two different reasons (not entirely unlike the heuristics behind large sieve estimates), every p-adic exponent datum that is to satisfy (15) must have $k \geqslant 0$ and $\ell \geqslant \frac{1}{2}$. Finally, there is no need to consider data with ($k \geqslant 0$ and) $\ell > 1$, since such an estimate would be worse than that provided by the trivial datum $(0,1,0,0,(\kappa+\iota'+1,1,1+\iota'(2),\rho_p))$ in most ranges. Similarly, there is no need to consider data with $k > \frac{1}{2}$ (and $\ell \geqslant \frac{1}{2}$) since the estimate obtained would be worse than that provided by the first non-trivial p-adic exponent datum (36).

The following Lemma 6, which states that the exponent datum condition may be verified (with a minimal loss) over either sharp or smooth cutoff functions, will be convenient. We will need several pieces of notation. Let $C_0^1(\mathbb{R})$ denote the set of continuously differentiable functions $h:\mathbb{R}\to\mathbb{C}$ such that $\lim_{|t|\to\infty}|t|^N(|h(t)|+|h'(t)|)=0$ for every $N\in\mathbb{N}$. For an $h\in C_0^1(\mathbb{R})$, denote

$$\|h\|_\star = \inf_{t_0\in\mathbb{R}} \int_{-\infty}^{\infty} (|t-t_0|+1)|h'(t)|\,dt. \tag{17}$$

Note that the quantity $\|h\|_\star$ is invariant under translations, that is, each of the translates $h_x(t)=h(t+x)$ $(x\in\mathbb{R})$ has $\|h_x\|_\star=\|h\|_\star$.

Let $\mathcal{C}=(\mathbf{C}_i)_{i\in I}$ be a family of classes $\mathbf{C}_i$ of power series in $\mathbb{Q}_p^\times\mathbf{I}_0(\mathbb{Z}_p)$, each of which is invariant under translations in the sense of Lemma 5, and let $0\leqslant k\leqslant\frac{1}{2}\leqslant\ell\leqslant 1$, $\delta\in\mathbb{N}_0$, $n_0:I\to\mathbb{N}_0$, $w:I\to\mathbb{Z}$, $r:I\to\mathbb{R}$. We say that a triple $\tau=(k,\ell,(r,w,n_0))$ satisfies the condition $H(\delta)$ if the estimate

$$\sum_{M<m\leqslant M+B} e\biggl(\frac{f(m)}{p^n}\biggr) \ll p^{r(i)}\biggl(\frac{p^{n-w(i)}}{B}\biggr)^k B^\ell(\log p^{n-w(i)})^\delta$$

holds, with a uniform implied constant depending only on τ and δ (so, explicitly *not* on $i\in I$), for every $i\in I$, every $f\in\mathbf{C}_i$, and every $n\geqslant n_0(i)$, $M\in\mathbb{Z}$, and $0<B\leqslant p^{n-w(i)}$. We will also write the above condition with r and w in place of $r(i)$ and $w(i)$ for brevity. We say that τ satisfies the condition $H(\delta)^{sq}$ if, additionally, the right-hand side of the above bound is $\gg B^{1/2}$ uniformly for every $i\in I$ and all $0<B\leqslant p^{n-w(i)}$.

As the example most important for us, a quintuple $q=(k,\ell,r,\delta,(n_0,u_0,\kappa_0,\lambda_0))$ is a p-adic exponent datum if and only if, for the collection $\mathcal{C}=\{\mathbf{F}(w,y,\kappa,\lambda,u): w\in\mathbb{Z}, y\in\mathbb{Q}^+, \kappa\geqslant\kappa_0, \lambda\geqslant\lambda_0, u\geqslant u_0\}$, the triple $(k,\ell,(r,w+\kappa+\iota'(y),n_0))$ satisfies the condition $H(\delta)$. We have already seen in (16) that, for these triples, $H(\delta)$ automatically implies $H(\delta)^{sq}$. Recall that each of the classes $\mathbf{F}(w,y,\kappa,\lambda,u)$ is invariant under translations by Lemma 5.

With the same notation, we say that τ satisfies the condition $H_{\mathrm{sm}}(\delta)$ if the estimate

$$\sum_{m\in\mathbb{Z}} e\biggl(\frac{f(m)}{p^n}\biggr)h\biggl(\frac{m}{B}\biggr) \ll c(h)\cdot p^{r(i)}\biggl(\frac{p^{n-w(i)}}{B}\biggr)^k B^\ell(\log p^{n-w(i)})^\delta$$

holds, with a uniform implied constant depending only on τ and δ and with $c(h)$ depending only on the cutoff function h, for every $i\in I$, every $f\in\mathbf{C}_i$, and every $n\geqslant n_0(i)$, $0<B\leqslant p^{n-w(i)}$, and $h\in C_0^1(\mathbb{R})$. We say that τ satisfies the condition $H_{\mathrm{sm}}^\sharp(\delta)$ if the above holds with

$$c(h)=\|h\|_\star.$$

The conditions $H_{\mathrm{sm}}(\delta)^{sq}$ and $H_{\mathrm{sm}}^\sharp(\delta)^{sq}$ are defined analogously. Finally, denote

$$\delta_{1/2}=\begin{cases}1, & (k,\ell)=(\frac{1}{2},\frac{1}{2}),\\ 0, & \text{else};\end{cases}\qquad \delta_{01}=\begin{cases}1, & (k,\ell)=(0,1),\\ 0, & \text{else}.\end{cases}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Lemma 6. *Let $\mathcal{C} = (\mathbf{C}_i)_{i\in I}$ be a family of classes $\mathbf{C}_i$ of power series in $\mathbb{Q}_p^\times \mathbf{I}_0(\mathbb{Z}_p)$, each of which is invariant under translations in the sense of Lemma 5. Then, for every triple $\tau = (k, \ell, (r, w, n_0))$, $0 \leqslant k \leqslant \frac{1}{2} \leqslant \ell \leqslant 1$, $n_0 : I \to \mathbb{N}_0$, $w : I \to \mathbb{Z}$, $r : I \to \mathbb{R}$, and for every $\delta \in \mathbb{N}_0$, we have the following implications:*

$$H(\delta) \implies H^\sharp_{\mathrm{sm}}(\delta) \implies H_{\mathrm{sm}}(\delta), \quad H_{\mathrm{sm}}(\delta)^{sq} \implies H(\delta + \delta_{1/2})^{sq}.$$

Proof. Suppose that $H_{\mathrm{sm}}(\delta)^{sq}$ holds. Fix a smooth, compactly supported cutoff function $\phi \in C_c^\infty(\mathbb{R})$ with the following properties:

- $0 \leqslant \phi(x) \leqslant 1$ for all x;
- $\phi(x) = 0$ for all $x \notin [0, \frac{3}{4}]$;
- $\phi(x) + \phi((1+x)/2) = 1$ for all $0 \leqslant x \leqslant \frac{1}{2}$.

Using ϕ, we define smooth, compactly supported cutoff functions $\phi_i \in C_c^\infty(\mathbb{R})$ $(i \in \mathbb{N}_0)$ as follows: let

$$\phi_0(x) = \begin{cases} 1 - \phi(|x|), & |x| \leqslant \frac{1}{2}, \\ 0, & |x| > \frac{1}{2}, \end{cases}$$

and, for $i \geqslant 1$, let $\phi_i(x) = \phi(2^{i-1}|x| - (2^{i-1} - 1))$. Then, for all $i \geqslant 1$, $0 \leqslant \phi_i(x) \leqslant 1$ for all x, $\phi_i(x) = 0$ for all x with $|x| \notin [1 - 1/2^{i-1}, 1 - 1/2^{i+1}]$, and $\phi_{i-1}(x) + \phi_i(x) = 1$ for all x with $|x| \in [1 - 1/2^{i-1}, 1 - 1/2^i]$. Therefore, the cutoff function $\tilde{\phi}_i(x) = \sum_{j=0}^{i} \phi_j(x)$ satisfies:

- $0 \leqslant \tilde{\phi}_i(x) \leqslant 1$ for all x;
- $\tilde{\phi}_i(x) = 0$ for all x with $|x| \geqslant 1 - 1/2^{i+1}$;
- $\tilde{\phi}_i(x) = 1$ for all x with $|x| \leqslant 1 - 1/2^i$.

Now, let $f \in \mathbf{C}_i$, and let $n \geqslant n_0(i)$, $M \in \mathbb{Z}$, and $0 < B \leqslant p^{n-w(i)}$ be given. Since the class $\mathbf{C}_i$ is closed under translations, we have that $f_{M'} \in \mathbf{C}_i$ for every $M' \in \mathbb{Z}$. Write $B = 2^\beta C + B_1$, where $0 \leqslant B_1 < 2^\beta$, and $\beta \in \mathbb{N}$ will be suitably chosen later. Then,

$$\begin{aligned}
\sum_{M < m \leqslant M+B} e\left(\frac{f(m)}{p^n}\right) &= \sum_{m\in\mathbb{Z}} e\left(\frac{f(m)}{p^n}\right) \tilde{\phi}_{\beta-1}\left(\frac{m - M - 2^{\beta-1}C}{2^{\beta-1}C}\right) + \mathrm{O}(B_1 + C) \\
&= \sum_{m\in\mathbb{Z}} e\left(\frac{f_{M+2^{\beta-1}C}(m)}{p^n}\right) \phi_0\left(\frac{m}{2^{\beta-1}C}\right) \\
&\quad + \sum_{m\in\mathbb{Z}} \sum_{j=1}^{\beta-1} e\left(\frac{f_{M+2^{\beta-1}C}(m)}{p^n}\right) \phi\left(\frac{|m| - (2^{\beta-1} - 2^{\beta-j})C}{2^{\beta-j}C}\right) + \mathrm{O}\left(\frac{B}{2^\beta} + 2^\beta\right) \\
&= \sum_{m\in\mathbb{Z}} e\left(\frac{f_{M+2^{\beta-1}C}(m)}{p^n}\right) \phi_0\left(\frac{m}{2^{\beta-1}C}\right) + \sum_{j=1}^{\beta-1} \sum_{m\in\mathbb{Z}} e\left(\frac{f_{M+(2^\beta - 2^{\beta-j})C}(m)}{p^n}\right) \phi\left(\frac{m}{2^{\beta-j}C}\right) \\
&\quad + \sum_{j=1}^{\beta-1} \sum_{m\in\mathbb{Z}} e\left(\frac{f_{M+2^{\beta-j}C}(m)}{p^n}\right) \phi\left(-\frac{m}{2^{\beta-j}C}\right) + \mathrm{O}\left(\frac{B}{2^\beta} + 2^\beta\right).
\end{aligned}$$

Since each translate of f belongs to $\mathbf{C}_i$ and $2^{\beta-j}C \leqslant B \leqslant p^{n-w(i)}$, we may apply the condition $H_{\mathrm{sm}}(\delta)$ to see that the sum of the first three summands is at most

$$\begin{aligned}
&\ll p^r \left(\frac{p^{n-w}}{2^{\beta-1}C}\right)^k (2^{\beta-1}C)^\ell (\log p^{n-w})^\delta + \sum_{j=1}^{\beta-1} p^r \left(\frac{p^{n-w}}{2^{\beta-j}C}\right)^k (2^{\beta-j}C)^\ell (\log p^{n-w})^\delta \\
&\ll p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^\delta (1 + \delta_{1/2}\beta),
\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

recalling that $\ell \geqslant k$, with $\ell > k$ unless $k = \ell = \frac{1}{2}$. Finally, we choose β so that $2^\beta \asymp B^{1/2}$; then $\beta \asymp \log B \ll \log p^{n-w}$. We thus obtain

$$\sum_{M<m\leqslant M+B} e\left(\frac{f(m)}{p^n}\right) \ll p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^{\delta+\delta_{1/2}} + B^{1/2}$$
$$\ll p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^{\delta+\delta_{1/2}},$$

as desired, since the first term dominates in light of the condition $H(\delta)^{sq}$. This shows that τ satisfies $H(\delta+\delta_{1/2})^{sq}$, proving the implication $H_{\mathrm{sm}}(\delta)^{sq} \implies H(\delta+\delta_{1/2})^{sq}$.

Suppose that $H(\delta)$ holds. Let $h \in C_0^1(\mathbb{R})$ be arbitrary, and let $f \in \mathbf{C}_i$, $n \geqslant n_0(i)$, $M \in \mathbb{Z}$, and $0 < B \leqslant p^{n-w(i)}$ be given. Fix a $t_0 \in \mathbb{R}$, and let

$$\tilde{S}(t) = \begin{cases} \displaystyle\sum_{t_0 B \leqslant m \leqslant t} e(f(m)/p^n), & t > t_0 B, \\ 0, & t = t_0 B, \\ \displaystyle -\sum_{t \leqslant m < t_0 B} e(f(m)/p^n), & t < t_0 B. \end{cases}$$

We can break the sum defining $\tilde{S}(t)$ into at most $|t - t_0 B|/B + 1$ blocks of size at most B. Using the condition $H(\delta)$ to estimate each of the blocks, we find that

$$\tilde{S}(t) \ll \left(\frac{|t-t_0 B|}{B} + 1\right) \cdot p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^\delta.$$

Using summation by parts, we estimate

$$\sum_{m\in\mathbb{Z}} e\left(\frac{f(m)}{p^n}\right) h\left(\frac{m}{B}\right) = \int_{\mathbb{R}} h\left(\frac{t}{B}\right) d\tilde{S}(t) = -\frac{1}{B}\int_{\mathbb{R}} \tilde{S}(t) h'\left(\frac{t}{B}\right) dt$$
$$\ll \frac{1}{B}\int_{\mathbb{R}} \left(\frac{|t-t_0 B|}{B} + 1\right) \left|h'\left(\frac{t}{B}\right)\right| dt \cdot p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^\delta$$
$$= \int_{\mathbb{R}} (|t-t_0|+1)|h'(t)|\, dt \cdot p^r \left(\frac{p^{n-w}}{B}\right)^k B^\ell (\log p^{n-w})^\delta.$$

This estimate is valid, with a uniform implied constant, for every $t_0 \in \mathbb{R}$. Taking the infimum of the right-hand side over all $t_0 \in \mathbb{R}$, we find that $H_{\mathrm{sm}}^\sharp(\delta)$ holds. This proves that $H(\delta) \implies H_{\mathrm{sm}}^\sharp(\delta)$ and completes the entire proof, since $H_{\mathrm{sm}}^\sharp(\delta) \implies H_{\mathrm{sm}}(\delta)$ is trivial. □

4. *B*-process

We are now ready for the proof of the B-process, which relies on Poisson summation to replace an exponential sum with a short dual sum and on the method of stationary phase and the implicit function theorem to evaluate the dual sum. Although historical precedent would have us presenting the A-process first, we find that this order of exposition allows us to obtain tighter estimates.

The following lemma is a version of the p-adic analogue of the method of stationary phase and the starting point for the analysis of the Fourier transform $\hat{\mathbf{e}}_f(s)$ (defined below in (23)).

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

A variant of this method (as well as of Lemma 8) can be found in [IK04, §§ 3.5 and 12.3], but we include it for completeness as Lemma 7 and fine-tune the statement and proof to our particular situation.

Lemma 7 (Method of stationary phase). *Let p be a prime, let $f \in \mathbb{Q}_p^\times \mathbf{I}(\mathbb{Z}_p)$ be such that $f' \in (\mathbb{Z}_p + p^\mu t\mathbf{I}_0(\mathbb{Z}_p))$ for some $\mu \in \mathbb{N}_0$, and let $n, j \in \mathbb{N}$ be such that $j \leqslant n-1$ and*

$$2(n-j)+\mu \geqslant n+\iota'(2).$$

Then

$$\sum_{m \bmod p^n} e\biggl(\frac{f(m)}{p^n}\biggr) = \sum_{\substack{m \bmod p^n\\ f'(m)\equiv 0 \bmod p^j}} e\biggl(\frac{f(m)}{p^n}\biggr).$$

Proof. We can write

$$S = \sum_{m \bmod p^n} e\biggl(\frac{f(m)}{p^n}\biggr) = p^{-j}\sum_{m \bmod p^n}\sum_{k \bmod p^j} e\biggl(\frac{f(m+p^{n-j}k)}{p^n}\biggr).$$

We can use Taylor's expansion (9) to write

$$f(m+p^{n-j}k) = f(m)+p^{n-j}f'(m)k+\sum_{r=2}^{\infty}\frac{1}{r!}p^{r(n-j)}f^{(r)}(m)k^r.$$

We claim that, under our conditions, all terms in the rightmost sum are divisible by p^n. Indeed, writing $f'(t) = b_0+\sum_{k=1}^{\infty}p^\mu b_k t^k$, we have $f^{(r)}(t) = p^\mu\sum_{k=0}^{\infty}b_{k+r-1}(k+r-1)_{r-1}t^k$, so that

$$\operatorname{ord}_p\biggl(\frac{1}{r!}p^{r(n-j)}f^{(r)}(m)k^r\biggr) \geqslant (2(n-j)+\mu)+((r-2)(n-j)-\operatorname{ord}_p r).$$

That the right-hand side is divisible by p^n is now immediate for $r=2$ and $r=3$; for $r \geqslant 4$, the claim follows from $p^{r-2} \geqslant 2^{r-2} \geqslant r$.

It follows that

$$S = p^{-j}\sum_{m \bmod p^n} e\biggl(\frac{f(m)}{p^n}\biggr)\sum_{k \bmod p^j} e\biggl(\frac{f'(m)k}{p^j}\biggr).$$

The inner sum equals p^j if $f'(m) \equiv 0 \pmod{p^j}$ and vanishes otherwise. This gives the desired equality. □

The method of stationary phase, in some variation of that presented in Lemma 7, goes back at least to Salié [Sal32]. A simple instance of this method is the classical evaluation of the Gaussian sum, which we record for reference. We will in fact only use the most elementary case $n \in \{0,1\}$ of this lemma ($n \in \{2,3\}$ for $p=2$).

Lemma 8 (Gauss). *For a prime p, $n \in \mathbb{N}$, and $a \in \mathbb{Z}$ with $p \nmid a$, let*

$$\tau_a(p^n) = \sum_{m \bmod p^n} e\biggl(\frac{am^2}{p^n}\biggr).$$

Then

$$\tau_a(p^n) = p^{(n+\iota'(2))/2}\epsilon(a,p^n),$$

where $\epsilon(a,p^n)$ is a unit factor given explicitly as

$$\epsilon(a,p^n)=\begin{cases}1, & p\neq 2,\ 2\mid n,\\ \left(\dfrac{a}{p}\right), & p\equiv 1 \bmod 4,\ 2\nmid n,\\ \left(\dfrac{a}{p}\right)i, & p\equiv 3 \bmod 4,\ 2\nmid n;\end{cases}\qquad \epsilon(a,2^n)=\begin{cases}0, & p=2,\ n=1,\\ \dfrac{1+i^a}{\sqrt{2}}, & 2\mid n,\ n\geqslant 2,\\ \left(\dfrac{2}{a}\right)\dfrac{1+i^a}{\sqrt{2}}, & 2\nmid n,\ n\geqslant 3.\end{cases}$$

Proof. This is adapted to our notation from [BEW98, Theorems 1.5.1 and 1.5.2 and Proposition 1.5.3, p. 26]. □

In the following lemma, we develop the p-adic implicit function theorem which we will use to characterize the critical points in the exponential sum (23).

Lemma 9 (Implicit function theorem). *Let $f\in\mathbf{F}(w,y,\kappa,\lambda,u,\omega,\omega')$, and assume that*

$$u>\kappa-\lfloor\lambda\rfloor+\iota',\qquad \tilde{\lambda}=\min(\kappa-\rho_p(y),\lambda)>0.$$

Let $\tilde{g}_0=f'(0)p^{-w}-\omega'\in\mathbb{Z}_p$. Then there is a power series $\tilde{f}\in\mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$ such that

$$\tilde{f}(t)=p^{-\iota-\kappa}\omega^{-1}(1+p^{\iota'+\kappa}t)^{-1/y}-p^{-\iota-\kappa}\omega^{-1}+p^{u+\lfloor\lambda\rfloor-\kappa-\iota'}\tilde{g}(t)\tag{18}$$

for some $\tilde{g}\in\mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$ and such that

$$f'(\tilde{f}(t))p^{-w}=\tilde{g}_0+\omega'(1+p^{\iota'+\kappa}t).\tag{19}$$

Moreover, for $j\geqslant\iota'+\kappa$ and $s'\in\mathbb{Z}_p$, the congruence

$$f'(m)p^{-w}\equiv s'\pmod{p^j}$$

has solutions $m\in\mathbb{Z}_p$ if and only if $s'\equiv\tilde{g}_0+\omega'\pmod{p^{\iota'+\kappa}}$. In this case, writing $j'=j-\iota'-\kappa$ and $s'=\tilde{g}_0+\omega'(1+p^{\iota'+\kappa}t)$ for some $t\in\mathbb{Z}_p$ unique modulo $p^{j'}$, the above congruence holds if and only if

$$m\equiv\tilde{f}(t)\pmod{p^{j'}}.$$

Proof. Recall that

$$f'(t)p^{-w}=\omega'(1+p^{\iota+\kappa}\omega t)^{-y}+\gamma_0+p^u g(t),$$

where $g\in\mathbf{I}_0[\lambda](\mathbb{Z}_p)$. We can write

$$\gamma_0+p^u g(t)=\gamma_0+p^u g(0)+p^{u+\lfloor\lambda\rfloor-\kappa}p^{\kappa}tg_1(t)=\tilde{g}_0+p^{u'+\kappa}tg_1(t),$$

where $u'=u+\lfloor\lambda\rfloor-\kappa>\iota'$ and $g_1\in\mathbf{I}_0[\lambda](\mathbb{Z}_p)$. We will now construct a power series $\tilde{f}$ such that

$$\begin{aligned}f'(\tilde{f}(t))p^{-w}&=\tilde{g}_0+\omega'(1+p^{\iota+\kappa}\omega\tilde{f}(t))^{-y}+p^{u'+\kappa}\tilde{f}(t)g_1(\tilde{f}(t))\\&=\tilde{g}_0+\omega'(1+p^{\iota'+\kappa}t),\end{aligned}$$

with all numerical substitutions allowed for $t\in\mathbb{Z}_p$.

Let $\omega''=\omega'^{-1}$. Define a sequence of power series $\tilde{f}_k$ as follows:

$$\begin{aligned}\tilde{f}_0(t)&=\frac{(1+p^{\iota'+\kappa}t)^{-1/y}-1}{p^{\iota+\kappa}\omega},\\ \tilde{f}_{k+1}(t)&=\frac{\left(1+p^{\iota'+\kappa}t-p^{u'+\kappa}\omega''\tilde{f}_k(t)g_1(\tilde{f}_k(t))\right)^{-1/y}-1}{p^{\iota+\kappa}\omega}\quad(k\geqslant 0).\end{aligned}\tag{20}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Let $\rho_k = (k+1)(u'-\iota')$. We claim that $\tilde{f}_k$ is a sequence of power series with

$$\tilde{f}_0 \in \mathbf{I}_0^n[\kappa - \rho_p(y)](\mathbb{Z}_p) \quad \text{and} \quad \tilde{f}_k \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)\,(k \geqslant 1)$$

such that

$$\tilde{f}_{k+1} = \tilde{f}_k + p^{\rho_k}\tilde{F}_k \tag{21}$$

for some $\tilde{F}_k \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$.

We prove this claim by induction on k. For $k=0$, $\pi_{[\iota'+\kappa]}^{-1/y} \in \mathbf{I}_{\iota+\kappa}^1[\kappa - \rho_p(y)](\mathbb{Z}_p)$ implies that $\tilde{f}_0 \in \mathbf{I}_0^n[\kappa - \rho_p(y)](\mathbb{Z}_p)$. Then $g_1(\tilde{f}_0(t)) \in \mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$ and $\omega''\tilde{f}_0(t)g_1(\tilde{f}_0(t)) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. Applying Lemma 3,

$$\big(1 + p^{\iota'+\kappa}t - p^{(u'+\kappa-\iota')+\iota'} \cdot \omega''\tilde{f}_0(t)g_1(\tilde{f}_0(t))\big)^{-1/y} = (1+p^{\iota'+\kappa}t)^{-1/y} + p^{u'+\kappa-\iota'+\iota}\tilde{b}(t)$$

for some $\tilde{b}(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. We see that we can take $\tilde{F}_0(t) = \omega^{-1}\tilde{b}(t)$ in (21).

Assume that (21) holds for some $k \in \mathbb{N}_0$; then clearly $\tilde{f}_{k+1} \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. Moreover, according to Lemma 4, we can write

$$g_1(\tilde{f}_{k+1}(t)) = g_1(\tilde{f}_k(t) + p^{\rho_k}\tilde{F}_k(t)) = g_1(\tilde{f}_k(t)) + p^{\rho_k}g_2(t)$$

for some $g_2 \in \mathbf{I}_{0,1}^n[\tilde{\lambda}](\mathbb{Z}_p)$. We can rearrange

$$\begin{aligned}&\big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_{k+1}(t)g_1(\tilde{f}_{k+1}(t))\big)^{-1/y}\\ &\quad = \Big[\big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_k(t)g_1(\tilde{f}_k(t))\big)\\ &\qquad\quad - p^{(u'+\kappa+\rho_k-\iota')+\iota'}\omega''\big(\tilde{F}_k(t)g_1(\tilde{f}_k(t)) + \tilde{f}_{k+1}(t)g_2(t)\big)\Big]^{-1/y}.\end{aligned}$$

Since $g_1(\tilde{f}_k(t)) \in \mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$, we have that

$$\begin{gathered}1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_k(t)g_1(\tilde{f}_k(t)) \in \mathbf{I}_{\iota'+\kappa}^1[\tilde{\lambda}](\mathbb{Z}_p),\\ \tilde{F}_k(t)g_1(\tilde{f}_k(t)) + \tilde{f}_{k+1}(t)g_2(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p).\end{gathered}$$

Applying Lemma 3, we conclude that

$$\begin{aligned}&\big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_{k+1}(t)g_1(\tilde{f}_{k+1}(t))\big)^{-1/y}\\ &\quad = \big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_k(t)g_1(\tilde{f}_k(t))\big)^{-1/y} + p^{u'+\kappa+\rho_k-\iota'+\iota}\tilde{b}_k(t)\end{aligned}$$

for some $\tilde{b}_k(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. We see that we can take $\tilde{F}_{k+1}(t) = \omega^{-1}\tilde{b}_k(t)$ in (21), since $\rho_{k+1} = u' - \iota' + \rho_k$. This completes the inductive proof of (21).

We now define

$$\tilde{g}(t) = \sum_{k=0}^{\infty} p^{\rho_k - \rho_0}\tilde{F}_k(t), \quad \tilde{f}(t) = \tilde{f}_0(t) + p^{u'-\iota'}\tilde{g}(t). \tag{22}$$

In light of $u' > \iota'$, it is clear that the series converges and that $\tilde{g}(t), \tilde{f}(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. Moreover, for $r = |t|_p < p^{\tilde{\lambda}}$, we have (22) also as equalities of values, and $M_r\tilde{f} \doteq r$. We claim that $\tilde{f}$ has all desired properties; it is now immediate that (18) holds.

Define $\check{F}_k = \sum_{\ell=k}^{\infty} p^{\rho_\ell - \rho_k}\tilde{F}_\ell$. Then

$$\tilde{f}_k = \tilde{f} - p^{\rho_k}\check{F}_k$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

and $\check{F}_k \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. The second equation in (20) is equivalent to

$$1 + p^{\iota+\kappa}\omega\tilde{f}_{k+1}(t) = \big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}_k(t)g_1(\tilde{f}_k(t))\big)^{-1/y}.$$

Applying Lemma 3 and Lemma 4 as above (with $\tilde{f}_k(t)$, $\tilde{f}(t)$, and $-\check{F}_k(t)$ in place of $\tilde{f}_{k+1}(t)$, $\tilde{f}_k(t)$, and $\tilde{F}_k(t)$, respectively), we can rewrite the right-hand side of this equality to see that

$$\begin{aligned}1 + p^{\iota+\kappa}\omega\tilde{f}(t) &= 1 + p^{\iota+\kappa}\omega\tilde{f}_{k+1}(t) + p^{\rho_{k+1}+\iota+\kappa}\omega\check{F}_{k+1}(t)\\ &= \big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}(t)g_1(\tilde{f}(t))\big)^{-1/y} + p^{\rho_{k+1}+\iota+\kappa}(\check{b}_k(t) + \omega\check{F}_{k+1}(t))\end{aligned}$$

for some $\check{b}_k(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. For k large enough, this is possible only if

$$1 + p^{\iota+\kappa}\omega\tilde{f}(t) = \big(1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}(t)g_1(\tilde{f}(t))\big)^{-1/y}.$$

This equality of series in $\mathbf{I}^1_{\iota+\kappa}(\mathbb{Z}_p)$ is equivalent to

$$\begin{gathered}(1 + p^{\iota+\kappa}\omega\tilde{f}(t))^{-y} = 1 + p^{\iota'+\kappa}t - p^{u'+\kappa}\omega''\tilde{f}(t)g_1(\tilde{f}(t)),\\ f'(\tilde{f}(t)) = p^{w}\tilde{g}_0 + p^{w}\omega'(1 + p^{\iota'+\kappa}t).\end{gathered}$$

According to Lemma 2, the numerical substitution of $\tilde{f}(t)$ in f' is justified for all $|t|_p < p^{\tilde{\lambda}}$.

We pass to characterizing the solutions to the congruence $f'(m)p^{-w} \equiv s' \pmod{p^j}$, that is,

$$\tilde{g}_0 + \omega'(1 + p^{\iota+\kappa}\omega m)^{-y} + p^{u'+\kappa}mg_1(m) \equiv s' \pmod{p^j},$$

where $j \geqslant \iota' + \kappa$. Recalling that $\pi^{-y}_{[\iota+\kappa]} \in \mathbf{I}^1_{\iota'+\kappa}(\mathbb{Z}_p)$, it is seen that solutions m exist only if $s' = \tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa}t)$ for some $t \in \mathbb{Z}_p$, in which case the above congruence becomes equivalent to

$$f'(m)p^{-w} \equiv f'(\tilde{f}(t))p^{-w} \pmod{p^j}.$$

In light of $u' > \iota'$, the series $f'(t)p^{-w} = \sum_{k=0}^{\infty} a_k^{\sharp}t^k$ satisfies the conditions of Lemma 1 for every $r < p^{\tilde{\lambda}}$, with $|a_1^{\sharp}|_p = p^{-(\iota'+\kappa)}$. In particular, an $m \in \mathbb{Z}_p$ is a solution of the above congruence if and only if

$$m \equiv \tilde{f}(t) \pmod{p^{j'}},$$

as announced. □

Lemma 10. *Let $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$, and assume that*

$$\min(n - w, u + \lfloor\lambda\rfloor) > \kappa + \iota', \quad \tilde{\lambda} = \min(\kappa - \rho_p(y), \lambda) > 0.$$

Let

$$\hat{\mathbf{e}}_f(s) = \sum_{m \bmod p^{n-w}} e\bigg(\frac{f(m)p^{-w} - sm}{p^{n-w}}\bigg), \tag{23}$$

and let $\varepsilon_\lambda = \lfloor\lambda\rfloor - \lceil\tilde{\lambda}\rceil$. Then, assuming additional conditions listed below if $p \in \{2, 3\}$, there exists a power series $\breve{f} \in \mathbf{F}(\breve{w}, y^{-1}, \kappa, \tilde{\lambda}, \breve{u}, 1, -\omega'\omega^{-1})$ with $\breve{f}' \in p^{w+\iota'+\kappa}\mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$, where

$$\breve{w} = w + \mathrm{ord}_p y, \quad \breve{u} = u + \varepsilon_\lambda - \mathrm{ord}_p y,$$

and an $\epsilon \in \mathbb{C}$, $|\epsilon| = 1$ such that

$$\hat{\mathbf{e}}_f(s) = \hat{\mathbf{e}}_f(\tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa}t)) = \epsilon p^{(n-w+\iota'+\kappa)/2} e\bigg(\frac{\breve{f}(t)}{p^n}\bigg)$$

if $s = \tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t)$ for some $t \in \mathbb{Z}_p$, and $\hat{\mathbf{e}}_f(s) = 0$ otherwise. The unit ϵ depends only on ω, ω', y, p, the parity of $n - w + \iota' + \kappa - \iota'(2)$, and, for $p = 2$ only, on $p^{u-\kappa-\iota'} g'(0)$; in particular, it is independent of s.

In the case $p \in \{2, 3\}$, we must make additional assumptions. Let $\nu \in \{0, 1\}$ be the residue of $n - w + \iota' + \kappa - \iota'(2)$ modulo 2, $n_1 = n - w - \kappa - \iota' - 1$, and $\kappa + \iota'(y + 1) = \nu + 2\iota'(2) + \kappa_1$. Then assume additionally that

$$\kappa + \iota'(y + 1) \geqslant \nu + 2\iota'(2), \quad n_1 \geqslant 2\iota'(2)\nu, \quad n_1 + \kappa_1 \geqslant \iota'(3).$$

These assumptions are automatically satisfied if $\kappa \geqslant 1 + \iota'(4)$ and $n - w > \iota' + \kappa + \iota'(12)$, or if $\kappa \geqslant 1 + \iota'(12)$ and $n - w > \iota' + \kappa + \iota'(4)$.

Proof. In light of $\pi^{-y}_{[\iota+\kappa]} \in \mathbf{I}^1_{\iota'+\kappa}(\mathbb{Z}_p)$ and $u + \lceil \lambda \rceil > \iota' + \kappa$, we have that $p^{-w} f'(t) \in \mathbb{Z}_p + p^{\mu} t \mathbf{I}_0(\mathbb{Z}_p)$, with $\mu = \iota' + \kappa$. Write

$$n - w + \iota' + \kappa - \iota'(2) = 2j + \nu,$$

with $j \in \mathbb{N}$ and $\nu \in \{0, 1\}$. Note that, under our assumptions,

$$\iota' + \kappa \leqslant j < n - w,$$

as well as

$$2(n - w - j) + (\iota' + \kappa) \geqslant n - w + \iota'(2).$$

This shows that all conditions are satisfied for an application of Lemma 7 to (23). According to Lemma 7, the summation in (23) can be restricted to indices m for which

$$f'(m) p^{-w} \equiv s \pmod{p^j}. \tag{24}$$

All conditions are also satisfied for an application of Lemma 9. Let $\tilde{f}$ be the power series whose existence is established there, and let $j' = j - \iota' - \kappa$. According to Lemma 9, we have that indices m satisfying (24) exist if and only if

$$s = \tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t)$$

for some $t \in \mathbb{Z}_p$ (with congruence classes of $s \bmod p^j$ for which (24) is solvable in one-to-one correspondence with congruence classes of $t \bmod p^{j'}$), in which case an $m \bmod p^{n-w}$ satisfies (24) if and only if $m = \tilde{f}(t) + p^{j'} q$ for some $q \bmod p^{n-w-j'}$.

Consider two functions $\breve{f}(t, q) : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ and $\breve{f}(t) : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by their pointwise values as

$$\begin{gathered}\breve{f}(t, q) = f(\tilde{f}(t) + p^{j'} q) - p^w(\tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t))(\tilde{f}(t) + p^{j'} q),\\ \breve{f}(t) = \breve{f}(t, 0) = f(\tilde{f}(t)) - p^w(\tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t))\tilde{f}(t).\end{gathered} \tag{25}$$

With this notation, we have proved so far that

$$\hat{\mathbf{e}}_f(s) = \hat{\mathbf{e}}_f(\tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t)) = \sum_{q \bmod p^{n-w-j'}} e\left(\frac{\breve{f}(t, q)}{p^n}\right) \tag{26}$$

if $s = \tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t)$ for some $t \in \mathbb{Z}_p$, and $\hat{\mathbf{e}}_f(s) = 0$ otherwise.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Using the Taylor expansion (9), we obtain, for every $t, q \in \mathbb{Z}_p$, an equality of values

$$\begin{aligned}\breve{f}(t,q) &= \sum_{r=0}^{\infty} \frac{f^{(r)}(\tilde{f}(t))}{r!}(p^{j'}q)^r - p^w(\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t))(\tilde{f}(t)+p^{j'}q) \\ &= \breve{f}(t) + \big[f'(\tilde{f}(t)) - p^w(\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t))\big]p^{j'}q + \sum_{r=2}^{\infty} \frac{f^{(r)}(\tilde{f}(t))}{r!}p^{rj'}q^r \\ &= \breve{f}(t) + \frac{1}{2}f''(\tilde{f}(t))p^{2j'}q^2 + \sum_{r=3}^{\infty} \frac{f^{(r)}(\tilde{f}(t))}{r!}p^{rj'}q^r,\end{aligned}$$

recalling the defining property (19) of $\tilde{f}$. Note that

$$f^{(r)}(t)p^{-w} = \omega'(-y)_{r-1}(p^{\iota+\kappa}\omega)^{r-1}(1+p^{\iota+\kappa}\omega t)^{-y-r+1} + p^u g^{(r-1)}(t). \tag{27}$$

Since $u + \lceil\lambda\rceil > \iota' + \kappa$, we have that

$$\begin{aligned}\nu_2 := \operatorname{ord}_p(\tfrac{1}{2}f''(\tilde{f}(t))p^{2j'}) &= 2j' + w + \kappa + \iota' - \iota'(2) \\ &= 2j + w - \kappa - \iota' - \iota'(2) \\ &= n - \nu - 2\iota'(2).\end{aligned}$$

We now consider the remaining infinite sum E in the Taylor expansion for $\breve{f}(t,q)$ and set conditions under which $\operatorname{ord}_p E \geqslant n$ holds. We have that, for $r \geqslant 3$,

$$\begin{aligned}&\operatorname{ord}_p\bigg(\frac{f^{(r)}(\tilde{f}(t))}{r!}p^{rj'}q^r\bigg) - w \\ &\quad\geqslant \min\big((r-1)\kappa + rj' + \iota' + \iota'(y+1) - \operatorname{ord}_p r!, u + \lceil(r-1)\lambda\rceil + rj' - \operatorname{ord}_p r\big).\end{aligned}$$

We now carefully (and tediously) examine each of the two terms in the above expression, which we denote by $\nu_{r,1}(p)$ and $\nu_{r,2}(p)$. (This examination is not pleasant. At the first reading, the reader is encouraged to skip it or consider the case $p \notin \{2,3\}$, for which we will see that no further assumptions are needed.)

Denote temporarily $\iota'' = \iota'(y+1)$. Using that $\operatorname{ord}_p r! \leqslant (r-1)/(p-1)$, we have that, for $r \geqslant 3$,

$$\begin{aligned}\nu_{r,1}(p) &:= (r-1)\kappa + rj' + \iota' + \iota'' - \operatorname{ord}_p r! \\ &\geqslant \lceil(r-1)(\kappa + j' - \rho_p)\rceil + j' + \iota' + \iota'' \\ &\geqslant \lceil 2\kappa + 3j' - 2\rho_p\rceil + \iota' + \iota'' \\ &= 2\kappa + 3j' + \iota' + \iota'' - \iota'(12).\end{aligned}$$

In fact, we have the slightly stronger estimate

$$\nu_{r,1}(p) \geqslant 2\kappa + 3j' + \iota' + \iota'' - \iota'(6).$$

Namely, when $p = 2$, this follows by direct verification for $r = 3$ and from $\nu_{r,1}(2) \geqslant \lceil 3\kappa + 4j' - 3\rho_2\rceil + \iota' + \iota''$ and $\kappa \geqslant 2$ for $r \geqslant 4$.

On the other hand,

$$\begin{aligned}\nu_{r,2}(p) &:= u + \lceil(r-1)\lambda\rceil + rj' - \operatorname{ord}_p r \\ &\geqslant u + rj' + \lceil(r-1)(\lambda - \rho_p)\rceil \\ &\geqslant u + 3j' + \lceil 2(\lambda - \rho_p)\rceil.\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

In fact, recalling also that $\lambda \in \mathbb{N}$ for $p = 2$, we have $\nu_{3,2}(2) = u + 3j' + 2\lambda$ and $\nu_{4,2}(2) = u + 4j' + 3\lambda - 2$; since $\operatorname{ord}_2 r \leqslant r - 5$ for $r \geqslant 5$, we also have $\nu_{r,2}(2) \geqslant u + 5j' + 4\lambda > \nu_{3,2}(2)$ for all $r \geqslant 5$, and so

$$\nu_{r,2}(p) \geqslant u + 3j' + \hat{\nu}_2, \quad \hat{\nu}_2 := \begin{cases} \lceil 2(\lambda - \rho_p) \rceil, & p \geqslant 3, \\ \min(2\lambda, j' + 3\lambda - 2), & p = 2. \end{cases}$$

Summing up, we have

$$\operatorname{ord}_p E \geqslant \nu_E := \min\bigl(2\kappa + 3j' + \iota' + \iota'' - \iota'(6), u + 3j' + \hat{\nu}_2\bigr) + w.$$

This gives us two conditions that need to be met for $\nu_E \geqslant n$. The first is that

$$\begin{aligned} &2\kappa + 3j' + \iota' + \iota'' - \iota'(6) \\ &\quad = 3j - 3\iota' - \kappa + \iota' + \iota'' - \iota'(6) \\ &\quad = \tfrac{3}{2}(n - w + \iota' + \kappa - \iota'(2)) - \tfrac{3}{2}\nu - 3\iota' - \kappa + \iota' + \iota'' - \iota'(6) \geqslant n - w, \end{aligned}$$

which is equivalent to

$$(n - w - \iota' + \kappa - \iota'(2)) - \nu + 2\iota'' \geqslant 2\nu + \iota'(16 \cdot 9).$$

By parity considerations, this inequality will be satisfied whenever

$$(n - w) + \kappa + 2\iota'' \geqslant \iota' + 2\nu + \iota'(32 \cdot 9). \tag{28}$$

In light of $n - w = \kappa + \iota' + 1 + n_1$, $n_1 \geqslant 0$, the above is satisfied whenever

$$2\kappa + 2\iota'(y + 1) + 1 + n_1 \geqslant 2\nu + \iota'(32 \cdot 9),$$

and this is automatically satisfied for $p \notin \{2, 3\}$. For $p \in \{2, 3\}$, substituting $\kappa + \iota'' = \nu + 2\iota'(2) + \kappa_1$, $\kappa_1 \geqslant 0$, the above inequality reads as

$$1 + n_1 + 2\kappa_1 \geqslant \iota'(18),$$

which is trivially satisfied in light of the condition that $n_1 + \kappa_1 \geqslant \iota'(3)$.

The other condition for $\nu_E \geqslant n$ is that

$$\begin{gathered} u + 3j' + \hat{\nu}_2 = u + \tfrac{3}{2}(n - w + \iota' + \kappa - \iota'(2)) - \tfrac{3}{2}\nu - 3\iota' - 3\kappa + \hat{\nu}_2 \geqslant n - w \\ (n - w - 3\iota' - 3\kappa - 3\iota'(2)) - \nu + 2u + 2\hat{\nu}_2 \geqslant 2\nu. \end{gathered}$$

Again, by parity considerations, this inequality will be satisfied whenever

$$(n - w) + 2u + 2\hat{\nu}_2 \geqslant 3\iota' + 3\kappa + 2\nu + \iota'(8). \tag{29}$$

We first comment on how (29) is always satisfied for $p \geqslant 3$. Indeed, for $p \geqslant 3$ we have that

$$\hat{\nu}_2 = \lceil 2(\lambda - \rho_p) \rceil \geqslant \lfloor \lambda \rfloor;$$

this is trivially true if $\lambda = \rho_p$ and follows from $2(\lambda - \rho_p) \geqslant \lambda$ if $\lambda \geqslant 2\rho_p$. The inequality (29) now follows from $n - w \geqslant \iota' + \kappa + 1$ and $u + \lfloor \lambda \rfloor \geqslant \iota' + \kappa + 1$.

Verifying the condition (29) for $p = 2$ involves checking all cases. The above argument clearly applies if $\hat{\nu}_2 = 2\lambda$. If $\hat{\nu}_2 = j' + 3\lambda - 2$, then (substituting for j' as above), (29) reads as

$$\begin{gathered} (n - w) + 2u + 2j - 2\iota' - 2\kappa + 6\lambda - 4 \geqslant 3\iota' + 3\kappa + 2\nu + 3 \\ 2(n - w) + 2u + 6\lambda \geqslant 4\iota' + 4\kappa + 3\nu + 8, \end{gathered} \tag{30}$$

and this follows immediately in light of $n - w \geqslant \iota' + \kappa + 1 + 2\iota'(2)\nu$.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Having checked that $\nu_E \geqslant n$, we conclude that

$$\breve{f}(t,q) \equiv \breve{f}(t) + \tfrac{1}{2} f''(\tilde{f}(t)) p^{2j'} q^2 \pmod{p^n}.$$

Writing $\tilde{\nu} = n - \nu_2 = \nu + 2\iota'(2)$, the summation in the intermediate stationary phase expression (26) becomes

$$\begin{aligned}\hat{\mathbf{e}}_f(\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t)) &= \sum_{q \bmod p^{n-w-j'}} e\biggl(\frac{\breve{f}(t) + \frac{1}{2} f''(\tilde{f}(t)) p^{2j'} q^2}{p^n}\biggr) \\ &= p^{(n-w-j'-\tilde{\nu})} e\biggl(\frac{\breve{f}(t)}{p^n}\biggr) \sum_{q \bmod p^{\tilde{\nu}}} e\biggl(\frac{\frac{1}{2} f''(\tilde{f}(t)) p^{2j'-\nu_2} q^2}{p^{\tilde{\nu}}}\biggr).\end{aligned}$$

The remaining sum can be evaluated by Lemma 8 as

$$p^{(\tilde{\nu}+\iota'(2))/2} \epsilon(\tfrac{1}{2} f''(\tilde{f}(t)) p^{2j'-\nu_2}, p^{\tilde{\nu}}),$$

where, for an odd prime p, $\epsilon(a, p^{\tilde{\nu}})$ depends on p, the parity of $\tilde{\nu}$, and the class of a mod p only, while for $p = 2$ and $\tilde{\nu} \in \{2,3\}$, $\epsilon(a, 2^{\tilde{\nu}})$ also depends on the class of a mod $2^{\tilde{\nu}}$. We have already seen (compare (27) for $r = 2$) that, for an odd p (when $\tilde{\nu} \in \{0,1\}$),

$$a = \tfrac{1}{2} f''(\tilde{f}(t)) p^{2j'-\nu_2} \equiv \omega\omega'(-y/2)|y/2|_p \pmod{p^{\tilde{\nu}}}.$$

In the case $p = 2$ (when $\tilde{\nu} \in \{2,3\}$), considering the power ν_2^+ of p in non-constant terms in (27), we find that

$$\begin{aligned}\nu_2^+ - \nu_2 &\geqslant \min\bigl(\kappa + \iota'', u + \lceil 2\lambda \rceil + \iota'(2) - \kappa - \iota', u + \lceil 3\lambda \rceil - \kappa - \iota'\bigr) \\ &\geqslant \min(\nu + 2\iota'(2), 3) = \tilde{\nu},\end{aligned}$$

and therefore

$$a = \tfrac{1}{2} f''(\tilde{f}(t)) p^{2j'-\nu_2} \equiv \omega\omega'(-y)|y|_p + p^{u-\kappa-\iota'} g'(0) \pmod{p^{\tilde{\nu}}}$$

in this case.

We conclude that, in any case,

$$\hat{\mathbf{e}}_f(\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t)) = p^{\tilde{n}/2} \epsilon\bigl(\omega\omega'(-y/2)|y/2|_p + p^{u-\kappa-\iota'} g'(0), p^{\tilde{\nu}}\bigr) e\biggl(\frac{\breve{f}(t)}{p^n}\biggr),$$

where

$$\begin{aligned}\tilde{n} &= 2(n - w - j' - \tilde{\nu}) + (\tilde{\nu} + \iota'(2)) \\ &= 2(n-w) - 2j + 2\iota' + 2\kappa - \nu - \iota'(2) \\ &= n - w + \iota' + \kappa.\end{aligned}$$

Note that (25) also defines $\breve{f}(t)$ as a formal power series; since $r_f = r_{f'} \geqslant p^{\tilde{\lambda}}$, $\tilde{f}(t) \in \mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$, and, for every $r < p^{\tilde{\lambda}}$, $M_r \tilde{f} \doteq r$, the numerical substitution of $\tilde{f}(t)$ in (25) is allowed for $|t|_p < p^{\tilde{\lambda}}$. To complete the proof of Lemma 10, it remains to prove that $\breve{f}$ belongs to the announced classes. According to the chain rule (6), we obtain from (25), (19), and (18) that

$$\begin{aligned}\breve{f}'(t) &= f'(\tilde{f}(t))\tilde{f}'(t) - p^w(\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t))\tilde{f}'(t) - \omega' p^{w+\iota'+\kappa} \tilde{f}(t) \\ &= -\omega' p^{w+\iota'+\kappa} \tilde{f}(t) \\ &= -\omega'\omega^{-1} p^{w+\mathrm{ord}_p y}(1+p^{\iota'+\kappa}t)^{-1/y} + \omega'\omega^{-1} p^{w+\mathrm{ord}_p y} - \omega' p^{w+u+\lfloor\lambda\rfloor} \tilde{g}(t).\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

This clearly shows that $\breve{f}' \in p^{w+\iota'+\kappa}\mathbf{I}_0^n[\tilde{\lambda}](\mathbb{Z}_p)$. Recalling Definition 1, we have that, indeed, $\breve{f} \in \mathbf{F}(\breve{w}, 1/y, \kappa, \tilde{\lambda}, \breve{u}, 1, -\omega'\omega^{-1})$ with

$$\breve{w} = w + \operatorname{ord}_p y, \quad \breve{u} = u + \lfloor \lambda \rfloor - \lceil \tilde{\lambda} \rceil - \operatorname{ord}_p y,$$

as announced. □

We would like to point out the following feature of (23), which is a complete exponential sum modulo p^{n-w}. That such exponential sums reduce to sums over the (approximate) critical points is classical; however, in general, one also encounters contributions from singular critical points, and these can be very difficult to evaluate or estimate. An extremely important feature of our definition of the class $\mathbf{F}$ is that it guarantees that we never encounter singular points, while still being sufficiently broad to cover all cases of interest for the estimation of short character sums. It is this feature that allows for the handsome, compact looks of the result of Lemma 10, the main thrust of whose proof is to explicate the p-adic implicit function $\tilde{f}$ in a neighborhood of a non-singular critical point and collect all contributions through explicit computations with p-adic Gaussians.

We also remark that many of the conditions included in Lemma 10 for $p \in \{2, 3\}$ can be relaxed or altogether dropped by allowing higher-order terms and directly evaluating the resulting sums. For example, the condition $n-w > \iota'+\kappa$ actually suffices for (30) in the case $p = 2$. Namely, (30) also holds if $n - w = \iota' + \kappa + 1$ (when $\nu = 0$), or if $u + \lambda \geqslant \iota' + \kappa + 2$, or if $\lambda \geqslant 2$. In the remaining case $n - w = \iota' + \kappa + 2$, $\nu = 1$, $\tilde{\nu} = 3$, $j' = 0$, $\lambda = 1$, $u = \iota' + \kappa$, we incur the extra term

$$\frac{f^{(iv)}(\tilde{f}(t))}{4!} p^{4j'} q^4 \equiv A_2 p^{n-1} q^4 \pmod{p^n},$$

where $A_2 = p^{u+w-n+1} g^{(iii)}(0)/4! \in \mathbb{Z}_2$, and the summation in (26) becomes

$$\hat{\mathbf{e}}_f(\tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa} t)) = p^{n-w-3} e\left(\frac{\breve{f}(t)}{p^n}\right) \sum_{q \bmod 8} e\left(\frac{aq^2 + 4A_2 q^4}{8}\right).$$

Since $4A_2q^4 \equiv 4A_2q^2 \pmod 8$, the inner sum can again be evaluated by Lemma 8, yielding Lemma 10 with only a change in the value of ϵ. However, we chose the current formulation, which reflects conditions that guarantee a purely quadratic-term expansion at each stationary point.

In the applications of Lemma 10, we will simply assume that $\kappa \geqslant 1 + \iota'(4)$ and $n - w > \iota' + \kappa + \iota'(12)$; while these conditions can occasionally be somewhat relaxed, we will not be concerned with this aspect, which is anyway relevant for $p \in \{2, 3\}$ only.

We collect the fruits of our labor in the following summation formula.

Theorem 3 (Summation formula). *Let $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$, $n \in \mathbb{N}$, $B > 0$, and a Schwarz function $h \in C_0^\infty(\mathbb{R})$ be given, and assume that*

$$\begin{gathered} \kappa \geqslant 1 + \iota'(4), \quad n - w > \kappa + \iota' + \iota'(12), \\ u + \lfloor \lambda \rfloor > \kappa + \iota', \quad \tilde{\lambda} = \min(\kappa - \rho_p(y), \lambda) > 0. \end{gathered} \tag{31}$$

Let $\varepsilon_\lambda = \lfloor \lambda \rfloor - \lceil \tilde{\lambda} \rceil$. Then there exists a function

$$\mathring{f} \in \mathbf{F}(w + \operatorname{ord}_p y, y^{-1}, \kappa, \tilde{\lambda}, u + \varepsilon_\lambda - \operatorname{ord}_p y, \omega'^{-1}, -\omega^{-1}) \tag{32}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

depending on f only and an $\epsilon \in \mathbb{C}$, $|\epsilon| = 1$, such that

$$\sum_{m\in\mathbb{Z}} e\left(\frac{f(m)}{p^n}\right) h\left(\frac{m}{B}\right) = \frac{\epsilon B}{p^{(n-w-\iota'-\kappa)/2}} \sum_{t\in\mathbb{Z}} e\left(\frac{\mathring{f}(t)}{p^n}\right) \hat{h}_{f,B}\left(\frac{t}{p^{n-w-\iota'-\kappa}/B}\right),$$

where $\hat{h}_{f,B}$ is a reflected translate of the Fourier transform $\hat{h}$ given by

$$\hat{h}_{f,B}(t) = \hat{h}\left(-t - \frac{f'(0)}{p^n/B}\right).$$

Proof. Let S denote the sum on the left-hand side of the equality to be proved. Since $e(f(t)/p^n)$ is periodic with period p^{n-w}, we have that

$$\begin{aligned} S &= \sum_{m \bmod p^{n-w}} \sum_{q\in\mathbb{Z}} e\left(\frac{f(m+p^{n-w}q)}{p^n}\right) h\left(\frac{m+p^{n-w}q}{B}\right) \\ &= \sum_{m \bmod p^{n-w}} e\left(\frac{f(m)p^{-w}}{p^{n-w}}\right) h_B^{\sharp}(m), \end{aligned} \tag{33}$$

where

$$h_B^{\sharp}(m) = \sum_{q\in\mathbb{Z}} h\left(\frac{m+p^{n-w}q}{B}\right)$$

is a $(\mathbb{Z}/p^{n-w}\mathbb{Z})$-periodic function. Applying Parseval's identity, we have that

$$S = \frac{1}{p^{n-w}} \sum_{s \bmod p^{n-w}} \hat{\mathbf{e}}_f(s)\hat{h}_B^{\sharp}(-s),$$

where $\hat{\mathbf{e}}_f(s)$ is as in (23), while, by unfolding,

$$\begin{aligned} \hat{h}_B^{\sharp}(s) &= \sum_{m \bmod p^{n-w}} h_B^{\sharp}(m) e\left(-\frac{sm}{p^{n-w}}\right) \\ &= \sum_{m \bmod p^{n-w}} \sum_{q\in\mathbb{Z}} h\left(\frac{m+p^{n-w}q}{B}\right) e\left(-\frac{s(m+p^{n-w}q)}{p^{n-w}}\right) \\ &= \sum_{m\in\mathbb{Z}} h\left(\frac{m}{B}\right) e\left(-\frac{sm}{p^{n-w}}\right). \end{aligned}$$

Applying the Poisson summation formula, we find that

$$\hat{h}_B^{\sharp}(s) = \sum_{\sigma\in\mathbb{Z}} \int_{-\infty}^{\infty} h\left(\frac{x}{B}\right) e\left(-\frac{sx}{p^{n-w}} - \sigma x\right) dx = B \sum_{\sigma\in\mathbb{Z}} \hat{h}\left(\frac{s}{p^{n-w}/B} + B\sigma\right),$$

where $\hat{h}$ denotes the usual Fourier transform. Therefore,

$$S = \frac{B}{p^{n-w}} \sum_{s \bmod p^{n-w}} \sum_{\sigma\in\mathbb{Z}} \hat{\mathbf{e}}_f(s)\hat{h}\left(-\frac{s}{p^{n-w}/B} + B\sigma\right). \tag{34}$$

We remark that, while the expression of S as (34) can be reached in fewer steps, we have structured the above proof so as to emphasize the rôle of duality in passing from a long sum in (33) to a short one or conversely.

We now crucially apply Lemma 10. According to this lemma, which may be applied in light of (31), the Fourier transform $\hat{\mathbf{e}}_f(s)$ vanishes unless $s = \tilde{g}_0 + \omega'(1 + p^{\iota'+\kappa}t)$ for some $t \in \mathbb{Z}_p$, in which case $\hat{\mathbf{e}}_f(s)$ is given in terms of the exponential $e(\breve{f}(t)/p^n)$, with the function $\breve{f}$ as in the statement of Lemma 10. Using this result, we obtain

$$\begin{aligned} S &= \frac{B}{p^{n-w}} \epsilon p^{(n-w+\iota'+\kappa)/2} \sum_{t \bmod p^{n-w-\iota'-\kappa}} \sum_{\sigma\in\mathbb{Z}} e\biggl(\frac{\breve{f}(t)}{p^n}\biggr) \hat{h}\biggl(-\frac{\tilde{g}_0 + \omega'(1+p^{\iota'+\kappa}t)}{p^{n-w}/B} + B\sigma\biggr) \\ &= \frac{\epsilon B}{p^{(n-w-\iota'-\kappa)/2}} \sum_{t \bmod p^{n-w-\iota'-\kappa}} \sum_{\sigma\in\mathbb{Z}} e\biggl(\frac{\breve{f}(\omega'^{-1}t)}{p^n}\biggr) \hat{h}\biggl(-\frac{(t - p^{n-w-\iota'-\kappa}\sigma) + (\tilde{g}_0 + \omega')p^{-\iota'-\kappa}}{p^{n-w-\iota'-\kappa}/B}\biggr) \\ &= \frac{\epsilon B}{p^{(n-w-\iota'-\kappa)/2}} \sum_{t\in\mathbb{Z}} e\biggl(\frac{\breve{f}(\omega'^{-1}t)}{p^n}\biggr) \hat{h}\biggl(-\frac{t + (\tilde{g}_0 + \omega')p^{-\iota'-\kappa}}{p^{n-w-\iota'-\kappa}/B}\biggr), \end{aligned}$$

by unfolding again. The statement of the theorem follows by setting

$$\mathring{f}(t) := \breve{f}(\omega'^{-1}t) \in \mathbf{F}(\breve{w}, y^{-1}, \kappa, \tilde{\lambda}, \breve{u}, \omega'^{-1}, -\omega^{-1}),$$

noting that $(\mathring{f}(t))' = \omega'^{-1}\breve{f}'(\omega'^{-1}t)$ and recalling that $\tilde{g}_0 + \omega' = f'(0)p^{-w}$. □

Theorem 4 (B-process). *If $(k, \ell, r, \delta, (n_0, u_0, \kappa_0, \lambda_0))$ is a p-adic exponent datum, then so is*

$$B(k, \ell, r, \delta, (n_0, u_0, \kappa_0, \lambda_0)) = \bigl(\ell - \tfrac{1}{2}, k + \tfrac{1}{2}, \tilde{r}, \tilde{\delta}, (\tilde{n}_0, \tilde{u}_0, \tilde{\kappa}_0, \tilde{\lambda}_0)\bigr),$$

where, denoting $\tilde{\lambda} = \min(\kappa - \rho_p(y), \lambda)$,

$$\begin{aligned} \tilde{r}(y, p, \kappa, \lambda) &= r(y^{-1}, p, \kappa, \tilde{\lambda}), \quad \tilde{\delta} = \delta + \delta_{01}, \\ \tilde{\kappa}_0(y, p) &= \max\bigl(1 + \iota'(4), \kappa_0(y^{-1}, p), \lambda_0(y^{-1}, p) + \rho_p(y)\bigr), \\ \tilde{\lambda}_0(y, p) &= \lambda_0(y^{-1}, p), \\ \tilde{n}_0(y, p, \kappa, \lambda) &= \max\bigl(\kappa + \iota' + 1 + \iota'(12), \mathrm{ord}_p y + n_0(y^{-1}, p, \kappa, \tilde{\lambda})\bigr), \\ \tilde{u}_0(y, p, \kappa, \lambda) &= \max\bigl(\kappa - \lfloor\lambda\rfloor + \iota' + 1, \mathrm{ord}_p y + u_0(y^{-1}, p, \kappa, \tilde{\lambda}) + \lceil\tilde{\lambda}\rceil - \lfloor\lambda\rfloor, 1\bigr). \end{aligned}$$

Proof. Let $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$ and $0 < B \leqslant p^{n-w-\iota'-\kappa}$ be given. Fix a Schwarz function $h \in C_0^\infty(\mathbb{R})$, and consider the sum

$$S = \sum_{m\in\mathbb{Z}} e\biggl(\frac{f(m)}{p^n}\biggr) h\biggl(\frac{m}{B}\biggr),$$

with an eye to invoking Lemma 6. According to Theorem 3, assuming that conditions (31) hold, we have that

$$S = \frac{\epsilon B}{p^{(n-w-\iota'-\kappa)/2}} \sum_{t\in\mathbb{Z}} e\biggl(\frac{\mathring{f}(t)}{p^n}\biggr) \hat{h}_{f,B}\biggl(\frac{t}{p^{n-w-\iota'-\kappa}/B}\biggr),$$

with $\hat{h}_{f,B}$ as in Theorem 3, $|\epsilon| = 1$, and

$$\mathring{f} \in \mathbf{F}\bigl(w + \mathrm{ord}_p\, y, y^{-1}, \kappa, \tilde{\lambda}, u + \varepsilon_\lambda - \mathrm{ord}_p\, y, \omega'^{-1}, -\omega^{-1}\bigr).$$

We now estimate the sum on the right-hand side using the given p-adic exponent datum and Lemma 6. We note that, importantly, the cutoff function $\hat{h}_{f,B}$ satisfies $\|\hat{h}_{f,B}\|_\star = \|\hat{h}\|_\star$, where $\|\cdot\|_\star$ is the (translation-invariant) quantity defined in (17) which enters the condition $H^\sharp_{\mathrm{sm}}(\delta)$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

in Lemma 6. The given exponent datum can be directly applied as long as

$$1 \leqslant p^{n-w-\iota'-\kappa}/B \leqslant p^{(n-w-\iota'+\iota-\kappa)-\iota},$$

which is trivially satisfied, and

$$\begin{gathered} n-w-\operatorname{ord}_p y \geqslant n_0(y^{-1},p,\kappa,\tilde{\lambda}), \quad \kappa \geqslant \kappa_0(y^{-1},p), \\ \tilde{\lambda} = \min(\kappa-\rho_p(y),\lambda) \geqslant \lambda_0(y^{-1},p), \quad u+\lfloor\lambda\rfloor-\lceil\tilde{\lambda}\rceil-\operatorname{ord}_p y \geqslant u_0(y^{-1},p,\kappa,\tilde{\lambda}). \end{gathered} \tag{35}$$

We thus find that

$$\begin{aligned} S &= \frac{\epsilon B}{p^{(n-w-\iota'-\kappa)/2}} \sum_{t\in\mathbb{Z}} e\left(\frac{\mathring{f}(t)}{p^n}\right) \hat{h}_{f,B}\left(\frac{t}{p^{n-w-\iota'-\kappa}/B}\right) \\ &\ll \|\hat{h}_{f,B}\|_\star \cdot \frac{B}{p^{(n-w-\iota'-\kappa)/2}} p^r \left(\frac{p^{(n-w-\iota'+\iota)-\kappa-\iota}}{p^{n-w-\iota'-\kappa}/B}\right)^k \left(\frac{p^{n-w-\iota'-\kappa}}{B}\right)^\ell (\log p^{(n-w-\iota'+\iota)-\kappa-\iota})^\delta \\ &= \|\hat{h}\|_\star \cdot p^{r-(\iota'+\kappa)\ell+(\iota'+\kappa)/2} B^{1+k-\ell} (p^{n-w})^{\ell-1/2} (\log p^{n-w-\kappa-\iota'})^\delta \\ &= \|\hat{h}\|_\star \cdot p^{\tilde{r}} \left(\frac{p^{n-w-\kappa-\iota'}}{B}\right)^{\ell-1/2} B^{k+1/2} (\log p^{n-w-\kappa-\iota'})^\delta, \end{aligned}$$

with

$$\tilde{r} = \tilde{r}(y,p,\kappa,\lambda) = r(y^{-1},p,\kappa,\tilde{\lambda}).$$

We now apply Lemma 6 again. Since the estimate proved above holds with a constant depending on the cutoff function h only, we have, according to the implication $H_{\mathrm{sm}}(\delta)^{sq} \implies H(\delta+\delta_{1/2})^{sq}$, that, for every $M \in \mathbb{Z}$ and every $0 < B \leqslant p^{n-w-\kappa-\iota'}$,

$$\sum_{M<m\leqslant M+B} e\left(\frac{f(m)}{B}\right) \ll p^{\tilde{r}(y,p)} \left(\frac{p^{n-w-\kappa-\iota'}}{B}\right)^{\ell-1/2} B^{k+1/2} (\log p^{n-w-\kappa-\iota'})^{\tilde{\delta}},$$

with $\tilde{\delta} = \delta+\delta_{01}$ (and δ_{01} equal to the $\delta_{1/2}$ applied to the pair $(\ell-\frac{1}{2}, k+\frac{1}{2})$) and a uniform implied constant. This estimate is valid as long as all conditions listed in (31) and (35) are satisfied; this gives us the p-adic exponent datum announced in the statement of the theorem. □

In particular, applying Theorem 4 to the trivial p-adic exponent datum

$$\omega_{01} = (0,1,0,0,(\kappa+\iota'+1,1,1+\iota'(2),\rho_p)),$$

we obtain the following important datum:

$$\omega_{1/2} = \left(\tfrac{1}{2},\tfrac{1}{2},0,1,(\kappa+\iota'+1+\iota'(12),\max(\kappa-\lfloor\lambda\rfloor+\iota'+1,1),1+\iota'(4),\rho_p)\right). \tag{36}$$

5. *A*-process

The A-process relies on a procedure in which an estimate on the exponential sum (4) is obtained by comparing it to sums obtained by replacing f with its differences over pairs of points in appropriate p-adic neighborhoods (see (37) below); this has the effect of considerably reducing the modulus relative to the length of the summation. This estimate can be seen as an adaptation of the classical Weyl–van der Corput inequality. For clarity, we state the underlying inequality separately and in some generality.

Lemma 11. *Let $b : \mathbb{Z} \to \mathbb{C}$ be an arbitrary function such that $|b(t)| \ll 1$ for every $t \in \mathbb{Z}$. Let $M \in \mathbb{Z}$ and $B \in \mathbb{N}$, and let*

$$S = \sum_{M<m\leqslant M+B} b(m).$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Then, for every positive integer $0 < H \leqslant B$,

$$S^2 \ll BH + H \sum_{0<|h|<B/H} \biggl| \sum_{m \in J(h)} b(m+hH)\overline{b(m)} \biggr|,$$

where

$$J(h) = (M, M+B-hH] \cap (M-hH, M+B]$$

is an interval of length $|J(h)| = B - |h|H \leqslant B$.

Proof. Let $I(m)$ be an interval of the real axis depending on $m \in \mathbb{Z}$ defined as

$$I(m) = \{t \in \mathbb{R} : M < m + tH \leqslant M+B\} = \biggl(\frac{M-m}{H}, \frac{M+B-m}{H}\biggr].$$

Note that $|I(m)| = B/H$ for every $m \in \mathbb{Z}$. We can adapt Weyl's 'smoothing' trick to write

$$\begin{aligned}
&\sum_{M-H<m\leqslant M+B} \sum_{h\in I(m)} b(m+hH) \\
&\quad= \sum_{M<m\leqslant M+B} b(m) \cdot \# \left\{ (m_1, h) : \begin{matrix} M-H < m_1 \leqslant M+B, \\ h \in I(m_1),\ m = m_1 + hH \end{matrix} \right\} \\
&\quad= \sum_{M<m\leqslant M+B} b(m) \cdot \#\{h \in \mathbb{Z} : M-H < m-hH \leqslant M+B\} \\
&\quad= \sum_{M<m\leqslant M+B} b(m)\biggl(\frac{B}{H} + \mathrm{O}(1)\biggr) = \frac{B}{H}S + \mathrm{O}(B).
\end{aligned}$$

The second equality follows from an observation that, given $m \in (M, M+B]$, $m_1 \in (M-H, M+B]$, and $h \in \mathbb{Z}$ such that $m = m_1 + hH$, the condition $h \in I(m_1)$ is automatically satisfied.

Applying the Cauchy–Schwarz inequality, we have that

$$\begin{aligned}
\frac{B^2}{H^2}S^2 &\ll \biggl| \sum_{M-H<m\leqslant M+B} \sum_{h\in I(m)} b(m+hH) \biggr|^2 + B^2 \\
&\ll B \sum_{M-H<m\leqslant M+B} \biggl| \sum_{h\in I(m)} b(m+hH) \biggr|^2 + B^2 \\
&\ll \frac{B^3}{H} + B \sum_{M-H<m\leqslant M+B} \sum\sum_{h_1,h_2\in I(m),\ h_1\neq h_2} b(m+h_1H)\overline{b(m+h_2H)} + B^2 \\
&\ll \frac{B^3}{H} + B \sum\sum\sum_{\substack{M-H<m\leqslant M+B,\ 0<|h|<B/H, \\ g\in I(m),\ g+h\in I(m)}} b((m+gH)+hH)\overline{b(m+gH)} \\
&= \frac{B^3}{H} + B \sum_{0<|h|<B/H} \sum_{-B/H<g<B/H+1} \sum_{m\in J(h)} b(m+hH)\overline{b(m)} \\
&\ll \frac{B^3}{H} + \frac{B^2}{H} \sum_{0<|h|<B/H} \biggl| \sum_{m\in J(h)} b(m+hH)\overline{b(m)} \biggr|,
\end{aligned}$$

with $J(h)$ as in the statement of the lemma. This gives the desired inequality. □

The condition $|b(t)| \ll 1$ is not essential and was introduced only with our application in mind. Following the proof practically verbatim with an extra application of the Cauchy–Schwarz inequality to estimate the error term from the smoothing, one can prove that, for every function $b : \mathbb{Z} \to \mathbb{C}$,

$$S^2 \ll H \sum_{0 \leqslant |h| < B/H} \left| \sum_{m \in J(h)} b(m + hH)\overline{b(m)} \right|,$$

with the term $h = 0$ accounting for the diagonal contribution; the statement of the lemma follows trivially when $|b(t)| \ll 1$.

We will use Lemma 11 with $b(t) = e(f(t)/p^n)$ and with $H = p^\chi$ chosen as a power of p. The estimate we just proved reads as

$$S^2 \ll BH + H \sum_{0 < |h| < B/H} \left| \sum_{m \in J(h)} e\left(\frac{f(m + p^\chi h) - f(m)}{p^n} \right) \right|. \tag{37}$$

In the following lemma, we consider the function appearing in the inner exponential sum.

LEMMA 12. *Let $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$, and assume that*

$$u > \kappa - \lfloor \lambda \rfloor + \iota' \quad \text{and} \quad \lambda + \chi > \rho_p.$$

Let $\tilde{\varepsilon}(y) = 1$ if $\operatorname{ord}_p y < 0$ and $\tilde{\varepsilon}(y) = 0$ otherwise, and let

$$\tilde{\lambda} = \min(\kappa - \tilde{\varepsilon}(y)\rho_p, \lambda), \quad \mu = \min(2\kappa + \iota' - \iota'(2) - \tilde{\varepsilon}(y), u + \lfloor 2\lambda - \rho_p \rfloor).$$

Let $\chi \geqslant 0$, $h \in \mathbb{Z}_p^\times$ be fixed. Then there exists a power series $g_1 \in \mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$ with $g_1' \in p^\mu \mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$ such that the equality

$$f_{\chi,h}(t) := f(t + p^\chi h) - f(t) = p^\chi h f'(t) + p^{2\chi + w} g_1(t)$$

holds for all $|t|_p < p^{\tilde{\lambda}}$. In particular,

$$\begin{aligned} f_{\chi,h} \in \mathbf{F}\big(&w + \chi + \kappa + \iota', y + 1, \kappa, \tilde{\lambda}, \\ &\min(u + \lfloor \lambda \rfloor - \kappa - \iota', \chi + \kappa - \iota'(2) - \varepsilon(y)), \omega, \omega\omega'(-y)|y|_p h\big). \end{aligned}$$

Proof. Since $r_f = r_{f'} \geqslant p^{\tilde{\lambda}}$, we have according to (9) the equality of values

$$f(t + p^\chi h) - f(t) = p^\chi h f'(t) + p^{2\chi} h^2 \sum_{r=2}^{\infty} p^{(r-2)\chi} h^{r-2} \frac{f^{(r)}(t)}{r!}$$

for every $|t|_p < p^{\tilde{\lambda}}$.

We now consider the infinite sum of the series on the right-hand side as a formal sum. With $g(t)$ as in (11) and writing $g'(t) = \sum_{j=0}^{\infty} g_j t^j \in \mathbf{I}_{0,1}[\lambda](\mathbb{Z}_p)$, the coefficient of the rth series with t^j $(j \geqslant 0)$ equals

$$a_{rj} = \frac{h^{r-2} p^{w + (r-2)\chi}}{r!} \left(\omega' \omega^{j+r-2} p^{\kappa + \iota' + (\iota + \kappa)(j+r-2)} \frac{(-y-1)_{j+r-2}}{j!} + p^u g_{j+r-2} (j + r - 2)_{r-2} \right).$$

It follows that

$$\begin{aligned} \operatorname{ord}_p(a_{rj}) &\geqslant w + (r-2)\chi - \operatorname{ord}_p(r!) + \min\big(\kappa(j + r - 1) - \tilde{\varepsilon}(y) \operatorname{ord}_p(j!) + \iota', u + \lceil \lambda(j + r - 1) \rceil\big) \\ &\geqslant w + \min\big(\lceil (\kappa + \chi - \rho_p)(r - 2) - \rho_p \rceil + \lceil (\kappa - \tilde{\varepsilon}(y)\rho_p) j \rceil + \kappa + \iota', \\ &\qquad u + \lceil \lambda(j + 1) + (r - 2)(\lambda + \chi - \rho_p) - \rho_p \rceil\big). \end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

According to our discussion in (10), since $\min(\kappa,\lambda)+\chi>\rho_p$, the formal sum of power series converges to a power series $\tilde{g}_1(t)=\sum_{j=0}^{\infty}\tilde{g}_j t^j$ with

$$\operatorname{ord}_p \tilde{g}_j \geqslant w+\min\bigl(\lceil(\kappa-\tilde{\varepsilon}(y)\rho_p)j\rceil+\kappa+\iota'-\iota'(2), u+\lceil\lambda(j+1)-\rho_p\rceil\bigr);$$

moreover, we have that $\tilde{g}_1(t)\in p^w\mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$, and the pointwise equality of values holds for all $|t|_p<p^{\tilde{\lambda}}$. Hence we can take $g_1(t)=h^2p^{-w}\tilde{g}_1(t)$. We also have that

$$\operatorname{ord}_p((j+1)\tilde{g}_{j+1})\geqslant w+\min\bigl(\lceil(\kappa-\tilde{\varepsilon}(y)\rho_p)j\rceil+2\kappa+\iota'-\iota'(2)-\tilde{\varepsilon}(y), u+\lceil\lambda(j+2)-\rho_p\rceil\bigr),$$

so that $g_1'(t)\in p^{\mu}\mathbf{I}_0[\tilde{\lambda}](\mathbb{Z}_p)$ with $\mu=\min(2\kappa+\iota'-\iota'(2)-\tilde{\varepsilon}(y), u+\lfloor 2\lambda-\rho_p\rfloor)$, as announced. □

The following theorem establishes the p-adic A-process. Its statement may appear somewhat frightening, but this is due to our desire to work in full generality. We will see in § 6 how one obtains very concrete and easy to work with exponent data as long as one stays away from a finite number of primes and makes a concrete choice of κ. To keep the expressions manageable, we write $g(y^{\pm})$ to denote $\max(g(y),g(y^{-1}))$.

Theorem 5 (A-process). *If $(k,\ell,r,\delta,(n_0,u_0,\kappa_0,\lambda_0))$ is a p-adic exponent datum, then*

$$A(k,\ell,r,\delta,(n_0,u_0,\kappa_0,\lambda_0))=\left(\frac{k}{2(k+1)},\frac{k+\ell+1}{2(k+1)},\tilde{r},\tilde{\delta},(\tilde{n}_0,\tilde{u}_0,\tilde{\kappa}_0,\tilde{\lambda}_0)\right)$$

is also a p-adic exponent datum.

Here, if $0<k\leqslant\frac{1}{2}\leqslant\ell<1$, then, denoting $\tilde{\lambda}=\min(\kappa-\rho_p(y),\lambda)$,

$$\tilde{r}(y,p,\kappa,\lambda)=\frac{r+k\bigl(1-\kappa-\min(\iota'(y+1),\iota'(y^{-1}+1))\bigr)}{2(k+1)},\quad \tilde{\delta}=\frac{\max(1,\delta)}{2},$$

as well as

$$\begin{aligned}\tilde{\kappa}_0(y,p)&=\max\bigl(1+\iota'(4),\kappa_0(y^{\pm}+1,p),\rho_p(y)+\lambda_0(y^{\pm}+1,p),\rho_p(y)+2\rho_p\bigr),\\ \tilde{\lambda}_0(y,p)&=\max\bigl(\lambda_0(y^{\pm}+1,p),2\rho_p\bigr),\\ \tilde{u}_0(y,p,\kappa,\lambda)&=\max\bigl(1,u_0(y+1,p,\kappa,\tilde{\lambda})+\kappa-\lfloor\lambda\rfloor+\iota'(y),\\ &\qquad u_0(y^{-1}+1,p,\kappa,\tilde{\lambda})+\kappa+\lceil\tilde{\lambda}\rceil-\lfloor\lambda\rfloor-\lfloor\tilde{\lambda}\rfloor+\iota'(y),\\ &\qquad 2\kappa-\lfloor\lambda\rfloor-\lfloor\tilde{\lambda}\rfloor+\iota'(y(y+1))+1,\\ &\qquad 2\kappa+\lceil\tilde{\lambda}\rceil-\lfloor\lambda\rfloor-2\lfloor\tilde{\lambda}\rfloor+\iota'(y)+\iota'(y^{-1}+1)+1\bigr),\\ \tilde{n}_0(y,p,\kappa,\lambda)&=\kappa+\iota'(y)+\Biggl\lceil\max\Biggl(2\kappa+2\iota'(y^{\pm}+1)+2\iota'(12),\\ &\qquad n_0(y^{\pm}+1,p,\kappa,\tilde{\lambda})+\kappa+\iota'(y^{\pm}+1)-1,\\ &\qquad \tfrac{3}{2}n_0(y^{\pm}+1,p,\kappa,\tilde{\lambda})-\tfrac{1}{2}\kappa-\tfrac{1}{2}\iota'(y^{\pm}+1)-\tfrac{3}{2},\\ &\qquad n_0(y^{\pm}+1,p,\kappa,\tilde{\lambda})+\iota'(2)+\iota'(y^{\pm}+1)+\varepsilon(y^{\pm})-\lfloor\tilde{\lambda}\rfloor,\\ &\qquad \frac{2(r+\kappa+\iota'(y^{\pm}+1))+(k-1)}{1-\ell},\\ &\qquad \varepsilon_u\biggl(\frac{2k+1-\ell}{k}(u_0(y^{\pm}+1,p,\kappa,\tilde{\lambda})-\kappa+\iota'(2)+\varepsilon(y^{\pm}))\\ &\qquad\quad -\frac{r-1}{k(k+1)}+\frac{\kappa+\iota'(y^{\pm}+1)}{k+1}\biggr)\Biggr)\Biggr\rceil,\end{aligned}$$

where $\varepsilon_u=0$ if $u_0(y^{\pm}+1,p,\kappa,\tilde{\lambda})-\kappa+\iota'(2)+\varepsilon(y^{\pm})\leqslant 0$ and $\varepsilon_u=1$ otherwise.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

If $k = 0$, the above holds with

$$\tilde{r}(y) = r(y)/2, \quad \tilde{\delta} = \delta/2,$$
$$\tilde{\kappa}_0 = \kappa_0(y,p), \quad \tilde{\lambda}_0 = \lambda_0(y,p), \quad \tilde{n}_0 = n_0, \quad \tilde{u}_0 = u_0.$$

If $\ell = 1$, the above holds with

$$\tilde{r}(y) = 0, \quad \tilde{\delta} = \frac{k}{k+1}, \quad \tilde{\kappa}_0 = 1 + \iota'(4), \quad \tilde{\lambda}_0 = \rho_p,$$
$$\tilde{n}_0 = \kappa + \iota'(y) + 1 + \iota'(12), \quad \tilde{u}_0 = \max(\kappa - \lfloor\lambda\rfloor + \iota'(y) + 1, 1).$$

Proof. Let $f \in \mathbf{F}(w, y, \kappa, \lambda, u, \omega, \omega')$, $M \in \mathbb{Z}$, and $0 < B \leqslant p^{n-w-\kappa-\iota'}$ be given, and let

$$S = \sum_{M < m \leqslant M+B} e\biggl(\frac{f(m)}{p^n}\biggr).$$

We consider the principal case $0 < k \leqslant \frac{1}{2} \leqslant \ell < 1$; the complementary cases are easy and will be addressed at the end of the proof. Denote $\tilde{w} = w + \kappa + \iota'$, and let ρ and σ be real parameters, to be suitably chosen later. We seek to prove an estimate of the form

$$S \ll p^{\tilde{r}}\biggl(\frac{p^{n-\tilde{w}}}{B}\biggr)^{k/(2(k+1))} B^{(k+\ell+1)/(2(k+1))}(\log p^{n-\tilde{w}})^{\tilde{\delta}}. \tag{38}$$

The basic strategy is to estimate S by applying the given p-adic exponent datum to the inner sum in (37). For this purpose, we will choose H to be a positive integer, in fact a power of p, satisfying

$$H = p^{\chi} = p^{\sigma}\biggl(\frac{p^{n-\tilde{w}}}{B}\biggr)^{k/(k+1)} B^{\ell/(k+1)} \tag{39}$$

for some $\sigma \in \mathbb{R}$ to be suitably chosen. It turns out that this strategy works well if B is neither too small nor too large, in a sense which will be made precise.

To make the discussion easier to follow, we present the proof in two parts. The principal range for B, along with the easy case when B is small, is treated in the first part of the proof. We will address the range when B is large in the second part of the proof by using the summation formula of Theorem 3 to shorten the sum down to the first range.

1. Range $1 \leqslant B \leqslant p^{n-\tilde{w}-\rho}/H$. If $1 \leqslant B \leqslant H$, then we use the trivial bound $|S| \leqslant B$ to obtain

$$|S| \leqslant B \leqslant (BH)^{1/2} = p^{\sigma/2}\biggl(\frac{p^{n-\tilde{w}}}{B}\biggr)^{k/(2(k+1))} B^{(k+\ell+1)/(2(k+1))}.$$

This suffices for (38) as long as

$$\tilde{r} \geqslant \sigma/2 + o_p, \tag{40}$$

where (here and on) we denote $o_p = \mathrm{O}(1/\log p)$ and $0 \leqslant o_p^+ \ll 1/\log p$, so that $p^{o_p}, p^{o_p^+} \asymp 1$.

We now consider the range $H \leqslant B \leqslant p^{n-\tilde{w}-\rho}/H$, which is of principal interest. The lower bound on B implies that

$$H \geqslant p^{\sigma}\biggl(\frac{p^{n-\tilde{w}}}{H}\biggr)^{k/(k+1)} H^{\ell/(k+1)} = p^{\sigma}(p^{n-\tilde{w}})^{k/(k+1)} H^{(\ell-k)/(k+1)},$$
$$H \geqslant p^{\sigma/(2k+1-\ell)}(p^{n-\tilde{w}})^{k/(2k+1-\ell)}, \tag{41}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

since we are assuming that $(k,\ell)\neq(0,1)$. The upper bound on B can be equivalently written as

$$B\leqslant p^{n-\tilde{w}-\rho}p^{-\sigma}\bigg(\frac{p^{n-\tilde{w}}}{B}\bigg)^{-k/(k+1)}B^{-\ell/(k+1)}=p^{-(\rho+\sigma)}(p^{n-\tilde{w}})^{1/(k+1)}B^{-(\ell-k)/(k+1)}$$

$$B\leqslant p^{-(\rho+\sigma)(k+1)/(\ell+1)}(p^{n-\tilde{w}})^{1/(\ell+1)}. \tag{42}$$

We will assume that

$$\rho\geqslant\hat{\kappa},$$

where $\hat{\kappa}=\kappa+\iota'(y+1)$, thus ensuring that

$$B\leqslant p^{n-\tilde{w}-\chi-\hat{\kappa}}.$$

We can rewrite (37), the result of Weyl differencing (Lemma 11), as

$$S^2\ll BH+H\sum_{0<|h|<B/H}\bigg|\sum_{m\in J(h)}e\bigg(\frac{f_{\chi,h}(m)}{p^n}\bigg)\bigg|, \tag{43}$$

where $f_{\chi,h}(t)=f(t+p^{\chi}h)-f(t)$. According to Lemma 12, assuming that

$$u>\kappa-\lfloor\lambda\rfloor+\iota'(y),\quad \lambda+\chi+\mathrm{ord}_p\,h>\rho_p, \tag{44}$$

we have that

$$\begin{aligned}f_{\chi,h}\in\mathbf{F}\big(&w+\chi+\mathrm{ord}_p\,h+\kappa+\iota',y+1,\kappa,\tilde{\lambda},\\ &\min(u+\lfloor\lambda\rfloor-\kappa-\iota',\chi+\mathrm{ord}_p\,h+\kappa-\iota'(2)-\varepsilon(y)),\omega,\omega'h|h|_p(-y)|y|_p\big).\end{aligned}$$

The inner sum $S(h)$ in (43) will be estimated using an appropriate existing p-adic exponent datum. Write $\tilde{w}_\chi=\chi+\tilde{w}$, $h_p=|h|_p^{-1}=p^{\chi_p}$. We see that we can use the given p-adic exponent datum for those values of h for which χ_p satisfies

$$n-\tilde{w}_\chi-\chi_p\geqslant n_0:=n_0(y+1,p,\kappa,\tilde{\lambda}),$$

as long as all other conditions are satisfied. We separate the sum in (43) into two appropriate ranges for h as

$$S^2\ll BH+H(S_1+S_2),$$

where

$$S_1=\sum_{\substack{0<|h|<B/H\\0\leqslant\chi_p\leqslant n-\tilde{w}_\chi-n_0}}|S(h)|,\quad S_2=\sum_{\substack{0<|h|<B/H\\\chi_p>n-\tilde{w}_\chi-n_0}}|S(h)|.$$

We think of BH and HS_1 as the two main terms in this estimate on S^2. All other terms we encounter will be estimated so as to be (essentially) majorized by upper bounds on one of them (as was already done in the case $B\leqslant H$).

We first estimate S_1. The inner sum $S(h)$ in S_1 can be estimated using the given p-adic exponent datum as long as

$$\begin{gathered}\kappa\geqslant\kappa_0(y+1,p),\quad \tilde{\lambda}=\min(\kappa-\rho_p(y),\lambda)\geqslant\lambda_0(y+1,p),\\ u\geqslant u_0(y+1,p,\kappa,\tilde{\lambda})+\kappa-\lfloor\lambda\rfloor+\iota'(y),\end{gathered} \tag{45}$$

as well as

$$\chi\geqslant u_0(y+1,p,\kappa,\tilde{\lambda})-\kappa+\iota'(2)+\varepsilon(y).$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

The latter condition is trivially satisfied when the right-hand side is non-positive. If this is not the case, we still need this inequality only in the range (41), so that it is satisfied whenever

$$n-\tilde{w}\geqslant\varepsilon_u\biggl(\frac{2k+1-\ell}{k}(u_0(y+1,p,\kappa,\tilde{\lambda})-\kappa+\iota'(2)+\varepsilon(y))-\frac{\sigma}{k}\biggr).\tag{46}$$

Writing $r=r(y+1,p,\kappa,\tilde{\lambda})$, we thus obtain the estimate

$$\begin{aligned}|S(h)|&\ll p^r\biggl(\frac{p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}}{|J(h)|}\biggr)^k|J(h)|^\ell(\log p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}})^\delta\\&\leqslant p^r\biggl(\frac{p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}}{B}\biggr)^kB^\ell(\log p^{n-\tilde{w}})^\delta\end{aligned}$$

valid for all h appearing in S_1 for which $|J(h)|\leqslant p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}$, as well as the estimate

$$|S(h)|\ll p^r(p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}})^\ell\biggl(\frac{|J(h)|}{p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}}+1\biggr)(\log p^{n-\tilde{w}})^\delta,$$

valid for all h in S_1 regardless of the size of $|J(h)|$. Combining these estimates, we find that, assuming that (45) and (46) are satisfied, we have

$$\begin{aligned}HS_1&\ll p^rB\biggl(\frac{p^{n-\tilde{w}_\chi-\hat{\kappa}}}{B}\biggr)^kB^\ell(\log p^{n-\tilde{w}})^\delta\\&\quad+p^rH\sum_{\substack{0<|h|<B/H,\\ \chi_p>n-\tilde{w}_\chi-\hat{\kappa}-\log B/\log p}}\frac{B}{(p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}})^{1-\ell}}(\log p^{n-\tilde{w}})^\delta.\end{aligned}$$

The second term of this estimate is

$$\begin{aligned}&\leqslant p^r\frac{BH}{p^{(n-\tilde{w}_\chi-\hat{\kappa})(1-\ell)}}\sum_{\psi>n-\tilde{w}_\chi-\hat{\kappa}-\log B/\log p}p^{\psi(1-\ell)}\frac{B/H}{p^\psi}(\log p^{n-\tilde{w}})^\delta\\&\ll p^r\frac{B^2}{p^{(n-\tilde{w}_\chi-\hat{\kappa})(1-\ell)}}\biggl(\frac{p^{n-\tilde{w}_\chi-\hat{\kappa}}}{B}\biggr)^{-\ell}(\log p^{n-\tilde{w}})^\delta=p^r\frac{B^{2+\ell}}{p^{n-\tilde{w}_\chi-\hat{\kappa}}}(\log p^{n-\tilde{w}})^\delta.\end{aligned}$$

In light of $B\leqslant p^{n-\tilde{w}_\chi-\hat{\kappa}}$, this term is $\ll p^rB^{1+\ell}(\log p^{n-\tilde{w}})^\delta$ and is absorbed in the first term of the estimate. Summing up, we have proved that, assuming (45) and (46),

$$HS_1\ll p^r\biggl(\frac{p^{n-\tilde{w}_\chi-\hat{\kappa}}}{B}\biggr)^kB^{1+\ell}(\log p^{n-\tilde{w}})^\delta.$$

We now turn our attention to S_2, where we estimate the inner sum $S(h)$ using the p-adic exponential datum (36). This is allowable as long as

$$n-\tilde{w}_\chi-\chi_p\geqslant\hat{\kappa}+1+\iota'(12)$$

as well as

$$\begin{gathered}\kappa\geqslant1+\iota'(4),\quad\tilde{\lambda}=\min(\kappa-\rho_p(y),\lambda)\geqslant\rho_p,\\u\geqslant2\kappa-\lfloor\lambda\rfloor-\lfloor\tilde{\lambda}\rfloor+\iota'(y(y+1))+1,\end{gathered}\tag{47}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

and

$$\chi + \chi_p \geqslant \iota'(2) + \iota'(y+1) + \varepsilon(y) + 1 - \lfloor \tilde{\lambda} \rfloor.$$

Note that the final condition is required for $\chi_p \geqslant n - \tilde{w}_\chi - n_0 + 1$, so that it is satisfied as long as

$$n - \tilde{w} - n_0 \geqslant \iota'(2) + \iota'(y+1) + \varepsilon(y) - \lfloor \tilde{\lambda} \rfloor. \tag{48}$$

Assuming this to be the case, we obtain the estimate

$$|S(h)| \ll (p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}})^{1/2}\biggl(\frac{|J(h)|}{p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}} + 1\biggr) \log p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}},$$

valid for all h appearing in S_2 for which $\chi_p \leqslant n - \tilde{w}_\chi - \hat{\kappa} - 1 - \iota'(12)$. Estimating the remaining summands in S_2 trivially as $|S(h)| \leqslant B$, we thus find that

$$\begin{aligned} HS_2 &\ll H \sum_{\psi \geqslant n-\tilde{w}_\chi-n_0+1} \frac{B/H}{p^\psi}\biggl(\frac{B}{p^{(n-\tilde{w}_\chi-\hat{\kappa}-\psi)/2}} + p^{(n-\tilde{w}_\chi-\hat{\kappa}-\psi)/2}\biggr)\log p^{n-\tilde{w}} \\ &\quad + H \sum_{\psi \geqslant n-\tilde{w}_\chi-\hat{\kappa}-\iota'(12)} \frac{B/H}{p^\psi} B \\ &\ll \frac{B^2}{p^{(n-\tilde{w}_\chi-\hat{\kappa})/2}} \frac{1}{p^{(n-\tilde{w}_\chi-n_0+1)/2}} \log p^{n-\tilde{w}} \\ &\quad + Bp^{(n-\tilde{w}_\chi-\hat{\kappa})/2} \frac{1}{p^{3(n-\tilde{w}_\chi-n_0+1)/2}} \log p^{n-\tilde{w}} + \frac{B^2}{p^{n-\tilde{w}_\chi-\hat{\kappa}-\iota'(12)}} \\ &\ll BH \frac{Bp^{(n_0-1)/2+\hat{\kappa}/2} + Bp^{\iota'(12)+\hat{\kappa}} + p^{3(n_0-1)/2-\hat{\kappa}/2}}{p^{n-\tilde{w}}} \log p^{n-\tilde{w}}. \end{aligned}$$

We now arrange for our parameters to be such that this upper bound on HS_2 is no more than $BH \log p^{n-\tilde{w}}$. (Here and below, we sacrifice a small power of logarithm for no other reason but clarity.) We will initially do this for the entire range $H \leqslant B \leqslant p^{n-\tilde{w}_\chi-\rho}$; this range will be restricted in the second part of the proof, relaxing the conditions to be imposed. Letting $\mu = \max((n_0-1)/2 + \hat{\kappa}/2, \iota'(12) + \hat{\kappa})$, the condition $Bp^\mu \leqslant p^{n-\tilde{w}}$ is, in light of the range (42) for B, satisfied whenever

$$\begin{gathered} p^{-(\rho+\sigma)(k+1)/(\ell+1)}(p^{n-\tilde{w}})^{1/(\ell+1)} p^\mu \leqslant p^{n-\tilde{w}}, \\ p^{-(\rho+\sigma)(k+1)/(\ell+1)} p^\mu \leqslant (p^{n-\tilde{w}})^{\ell/(\ell+1)}. \end{gathered}$$

Along with the condition that $p^{3(n_0-1)/2-\hat{\kappa}/2} \leqslant p^{n-\tilde{w}}$, we will have that $HS_2 \ll BH \log p^{n-\tilde{w}}$ as long as (47) and (48) hold as well as

$$\begin{gathered} n - \tilde{w} \geqslant \frac{\ell+1}{2\ell}(\max(n_0 - 1 + \hat{\kappa}, 2\iota'(12) + 2\hat{\kappa})) - (\rho+\sigma)\frac{k+1}{\ell}, \\ n - \tilde{w} \geqslant \frac{3}{2}n_0 - \frac{1}{2}\hat{\kappa} - \frac{3}{2}. \end{gathered} \tag{49}$$

Collecting all contributions from the estimations of HS_1 and HS_2, we find that, in the range under consideration, and assuming (44)–(49), we have that

$$\begin{aligned} S^2 &\ll BH + H(S_1 + S_2) \\ &\ll BH \log p^{n-\tilde{w}} + p^r \biggl(\frac{p^{n-\tilde{w}-\hat{\kappa}}}{B}\biggr)^k \frac{B^{1+\ell}}{H^k} (\log p^{n-\tilde{w}})^\delta. \end{aligned} \tag{50}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

An H satisfying

$$H^{k+1} = p^r \left(\frac{p^{n-\tilde{w}-\hat{\kappa}}}{B}\right)^k B^\ell$$

would be essentially optimal. We can't make this exact choice as we are bound by the condition that H be a non-negative power of p. However, it is reasonable to seek an H to be the power of p for which

$$c_H p^{(r-1)/(k+1)} \left(\frac{p^{n-\tilde{w}-\hat{\kappa}}}{B}\right)^{k/(k+1)} B^{\ell/(k+1)} \\ = H_* < H \leqslant H^* = c_H p^{(r+k)/(k+1)} \left(\frac{p^{n-\tilde{w}-\hat{\kappa}}}{B}\right)^{k/(k+1)} B^{\ell/(k+1)},$$

with a suitable choice of $c_H > 0$, since $H^* = pH_*$. Such a choice is admissible as long as $H^* \geqslant 1$. There are several ways to ensure this; we find it convenient to invoke the condition (55) below, which will be imposed anyway. In light of this condition, we have that $n - \tilde{w} - \hat{\kappa} + 1 \geqslant (n_0 - \hat{\kappa}) + \max(n - \tilde{w} - n_0 + 1, \frac{1}{2}(n_0 - \hat{\kappa} - 1))$, with the first of the two latter expressions $\geqslant \hat{\kappa}$, so that $n - \tilde{w} - \hat{\kappa} + 1 \geqslant (n_0 - \hat{\kappa}) + \max(\frac{1}{2}(n - \tilde{w} - n_0 + \hat{\kappa} + 1), \frac{1}{2}(n_0 - \hat{\kappa} - 1)) \geqslant (n_0 - \hat{\kappa}) + \frac{1}{4}(n - \tilde{w})$. It follows that $H^* \geqslant c_H \big(p^{r+(n_0-\hat{\kappa})k} (\log p^{n-\tilde{w}})^\delta\big)^{1/(k+1)} p^{(n-\tilde{w})/(4(k+1))} / (\log p^{n-\tilde{w}})^\delta \geqslant 1$ for a sufficiently large $c_H > 1$ (depending only on the initial p-adic exponent datum in Theorem 5), since the second factor is trivially $\gg 1$, while the first factor is $\gg 1$ as seen (following Definition 2) after (16).

With such a choice of H, we have

$$\frac{r - 1 - k\hat{\kappa}}{k+1} + o_p^+ < \sigma \leqslant \frac{r + k - k\hat{\kappa}}{k+1} + o_p^+, \tag{51}$$

as well as

$$S^2 \ll p^{(r+k-k\hat{\kappa})/(k+1)} \left(\frac{p^{n-\tilde{w}}}{B}\right)^{k/(k+1)} B^{(k+\ell+1)/(k+1)} (\log p^{n-\tilde{w}})^{\max(1,\delta)}.$$

We see that this is allowable for (38) as long as

$$\tilde{r} \geqslant \frac{r + k(1 - \kappa - \iota'(y+1))}{2(k+1)}, \quad \tilde{\delta} \geqslant \frac{\max(1,\delta)}{2}. \tag{52}$$

Note that the first of these two inequalities subsumes (40). Further, the first of the two conditions (44) is subsumed in (47). The second condition can also be dispensed with if $\lambda \geqslant 2\rho_p$ or if $\chi > 0$. We could ensure the latter by imposing a lower bound on $n - \tilde{w}$, but we keep things simple and make an innocuous assumption

$$\tilde{\lambda} \geqslant 2\rho_p \tag{53}$$

to take the place of (44), with a $\tilde{\lambda}$ in place of λ with an eye on the second part of the proof.

Summing up, we have proved that the estimate (38) holds for all $0 < B \leqslant p^{n-\tilde{w}_\chi-\rho}$ (where $\rho \geqslant \hat{\kappa}$), assuming that all conditions listed in (45)–(49), (52), (53), and (55) are met.

2. The complementary range, split at $p^{(n-\tilde{w})/2}$, and conclusion. The complementary range $p^{n-\tilde{w}_\chi-\rho} < B \leqslant p^{n-\tilde{w}}$ really *should* be treated in a different way, for in this range the supposed second main term in (50) does not correctly capture the full contribution of the terms $|S(h)|$ to HS_1, because the length of summation $|J(h)|$ in $S(h)$ is unfavorably large compared with the

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

modulus $p^{n-\tilde{w}_\chi-\chi_p-\hat{\kappa}}$ already for $\chi_p=0$. This is in the nature of the method. The Weyl–van der Corput inequality (Lemma 11) has the effect of substantially reducing the modulus relative to the length of the summation; this is its intended purpose. But if the length of the summation, which remains $\asymp B$, is too large, then this effect goes too far.

One way to deal with the supplementary range, in which B is rather large compared with the modulus $p^{n-\tilde{w}}$, is to apply the p-adic exponent datum (36) and then make sure that the resulting estimate $p^{(n-\tilde{w})/2}$ is no more than (38). (This approach should be compared to the application of the Pólya–Vinogradov inequality in [BLT64] to dispense with the range $x\gg q^{2/3}$ when estimating the sum $\sum_{n\leqslant x}\chi(n)$.) This turns out to work wonderfully for $p^{n-\tilde{w}_\chi}\leqslant B\leqslant p^{n-\tilde{w}}$, requiring no adjustments to the final result, and not too badly for $p^{n-\tilde{w}_\chi-\rho}<B<p^{n-\tilde{w}_\chi}$, where the price to be paid is that one must require $\tilde{r}\geqslant(\rho+\sigma)/2+o_p\geqslant(\hat{\kappa}+\sigma)/2+o_p$, which increases the final upper bound by a factor of at least $p^{\hat{\kappa}/2}$. This would not be horrible (and it is certainly inconsequential if one is only concerned with a fixed prime p), but we can do substantially better. If we think about the proof of the datum (36), we realize that it consists of an application of the summation formula of Theorem 3, followed by a trivial estimate of the resulting shortened sum. In this light, the range $p^{n-\tilde{w}_\chi}\leqslant B\leqslant p^{n-\tilde{w}}$ corresponds dually to the range $1\leqslant B\leqslant H$, in which our estimate (38) was indeed obtained by the trivial bound. It thus becomes clear that, to avoid losses for $B<p^{n-\tilde{w}_\chi}$, we should follow the application of the summation formula not by the trivial estimate but by *exactly the same estimates* that we used in the dual range $B>H$.

At this point, we reflect back on the range considered in the first part of the proof, choose

$$\rho=\hat{\kappa},$$

and instead claim (38) *for all* $1\leqslant B\leqslant p^{(n-\tilde{w})/2}$ *and only those* B. It suffices to establish (38) for all $1\leqslant B\leqslant p^{(n-\tilde{w})/2}/b$, where $b>0$ is a suitably chosen large constant. Note that, for all B in this interval,

$$\begin{aligned}p^{n-\tilde{w}_\chi-\hat{\kappa}}&\geqslant\frac{p^{n-\tilde{w}-\hat{\kappa}}}{p^{\sigma}(p^{(n-\tilde{w})/2}/b)^{(k+\ell)/(k+1)}}\\&=p^{-\hat{\kappa}-\sigma}b^{(k+\ell)/(k+1)}(p^{n-\tilde{w}})^{(k+2-\ell)/(2(k+1))}\\&=p^{-\hat{\kappa}-\sigma}b^{(k+\ell)/(k+1)}(p^{n-\tilde{w}})^{(1-\ell)/(2(k+1))}p^{(n-\tilde{w})/2}.\end{aligned}$$

We want to ensure that the left-hand side, which is a power of p, is at least $p^{(n-\tilde{w})/2}$; for this, it suffices to ensure that the right-hand side is $>p^{(n-\tilde{w}-1)/2}$. Keeping in mind the range for σ in (51) and adjusting the constant b as necessary, we conclude that the proof of the estimate (38) in the first part covers the entire range $1\leqslant B\leqslant p^{(n-\tilde{w})/2}$ as long as

$$n-\tilde{w}\geqslant\frac{2(k+1)}{1-\ell}\left(\hat{\kappa}+\frac{r+k-k\hat{\kappa}}{k+1}-\frac{1}{2}\right)=\frac{2(r+\kappa+\iota'(y+1))+(k-1)}{1-\ell}.\tag{54}$$

As we announced, this restriction of range also allows us to relax the condition (49) somewhat. In light of $B\leqslant p^{(n-\tilde{w})/2}$, the condition $Bp^{\mu}\leqslant p^{n-\tilde{w}}$ is satisfied whenever $n-\tilde{w}\geqslant 2\mu$, so we may replace (49) with

$$n-\tilde{w}\geqslant\max\bigl(n_0-1+\hat{\kappa},2\hat{\kappa}+2\iota'(12),\tfrac{3}{2}(n_0-1)-\tfrac{1}{2}\hat{\kappa}\bigr).\tag{55}$$

We now address the case when $B\geqslant p^{(n-\tilde{w})/2}$. Instead of S, consider

$$S'=\sum_{m\in\mathbb{Z}}e\left(\frac{f(m)}{p^n}\right)h\left(\frac{m}{B}\right).$$

According to Theorem 3, assuming that

$$\begin{gathered}\kappa \geqslant 1+\iota'(4), \quad n-\tilde{w} \geqslant 1+\iota'(12),\\ u+\lfloor\lambda\rfloor > \kappa+\iota', \quad \tilde{\lambda}=\min(\kappa-\rho_p(y),\lambda)>0,\end{gathered} \tag{56}$$

we have that

$$S' = \frac{\epsilon B}{p^{(n-\tilde{w})/2}} \sum_{t\in\mathbb{Z}} e\biggl(\frac{\mathring{f}(t)}{p^n}\biggr) \hat{h}_{f,B}\biggl(\frac{t}{p^{n-\tilde{w}}/B}\biggr),$$

with $|\epsilon|=1$ and $\mathring{f}$ as in (32):

$$\mathring{f} \in \mathbf{F}(w+\operatorname{ord}_p y, y^{-1}, \kappa, \tilde{\lambda}, u+\varepsilon_\lambda-\operatorname{ord}_p y, \omega'^{-1}, -\omega^{-1}).$$

Note that $\tilde{w}' := (w+\operatorname{ord}_p y)+\kappa+\iota = w+\kappa+\iota' = \tilde{w}$. Since $p^{n-\tilde{w}}/B \leqslant p^{(n-\tilde{w})/2}$, the first part of the proof shows that sharp-cutoff sums of $e(\mathring{f}(t)/p^n)$ of length no more than $p^{n-\tilde{w}}/B$ can be estimated as in (38), as long as $\mathring{f}$ satisfies all conditions accumulated in the process of proving this estimate. Referring to (45)–(48), (52), (54) and (55), we find that we require the following additional assumptions:

$$\begin{aligned}
&\kappa \geqslant \kappa_0(y^{-1}+1,p), \quad \tilde{\lambda} \geqslant \lambda_0(y^{-1}+1,p),\\
&u+\varepsilon_\lambda-\operatorname{ord}_p y \geqslant u_0(y^{-1}+1,p,\kappa,\tilde{\lambda})+\kappa-\lfloor\tilde{\lambda}\rfloor+\iota(y),\\
&n-\tilde{w} \geqslant \varepsilon_u\biggl(\frac{2k+1-\ell}{k}(u_0(y^{-1}+1,p,\kappa,\tilde{\lambda})-\kappa+\iota'(2)+\varepsilon(y^{-1}))-\frac{\sigma'}{k}\biggr),\\
&u+\varepsilon_\lambda-\operatorname{ord}_p y \geqslant 2\kappa-2\lfloor\tilde{\lambda}\rfloor+\iota'(y^{-1}(y^{-1}+1))+1,\\
&n-\tilde{w}-n_0' \geqslant \iota'(2)+\iota'(y^{-1}+1)+\varepsilon(y^{-1})-\lfloor\tilde{\lambda}\rfloor,\\
&\tilde{r} \geqslant \frac{r+k(1-\kappa-\iota'(y^{-1}+1))}{2(k+1)},\\
&n-\tilde{w} \geqslant \frac{2(r+\kappa+\iota'(y^{-1}+1))+(k-1)}{1-\ell},\\
&n-\tilde{w} \geqslant \max\bigl(n_0'-1+\hat{\kappa}', 2\hat{\kappa}'+2\iota'(12), \tfrac{3}{2}(n_0'-1)-\tfrac{1}{2}\hat{\kappa}'\bigr),
\end{aligned} \tag{57}$$

where

$$\begin{gathered}n_0' := n_0'(y^{-1}+1,p,\kappa,\tilde{\lambda}), \quad \hat{\kappa}' := \kappa+\iota'(y^{-1}+1),\\ \frac{r-1-k\hat{\kappa}'}{k+1}+o_p^+ < \sigma' \leqslant \frac{r+k-k\hat{\kappa}'}{k+1}+o_p^+.\end{gathered}$$

Assuming that these hold, and in light of $\|\hat{h}_{f,B}\|_\star = \|\hat{h}\|_\star$, we can estimate S', using also the implication $H(\delta) \implies H^\sharp_{\mathrm{sm}}(\delta)$ of Lemma 6, as

$$S' \ll \frac{B}{p^{(n-\tilde{w})/2}} p^{\tilde{r}} B^{k/(2(k+1))} \biggl(\frac{p^{n-\tilde{w}}}{B}\biggr)^{(k+\ell+1)/(2(k+1))} (\log p^{n-\tilde{w}})^{\tilde{\delta}},$$

with a uniform implied constant depending on h only. From this it follows that

$$\begin{aligned}
S' &\ll p^{\tilde{r}}(p^{n-\tilde{w}})^{\ell/(2(k+1))} B^{(2k+1-\ell)/(2(k+1))} (\log p^{n-\tilde{w}})^{\tilde{\delta}}\\
&= p^{\tilde{r}}(p^{n-\tilde{w}})^{k/(2(k+1))} B^{(\ell+1)/(2(k+1))} (\log p^{n-\tilde{w}})^{\tilde{\delta}} \biggl(\frac{p^{n-\tilde{w}}}{B^2}\biggr)^{(\ell-k)/(2(k+1))}\\
&\ll p^{\tilde{r}} \biggl(\frac{p^{n-\tilde{w}}}{B}\biggr)^{k/(2(k+1))} B^{(k+\ell+1)/(2(k+1))} (\log p^{n-\tilde{w}})^{\tilde{\delta}}
\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

for all $B \geqslant p^{(n-\tilde{w})/2}$. Using the implication $H(\delta) \implies H_{\mathrm{sm}}(\delta)$ of Lemma 6, it follows from the first part of the proof that the same estimate also holds for all $B \leqslant p^{(n-\tilde{w})/2}$ and thus for all $1 \leqslant B \leqslant p^{n-\tilde{w}}$. The same upper bound follows for S in light of $H_{\mathrm{sm}}(\delta)^{sq} \implies H(\delta)^{sq}$ of Lemma 6, since no extra factor of $\delta_{1/2}$ appears in the power of the logarithm because the exponent pair $(k/(2(k+1)), (k+\ell+1)/(2(k+1)))$ cannot equal $(\frac{1}{2}, \frac{1}{2})$.

The stated p-adic exponent datum for $0 < k \leqslant \frac{1}{2} \leqslant \ell < 1$ follows from collecting all conditions (45)–(48), (52)–(57).

The remaining cases $k = 0$ and $\ell = 1$ follow directly by convex interpolation from bounds given by known p-adic exponent data. If $k = 0$, we interpolate between the bound (15) for the given p-adic exponent datum and the trivial bound $S \ll B$ to obtain

$$S \ll (p^r B^\ell (\log p^{n-\tilde{w}})^\delta)^{1/2} B^{1/2} = p^{r/2} B^{(\ell+1)/2} (\log p^{n-\tilde{w}})^{\delta/2}.$$

If $\ell = 1$, we use convex interpolation between the bound (15) for the first non-trivial datum (36) and the trivial bound $S \ll B$ as follows:

$$S \ll (p^{(n-\tilde{w})/2} \log p^{n-\tilde{w}})^{k/(k+1)} B^{1/(k+1)} = \left(\frac{p^{n-\tilde{w}}}{B}\right)^{k/(2(k+1))} B^{(k+2)/(2(k+1))} (\log p^{n-\tilde{w}})^{k/(k+1)}. \qquad \square$$

We comment briefly on possible optimality of the obtained value of $\tilde{n}_0$. The condition that $\tilde{n}_0 \geqslant (1+\epsilon)n_0$ with a fixed $\epsilon = \epsilon(k,\ell) > 0$ appears essential to the Weyl differencing method. We do not believe that, for example, a condition of the form $\tilde{n}_0 \geqslant n_0 + C(k,\ell)$ can suffice in general. Substantial effort was put into making $1+\epsilon$ as small as we could, but it is not clear that the factor of $\frac{3}{2}$ is necessarily optimal.

While processes engaging some 'q-variant' of the Weyl–van der Corput inequality have been used by previous authors, our approach in Theorem 5 is, to our knowledge, novel in a number of ways, including the use of the $(\frac{1}{2}, \frac{1}{2})$ pair to reduce the required $\tilde{n}_0$ and of the summation formula to shorten the sum in the range $B \gg p^{(n-\tilde{w})/2}$ and obtain what are probably nearly optimal exponents, as well as the entire paradigm of the method applying to classes of p-adic analytic functions.

6. Application to L-functions

The relevance of the class $\mathbf{F}$ to Dirichlet L-functions stems from the following (in hindsight) simple Lemma 13. In a more elementary form, this line of reasoning seems to have been first used in the context of analysis of L-functions by Postnikov [Pos55].

Recall that the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ of invertible congruence classes modulo p^n is cyclic for an odd prime p and a product of the subgroup $\{\pm 1\}$ and a cyclic group of order 2^{n-2} if $p = 2$ and $n \geqslant 2$ (we ignore the trivial case $p^n = 2$ here). Let

$$\kappa_1 = 1 + \iota'(2),$$

and let $(\mathbb{Z}/p^n\mathbb{Z})_1^\times = \{a + p^n\mathbb{Z} : a \equiv 1 \bmod p^{\kappa_1}\}$. We have that $(\mathbb{Z}/p^n\mathbb{Z})^\times = G_n \times (\mathbb{Z}/p^n\mathbb{Z})_1^\times$ with a subgroup $G_n \cong (\mathbb{Z}/p^{\kappa_1}\mathbb{Z})^\times$.

Let Γ_n denote the set of all Dirichlet characters modulo p^n, and let Γ_{n1} denote the set of all characters of the subgroup $(\mathbb{Z}/p^n\mathbb{Z})_1^\times$. We have the isomorphism of dual groups $\Gamma_n = \hat{G}_n \times \Gamma_{n1}$, and restriction to $1 + p^{\kappa_1}\mathbb{Z}$ gives a natural surjection $\Gamma_n \twoheadrightarrow \Gamma_{n1}$.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

Lemma 13. *Let $n \geqslant \kappa_1$ be given. For every $a = a_0 p^{-n} \in p^{-n}\mathbb{Z}_p$,*

$$\chi_a(1+p^{\kappa_1}t) = e(a\log_p(1+p^{\kappa_1}t)) = e\bigg(\frac{a_0\log_p(1+p^{\kappa_1}t)}{p^n}\bigg)$$

defines a character $\chi_a \in \Gamma_{n1}$. Moreover, every character of Γ_{n1} is of this form, and the correspondence $a \mapsto \chi_a$ induces an isomorphism $p^{-n}\mathbb{Z}_p/p^{-\kappa_1}\mathbb{Z}_p \cong \Gamma_{n1}$, with primitive characters being those corresponding to $p^{-n}\mathbb{Z}_p^\times/p^{-\kappa_1}\mathbb{Z}_p$.

Proof. We saw in § 2 that the series $\lambda(x) = \log_p(1+x)$ has $r_\lambda = 1$ and $M_r\lambda \doteq r$ for all $r < r_p$. Since

$$\lambda(x+y+xy) = \lambda(x) + \lambda(y)$$

for every $x, y \in B_1$, it follows that χ_a is a multiplicative function $\chi_a : 1 + p^{\kappa_1}\mathbb{Z} \to S^1$. On the other hand, since $p^{\kappa_1}t \in B_{r_p}$ for every $t \in \mathbb{Z}$, we have that

$$\mathrm{ord}_p(a\log_p(1+p^{\kappa_1}t)) = \mathrm{ord}_p(ap^{\kappa_1}t).$$

Note that $\chi_a(1+p^{\kappa_1}t) = 1$ if and only if $a\log_p(1+p^{\kappa_1}t) \in \mathbb{Z}_p$. We see that $1 + p^n\mathbb{Z} \subseteq \ker\chi_a$, so that χ_a is indeed a character of $(\mathbb{Z}/p^n\mathbb{Z})_1^\times$.

It is immediate that $a \mapsto \chi_a$ is a homomorphism of groups $p^{-n}\mathbb{Z}_p \to \Gamma_{n1}$. Moreover, we see that χ_a is the trivial character if and only if $ap^{\kappa_1}t \in \mathbb{Z}_p$ for every $t \in \mathbb{Z}$ (and in particular for $t = 1$), that is, exactly when $a \in p^{-\kappa_1}\mathbb{Z}_p$, so that we have a monomorphism $p^{-n}\mathbb{Z}_p/p^{-\kappa_1}\mathbb{Z}_p \to \Gamma_{n1}$. This must be an isomorphism since $|p^{-n}\mathbb{Z}_p/p^{-\kappa_1}\mathbb{Z}_p| = |\Gamma_{n1}| = p^{n-\kappa_1}$; in particular, every character of Γ_{n1} is of the form χ_a for some $a \in p^{-n}\mathbb{Z}_p$. Since the characters of $\Gamma_{n-1,1}$ are consequently of the form χ_a for some $a \in p^{-n+1}\mathbb{Z}_p$, the primitive characters of Γ_{n1} correspond to $a \in p^{-n}\mathbb{Z}_p^\times$. □

Lemma 13 presents a parametrization of the restrictions to $1 + p^{\kappa_1}\mathbb{Z}$ of Dirichlet characters modulo p^n by classes of p-adic rationals. The isomorphism exhibited in the Lemma extends to an isomorphism of inductive limits $\mathbb{Q}_p/p^{-\kappa_1}\mathbb{Z}_p \cong \Gamma_1^{(p)}$, with $\Gamma_1^{(p)} = \bigcup_{n=1}^\infty \Gamma_{n1}$ being the group of restrictions of all Dirichlet characters modulo all non-negative powers of p to $1 + p^{\kappa_1}\mathbb{Z}$.

Let χ be a primitive character modulo $q > 1$ ($q = p^n$ in our case). The Dirichlet L-function $L(s,\chi)$ continues to an entire function and satisfies the functional equation

$$\Big(\frac{q}{\pi}\Big)^{s/2}\Gamma\Big(\frac{s+\varsigma}{2}\Big)L(s,\chi) = \varepsilon(\chi)\Big(\frac{q}{\pi}\Big)^{(1-s)/2}\Gamma\Big(\frac{1-s+\varsigma}{2}\Big)L(1-s,\bar{\chi}),$$

where $\varsigma = 0$ or 1 according to whether χ is even or odd, and

$$\varepsilon(\chi) = \frac{i^{-\varsigma}}{\sqrt{q}}\sum_{m \bmod q}\chi(m)e\Big(\frac{m}{q}\Big)$$

is a unit multiple of the normalized Gauss sum (see [IK04, Theorem 4.15 on p. 84]). We will use the following standard expansion of $L(\frac{1}{2},\chi)$ in terms of short Dirichlet polynomials.

Lemma 14 (Approximate functional equation). *Let χ be a primitive character modulo $q > 1$, and let A be a positive integer. Then*

$$L\Big(\frac{1}{2},\chi\Big) = \sum_{m=1}^\infty \frac{\chi(m)}{\sqrt{m}}V\Big(\frac{m}{\sqrt{q}}\Big) + \varepsilon(\chi)\sum_{m=1}^\infty \frac{\overline{\chi(m)}}{\sqrt{m}}V\Big(\frac{m}{\sqrt{q}}\Big),$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

where $V(y)$ is a smooth function of $y>0$ defined by

$$V(y)=\frac{1}{2\pi i}\int_{(3)} y^{-u}\bigg(\cos\frac{\pi u}{4A}\bigg)^{-4A}\frac{\Gamma(\frac{1}{4}+\frac{u+\varsigma}{2})}{\Gamma(\frac{1}{4}+\frac{\varsigma}{2})}\,\frac{du}{u},$$

and $V(y)$ and its derivatives satisfy the estimates

$$y^aV^{(a)}(y)\ll(1+y)^{-A},\quad y^aV^{(a)}(y)=\delta_{a0}+\mathrm{O}(y^{1/6}).$$

Proof. This is an instance of [IK04, Theorem 5.3 and Proposition 5.4, pp. 98–100], with $G(u)=(\cos\pi u/4A)^{-4A}$ as on p. 99. □

We now arrive at the theorem in which a p-adic exponent datum will be used to estimate the central value $L(\frac{1}{2},\chi)$.

Theorem 6. *Suppose that $(k,\ell,r,\delta,(n_0,u_0,\kappa_0,\lambda_0))$ is a p-adic exponent datum. Let $\delta'=1$ if $\ell=k+\frac{1}{2}$, and $\delta'=0$ otherwise.*

If $\ell\geqslant k+\frac{1}{2}$, then, for every $\kappa\geqslant\max(\kappa_0(1,p),1+\iota'(2))$ and with $r=r(1,p,\kappa,\infty)$, and for every $n\geqslant\max(n_0(1,p,\kappa,\infty)+\kappa,2\kappa)$ and every primitive Dirichlet character χ modulo $q=p^n$,

$$L(\tfrac{1}{2},\chi)\ll p^{r+\kappa(1-k-\ell)}(p^n)^{[(k+\ell)/2-1/4]}(\log q)^{\delta+\delta'}.$$

If $\ell<k+\frac{1}{2}$, then, for every $\kappa\geqslant\max(\kappa_0(1,p),\lambda_0(1,p),1+\iota'(4))$ and with $r=r(1,p,\kappa,\kappa)$, and for every $n\geqslant\max(n_0(1,p,\kappa,\kappa)+\kappa,2\kappa+1+\iota'(12))$ and every primitive Dirichlet character χ modulo p^n,

$$L(\tfrac{1}{2},\chi)\ll p^{r+\kappa(1-k-\ell)}(p^n)^{[(k+\ell)/2-1/4]}(\log q)^{\delta}.$$

Proof. Using Lemma 14 with $A=2$, we can write $L(\frac{1}{2},\chi)=S+\varepsilon(\chi)S'$, where

$$S=\sum_{m=1}^{\infty}\frac{\chi(m)}{\sqrt{m}}V\bigg(\frac{m}{p^{n/2}}\bigg),\quad S'=\sum_{m=1}^{\infty}\frac{\overline{\chi(m)}}{\sqrt{m}}V\bigg(\frac{m}{p^{n/2}}\bigg).$$

We will prove an upper bound for S; the estimate on the sum S' is exactly the same with χ replaced by $\bar{\chi}$. We first consider the case $\ell\geqslant k+\frac{1}{2}$.

For every $1\leqslant c\leqslant p^\kappa$ such that $p\nmid c$, fix an integer c' with $cc'\equiv 1\ (\mathrm{mod}\ p^n)$. We can decompose S as

$$\begin{aligned}S&=\sum_{1\leqslant c\leqslant p^\kappa,p\nmid c}\ \sum_{m=0}^{\infty}\frac{\chi(c+p^\kappa m)}{\sqrt{c+p^\kappa m}}V\bigg(\frac{c+p^\kappa m}{p^{n/2}}\bigg)\\&=\sum_{1\leqslant c\leqslant p^\kappa,p\nmid c}\chi(c)\sum_{m=1}^{\infty}\chi(1+p^\kappa c'm)W_c(m)+\mathrm{O}(p^{\kappa/2})\end{aligned}$$

with the cutoff function

$$W_c(t)=\frac{1}{\sqrt{c+p^\kappa t}}V\bigg(\frac{c+p^\kappa t}{p^{n/2}}\bigg).$$

According to Lemma 13, the values of the primitive character χ modulo p^n on $1+p^{\kappa_1}\mathbb{Z}$ are given by a character χ_a for some $a=a_0p^{-n}$, $a_0\in\mathbb{Z}_p^\times$. Since $\kappa\geqslant\kappa_1$, we can write

$$S=\sum_{1\leqslant c\leqslant p^\kappa,p\nmid c}\chi(c)\sum_{m=1}^{\infty}e\bigg(\frac{a_0\log_p(1+p^\kappa c'm)}{p^n}\bigg)W_c(m)+\mathrm{O}(p^{\kappa/2}).\tag{58}$$

Recall from (13) that the phase $f_c(t) = a_0 \log_p(1 + p^\kappa c' t)$ belongs to $\mathbf{F}(\kappa, 1, \kappa, \infty, \infty, c', a_0 c')$. We estimate the inner sum $S(c)$ in (58) using a summation by parts argument similar to the one used in the proof of Lemma 6. Let

$$\tilde{S}(t) = \sum_{1 \leqslant m \leqslant t} e\biggl(\frac{f_c(m)}{p^n}\biggr)$$

if $t \geqslant 1$, and $\tilde{S}(t) = 0$ for $t < 1$. Since

$$n - \kappa \geqslant n_0, \quad \kappa \geqslant \kappa_0,$$

we can estimate $\tilde{S}(t)$ using the given p-adic exponential datum to find that

$$\tilde{S}(t) \ll p^r \biggl(\frac{p^{n-2\kappa}}{t}\biggr)^k t^\ell (\log q)^\delta \tag{59}$$

for $1 \leqslant t \leqslant p^{n-2\kappa}$, and, more generally, for all $t \geqslant 0$,

$$\tilde{S}(t) \ll p^r \biggl(p^{(n-2\kappa)k} t^{\ell-k} + \frac{t}{p^{(n-2\kappa)(1-\ell)}}\biggr)(\log q)^\delta.$$

Using summation by parts, we obtain

$$\begin{aligned} S(c) &= \int_{1-0}^{\infty} W_c(t)\, d\tilde{S}(t) = W_c(t)\tilde{S}(t)\bigg|_{1-0}^{\infty} - \int_1^\infty \tilde{S}(t) W_c'(t)\, dt \\ &\ll p^r (\log q)^\delta \int_1^\infty \biggl(p^{(n-2\kappa)k} t^{\ell-k} + \frac{t}{p^{(n-2\kappa)(1-\ell)}}\biggr) \\ &\quad \times \biggl(\frac{p^\kappa}{(c+p^\kappa t)^{3/2}}\biggl|V\biggl(\frac{c+p^\kappa t}{p^{n/2}}\biggr)\biggr| + \frac{p^{\kappa-n/2}}{\sqrt{c+p^\kappa t}}\biggl|V'\biggl(\frac{c+p^\kappa t}{p^{n/2}}\biggr)\biggr|\biggr)\, dt. \end{aligned}$$

Introducing a substitution $t = (p^{n/2}\tau - c)p^{-\kappa}$, we find that

$$S(c) \ll p^{r-n/4} (\log q)^\delta \int_{\tau_0}^\infty (p^{(n-2\kappa)(k+\ell)/2} \tau^{\ell-k} + p^{(n-2\kappa)(\ell-1/2)}\tau)\biggl(\frac{|V(\tau)|}{\tau^{3/2}} + \frac{|V'(\tau)|}{\sqrt{\tau}}\biggr)\, d\tau,$$

where $\tau_0 \geqslant p^{\kappa-n/2}$. Multiplying out the integrand, we obtain a sum of four improper integrals. In light of the asymptotic behavior of $V(\tau)$, all four of these integrals converge absolutely when extended to $(0, \infty)$ if $\ell - k > \frac{1}{2}$; in the case $\ell - k = \frac{1}{2}$, the same is true except that the integral of $|V(\tau)|\tau^{\ell-k-3/2}$ has a logarithmic singularity at zero. We thus have that

$$\begin{aligned} S(c) &\ll p^{r-n/4} (\log q)^\delta (p^{(n-2\kappa)(k+\ell)/2} (\log q)^{\delta'} + p^{(n-2\kappa)(\ell-1/2)}) \\ &\ll p^{r-(k+\ell)\kappa} (p^n)^{[(k+\ell)/2-1/4]} (\log q)^{\delta+\delta'}, \end{aligned}$$

since $(k+\ell)/2 \geqslant \ell/2 \geqslant \ell - 1/2$.

Going back to (58), we have that

$$S \ll p^{r+\kappa(1-k-\ell)} (p^n)^{[(k+\ell)/2-1/4]} (\log q)^{\delta+\delta'} + p^{\kappa/2}.$$

Since the estimate (59) holds for all $1 \leqslant t \leqslant p^{n-2\kappa}$, we know from (16) that its right-hand side is greater than $t^{1/2}$ throughout the same range. In particular, for $t = p^{n/2-\kappa}$, we find that

$$p^r (p^{n/2-\kappa})^{k+\ell} (\log q)^\delta \geqslant p^{n/4-\kappa/2},$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

from which it follows that the first term dominates in our estimate of S. This completes the proof in the case $\ell \geqslant k+\frac{1}{2}$.

If $\ell < k+\frac{1}{2}$, we apply the B-process (Theorem 4) to the given exponential datum and obtain a new datum

$$B(k,\ell,r,\delta,(n_0,u_0,\kappa_0,\lambda_0)) = \big(\ell-\tfrac{1}{2},k+\tfrac{1}{2},\tilde{r},\tilde{\delta},(\tilde{n}_0,\tilde{u}_0,\tilde{\kappa}_0,\tilde{\lambda}_0)\big),$$

where

$$\begin{gathered}\tilde{r}(1,p,\kappa,\infty) = r(1,p,\kappa,\kappa), \quad \tilde{\delta} = \delta+\delta_{01} = \delta,\\ \tilde{\kappa}_0(1,p) = \max\big(1+\iota'(4),\kappa_0(1,p),\lambda_0(1,p)\big),\\ \tilde{n}_0(1,p,\kappa,\infty) = \max\big(\kappa+1+\iota'(12),n_0(1,p,\kappa,\kappa)\big).\end{gathered}$$

Since $k+\frac{1}{2} > (\ell-\frac{1}{2})+\frac{1}{2}$, the first case of our theorem applies to this new p-adic exponent datum; this gives the stated result. □

We remark that the proof of Theorem 6 applies verbatim to estimation of the values $L(\frac{1}{2}+it,\chi)$ at any point along the critical line. Using the appropriate approximate functional equation from [IK04, Theorem 5.3 and Proposition 5.4], and denoting

$$V_s(y) = \frac{1}{2\pi i}\int_{(3)} y^{-u}\bigg(\cos\frac{\pi u}{4A}\bigg)^{-4A}\frac{\Gamma(\frac{1}{2}s+\frac{u+\varsigma}{2})}{\Gamma(\frac{1}{2}s+\frac{\varsigma}{2})}\frac{du}{u}, \quad W_c[s](t) = \frac{1}{(c+p^\kappa t)^s}V_s\bigg(\frac{c+p^\kappa t}{p^{n/2}}\bigg),$$

we find as above that

$$\begin{aligned}L\bigg(\frac{1}{2}+it,\chi\bigg) &\ll \int_1^\infty |\tilde{S}(\tau)|\bigg(\bigg|W_c\bigg[\frac{1}{2}+it\bigg]'(\tau)\bigg|+\bigg|W_c\bigg[\frac{1}{2}-it\bigg]'(\tau)\bigg|\bigg)\,d\tau+p^{\kappa/2}\\ &\ll p^{r+\kappa-n/4}(\log q)^\delta\int_{\tau_0}^\infty\big(p^{(n-2\kappa)(k+\ell)/2}\tau^{\ell-k}+p^{(n-2\kappa)(\ell-1/2)}\tau\big)\\ &\quad\times\bigg(\frac{(3+|t|)|V_{1/2+it}(\tau)|}{\tau^{3/2}}+\frac{|V'_{1/2+it}(\tau)|}{\sqrt{\tau}}\bigg)\,d\tau+p^{\kappa/2},\end{aligned}$$

with $\tau_0 \geqslant p^{\kappa-n/2}$. Using the asymptotic $y^aV_{1/2+it}^{(a)}(y) \ll (1+y/\sqrt{3+|t|})^{-A}$ and proceeding as above, we conclude that

$$\begin{aligned}L(\tfrac{1}{2}+it,\chi) &\ll (3+|t|)^{(\ell-k)/2+3/4}p^{r+\kappa-n/4+(n-2\kappa)(k+\ell)/2}(\log q)^{\delta+\delta'}\\ &\quad+(3+|t|)^{5/4}p^{r+\kappa-n/4+(n-2\kappa)(\ell-1/2)}(\log q)^\delta+p^{\kappa/2}\\ &\ll (3+|t|)^{5/4}p^{r+\kappa(1-k-\ell)}(p^n)^{[(k+\ell)/2-1/4]}(\log q)^{\delta+\delta'}.\end{aligned}$$

In the remainder of this section, we describe explicit p-adic exponent data and apply them to estimation of the central value $L(\frac{1}{2},\chi)$. The above bound (which is somewhat lossy for all non-trivial (k,ℓ) but conveniently compact), used with the same p-adic exponent data, then yields analogous estimates for $L(\frac{1}{2}+it,\chi)$ valid along the entire critical line with an explicit dependence on t, including the bound announced in the introduction.

Using Theorem 6, we can obtain a subconvex estimate on $L(\frac{1}{2},\chi)$ from every p-adic exponent datum in which $k+\ell<1$. We show how to obtain such p-adic exponent data by iterating the A- and B-processes (Theorems 5 and 4). We have seen that the p-adic exponent data can take rather complicated forms in general, to account for all the adjustments which need to be made at a finite number of special primes, possibly depending on y; the set of such primes was denoted by $P_0(y)$ in the definition of p-adic exponent data. We will, for simplicity, state our p-adic exponent

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

data in their cleanest form, in which they are valid away from finitely many primes, and state the exceptions; however, for the application to Theorem 6, it is important to remember that the method does apply to every single prime without exception.

Applying the A-process to the datum $\omega_{1/2}$, we obtain with some labor the datum

$$\begin{aligned}A(\omega_{1/2}) = AB(\omega_{01}) = \Big(&\tfrac{1}{6}, \tfrac{2}{3}, \tfrac{1}{6}(1-\kappa), \tfrac{1}{2},\\ &(\lceil \max(5\kappa-1, \varepsilon_u(\tfrac{13}{3}+\tfrac{5}{3}\kappa-3\lfloor\tilde{\lambda}\rfloor))\rceil,\\ &\max(2\kappa+\lceil\tilde{\lambda}\rceil-\lfloor\lambda\rfloor-2\lfloor\tilde{\lambda}\rfloor+1,1),1,2\rho_p)\Big)\end{aligned}$$

valid for all $p \notin \{2,3\}$ such that $\operatorname{ord}_p y = \operatorname{ord}_p(y+1) = 0$,

$$\begin{aligned}A^2B(\omega_{01}) = \Big(&\tfrac{1}{14}, \tfrac{11}{14}, \tfrac{1}{7}(1-\kappa), \tfrac{1}{2},\\ &(\lceil \max(8\kappa-3, \varepsilon_u'(3\kappa-\tfrac{9}{2}\lfloor\tilde{\lambda}\rfloor+5), \varepsilon_u(\tfrac{47}{7}\kappa+4\lceil\tilde{\lambda}\rceil-12\lfloor\tilde{\lambda}\rfloor+\tfrac{58}{7}))\rceil,\\ &\max(3\kappa+2\lceil\tilde{\lambda}\rceil-\lfloor\lambda\rfloor-4\lfloor\tilde{\lambda}\rfloor+1,1),1,2\rho_p)\Big)\end{aligned}$$

valid for all $p \notin \{2,3\}$ such that $\operatorname{ord}_p y = \operatorname{ord}_p(y+1) = \operatorname{ord}_p(y+2) = \operatorname{ord}_p(2y+1) = 0$ (ε_u' refers to the value of ε_u in the previous datum), and so on. We recall from the statement of Theorem 5 that, when constructing a new p-adic exponent datum Aq from an existing datum $q = (k, \ell, r, \delta, (n_0, u_0, \kappa_0, \lambda_0))$ using the A-process, ε_u is defined as $\varepsilon_u = 0$ if $u_0(y^{\pm}+1, p, \kappa, \tilde{\lambda}) - \kappa + \iota'(2) + \varepsilon(y^{\pm}) \leqslant 0$ and $\varepsilon_u = 1$ otherwise.

Our p-adic exponent data take an even simpler form if we restrict them to $\kappa = \tilde{\lambda}$, which is equivalent to $\lambda \geqslant \kappa$ and $\rho_p(y) = 0$. Note that this condition is always satisfied in the cases needed for Theorem 6 away from finitely many primes. Moreover, this condition 'propagates' through the recursive A- and B-processes, since a pair $(\kappa, \tilde{\lambda})$ always satisfies the condition $\kappa = \tilde{\lambda}$ away from finitely many primes (possibly depending on y) if the pair (κ, λ) does. Finally, note that, as shown below, with this restriction, every datum obtained from ω_{01} using the A- and B-processes has $u_0 = 1$; in particular, this means that, away from finitely many primes, we always have $\varepsilon_u = 0$ upon application of Theorem 5. With this convenient restriction, we thus obtain the following p-adic exponent data:

$$\begin{aligned}\omega_{01}[\kappa=\tilde{\lambda}] &= (0,1,0,0,(\kappa+1,1,1,\rho_p)),\\ &\qquad \operatorname{ord}_p y = 0,\\ B(\omega_{01})[\kappa=\tilde{\lambda}] &= (\tfrac{1}{2},\tfrac{1}{2},0,1,(\kappa+1,1,1,\rho_p)),\\ &\qquad p\notin\{2,3\}, \operatorname{ord}_p y = 0,\\ AB(\omega_{01})[\kappa=\tilde{\lambda}] &= (\tfrac{1}{6},\tfrac{2}{3},\tfrac{1}{6}(1-\kappa),\tfrac{1}{2},(5\kappa-1,1,1,2\rho_p)),\\ &\qquad p\notin\{2,3\}, \operatorname{ord}_p\{y,y+1\} = 0,\\ A^2B(\omega_{01})[\kappa=\tilde{\lambda}] &= (\tfrac{1}{14},\tfrac{11}{14},\tfrac{1}{7}(1-\kappa),\tfrac{1}{2},(8\kappa-3,1,1,2\rho_p)),\\ &\qquad p\notin\{2,3\}, \operatorname{ord}_p\{y,y+1,y+2,2y+1\} = 0,\\ A^3B(\omega_{01})[\kappa=\tilde{\lambda}] &= (\tfrac{1}{30},\tfrac{13}{15},\tfrac{1}{10}(1-\kappa),\tfrac{1}{2},(\lceil\tfrac{23}{2}\kappa-6\rceil,1,1,2\rho_p)),\\ &\qquad p\notin\{2,3\}, \operatorname{ord}_p\{y,y+1,y+2,y+3,2y+1,2y+3,3y+1,3y+2\} = 0,\\ BA^3B(\omega_{01})[\kappa=\tilde{\lambda}] &= (\tfrac{11}{30},\tfrac{8}{15},\tfrac{1}{10}(1-\kappa),\tfrac{1}{2},(\lceil\tfrac{23}{2}\kappa-6\rceil,1,1,2\rho_p)),\\ &\qquad p\notin\{2,3\}, \operatorname{ord}_p\{y,y+1,y+2,y+3,2y+1,2y+3,3y+1,3y+2\} = 0,\end{aligned}$$

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

$$\begin{aligned}ABA^3B(\omega_{01})[\kappa=\tilde{\lambda}] = (\tfrac{11}{82}, \tfrac{57}{82}, \tfrac{7}{41}(1-\kappa), \tfrac{1}{2}, (\lceil \tfrac{71}{4}\kappa - \tfrac{39}{4}\rceil, 1, 1, 2\rho_p)),&\\ p \notin \{2,3\}, \mathrm{ord}_p\{y, y+1, y+2, y+3, y+4, 2y+1, 2y+3, 2y+5,&\\ 3y+1, 3y+2, 3y+4, 3y+4, 3y+5, 4y+1, 4y+3, 5y+2, 5y+3\} = 0.&\end{aligned}$$

With a supply of p-adic exponent data, we can derive subconvex estimates on $L(\frac{1}{2},\chi)$, reflect back on our method, and prove Theorem 1. Applying Theorem 6 using the datum $AB(\omega_{01})$ and $\kappa = 1$, we get that, for every $n \geqslant 4$ and every primitive Dirichlet character χ modulo p^n with $p \notin \{2,3\}$,

$$L(\tfrac{1}{2},\chi) \ll p^{(n+1)/6}(\log p^n)^{3/2},$$

which recovers the Weyl exponent $\theta = \frac{1}{6}$ for a fixed p, as in [BLT64] and [FGM76], but with an explicit implied constant. Note that we cannot use special devices which allow one to precisely recover the Weyl exponent if one does not hope to iterate the process (as in [Hea78]). The estimate does improve upon the Burgess exponent $\theta = \frac{3}{16}$ for $n \geqslant 9$, although this is a minor point for us.

Note that, in the datum $AB(\omega_{01})$, $\frac{1}{6}+\frac{2}{3}=\frac{5}{6}$. To improve upon the Weyl exponent, we need a p-adic exponent datum with $k+\ell<\frac{5}{6}$. One such datum is provided by $ABA^3B(\omega_{01})$ above. Applying Theorem 6 with this datum and $\kappa = 1$, we get that for every $n \geqslant 8$ and every primitive Dirichlet character χ modulo p^n with $p \notin \{2,3,5,7\}$,

$$L(\tfrac{1}{2},\chi) \ll p^{7/41}(p^n)^{27/164}(\log p^n)^{1/2}. \tag{60}$$

This proves the main statement of Theorem 1,

$$L(\tfrac{1}{2},\chi) \ll p^r(p^n)^{\theta}(\log p^n)^{1/2}, \tag{61}$$

with $\theta = \frac{27}{164} < \frac{1}{6}$ and $r = \frac{7}{41}$ for all primitive characters χ modulo p^n, $p \notin \{2,3,5,7\}$, $n \geqslant 8$. Since the A- and B-processes produce p-adic exponent data effective for every prime p without exception, the same bound holds for all primitive characters χ modulo p^n also in the case $p \in \{2, 3, 5, 7\}$ for $n \geqslant n_0$, with different values of r and n_0 (and so also with the same values of r and n_0 by adjusting the implied constant). Further, a bound of the same form holds for all values of n by adjusting the value of r. Finally, if χ is induced from a primitive character χ_1 modulo p^{n_1}, $0 \leqslant n_1 \leqslant n$, then $L(s,\chi) = L(s,\chi_1)$ if $n_1 \geqslant 1$ and $L(s,\chi) = (1-p^{-s})L(s,\chi_1)$ if $n_1 = 0$, and so the statement follows also for non-primitive characters. This proves Theorem 1 for all Dirichlet characters to any prime power modulus with $\theta = \frac{27}{164}$.

Since $\frac{27}{164} \approx 0.1646 < \frac{1}{6}$, the estimate (60) breaks the Weyl exponent barrier for $n \geqslant n_0'$. As another benefit of our explicit calculations of full exponent data (including the values of n_0 and r), we can see that (60) improves on the Weyl exponent for all n for which $\frac{7}{41}+\frac{27}{164}n < \frac{1}{6}n$; this will be the case for all $n \geqslant 85$.

Note that no further improvement is obtained in (60) by taking a larger value of κ, and, equivalently, no harm is suffered by taking a smaller value of κ. This is in marked contrast to the works such as [FGM76, Hea78] in which the Weyl exponent is obtained, which essentially rely on a choice $\kappa > n/3 + \mathrm{O}(1)$. In our language, this ensures that, in appropriate ranges, $f_{\chi,h}(t)$ of Lemma 12 is essentially a quadratic polynomial; this in turn allows for a sharper treatment of one special instance of the A-process but precludes iteration. It is essential for this iterative method to adopt the exactly opposite paradigm that n is sufficiently *large* compared with κ, so that $f(t)/p^n$ behaves like a p-adic analytic function, rather than sufficiently *small* compared with κ (which presents simplifications in special cases but can obstruct the view of the analogy). It is quite possible that better (possibly substantially better) values of r and n_0 (but not θ)

in (61) can be obtained by fixing the value of κ in a range relative to n so that, by the time the iteration of A- and B-processes reaches the final application of Weyl differencing, we do have $\kappa > n/3 + \mathrm{O}(1)$ and can obtain a sharper estimate. This would be a welcome development, but we felt that it would distract from the main thrust of this paper.

The above proof, relying on Theorem 6, applies verbatim to any p-adic exponent pair (k, ℓ) and shows that the bound (61) holds with

$$\theta = \frac{k+\ell}{2} - \frac{1}{4}.$$

This brings to the fore the question of finding p-adic exponent pairs with $k + \ell$ as small as possible. It is immediate from Theorem 2 that the set of p-adic exponent pairs we can construct from $(0, 1)$ coincides with the set of (Archimedean) exponent pairs obtainable from $(0, 1)$ by the classical A- and B-processes, for which we refer to [GK91]. For example, a further specific pair which improves on (60) is Phillips's exponent pair $ABA^3BA^2BA^2B(0,1) = (\frac{97}{696}, \frac{480}{696})$ [Phi33], which gives $\theta = \frac{229}{1392} \approx 0.1645$.

The question of finding a value of θ as small as it is possible to obtain from the A- and B-processes was considered and solved by Rankin [Ran55]. Rankin proved that there is a $\theta_0 \approx 0.1645$ such that $\theta > \theta_0$ for every pair obtainable by A- and B-processes, and, conversely, for every $\theta_1 > \theta_0$, there is an exponent pair obtainable from $(0, 1)$ by A- and B-processes which yields $\theta \in (\theta_0, \theta_1)$. Our Theorem 2 shows that the corresponding p-adic processes will yield a p-adic exponent pair with the same value of θ; using Theorem 6 with this pair, we obtain a proof of Theorem 1 for any $\theta > \theta_0 \approx 0.1645$.

Acknowledgements

These results were prompted by a question posed by Kannan Soundararajan during an open problems session in a workshop on Zeta Functions and Their Riemann Hypotheses, held at the Courant Institute for Mathematical Sciences, New York University in 2002. Part of this work was done while the author visited the Centre Interfacultaire Bernoulli at the École Polytechnique Fédérale de Lausanne for the National Science Foundation-supported special semester on Group Actions in Number Theory in 2011. Most central claims and the paper as a whole took their final shape while the author visited the Max Planck Institute for Mathematics in Bonn during the 2011–12 academic year. The support and exceptional research infrastructure of both the EPFL and the Max Planck Institute for Mathematics are most gratefully acknowledged. The author also thankfully acknowledges support by the National Security Agency during the final phases of work. Finally, the author would like to thank Valentin Blomer, Gergely Harcos, and Peter Sarnak for helpful feedback.

References

BLT64 M. B. Barban, Yu. V. Linnik and N. G. Tshudakov, *On prime numbers in an arithmetic progression with a prime-power difference*, Acta Arith. **9** (1964), 375–390; MR 0171766 (30 #1993).

BEW98 B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts (Wiley, New York, 1998); MR 1625181 (99d:11092).

BM15a V. Blomer and D. Milićević, *p-adic analytic twists and strong subconvexity*, Ann. Sci. Éc. Norm. Supér. (4) **48** (2015), 561–605; MR 3377053.

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press

BM15b V. Blomer and D. Milićević, *The second moment of twisted modular L-functions*, Geom. Funct. Anal. **25** (2015), 453–516; doi: 10.1007/s00039-015-0318-7; MR 3334233.

Bou14 J. Bourgain, Decoupling, exponential sums and the Riemann zeta function, Preprint (2014), arXiv:1408.5794.

Bur63 D. A. Burgess, *On character sums and L-series. II*, Proc. Lond. Math. Soc. (3) **13** (1963), 524–536; MR 0148626 (26 #6133).

CI00 J. B. Conrey and H. Iwaniec, *The cubic moment of central values of automorphic L-functions*, Ann. of Math. (2) **151** (2000), 1175–1216; MR 1779567 (2001g:11070).

FGM76 A. Fujii, P. X. Gallagher and H. L. Montgomery, *Some hybrid bounds for character sums and Dirichlet L-series*, in *Topics in number theory (Proc. Colloq., Debrecen, 1974)*, Colloq. Math. Soc. János Bolyai, vol. 13 (North-Holland, Amsterdam, 1976), 41–57; MR 0434987 (55 #7949).

Gal72 P. X. Gallagher, *Primes in progressions to prime-power modulus*, Invent. Math. **16** (1972), 191–201; MR 0304327 (46 #3462).

GK91 S. W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums*, London Mathematical Society Lecture Note Series, vol. 126 (Cambridge University Press, Cambridge, 1991); MR 1145488 (92k:11082).

Hea78 D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions*, Invent. Math. **47** (1978), 149–170; MR 0485727 (58 #5549).

Hia14 G. A. Hiary, *Computing Dirichlet character sums to a power-full modulus*, J. Number Theory **140** (2014), 122–146; MR 3181649.

HMQ14 R. Holowinsky, R. Munshi and Z. Qi, *Character sums of composite moduli and hybrid subconvexity*, Contemp. Math., to appear. Preprint (2014), arXiv:1409.3797.

Hux05 M. N. Huxley, *Exponential sums and the Riemann zeta function. V*, Proc. Lond. Math. Soc. (3) **90** (2005), 1–41; MR 2107036 (2005h:11180).

Iwa74 H. Iwaniec, *On zeros of Dirichlet's L series*, Invent. Math. **23** (1974), 97–104; MR 0344207 (49 #8947).

IK04 H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53 (American Mathematical Society, Providence, RI, 2004); MR 2061214 (2005h:11005).

IS00 H. Iwaniec and P. Sarnak, *Perspectives on the analytic theory of L-functions*, Geom. Funct. Anal. (2000), Special Volume, Part II, 705–741, GAFA 2000 (Tel Aviv, 1999); MR 1826269 (2002b:11117).

Kat07 S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37 (American Mathematical Society, Providence, RI, 2007); MR 2298943 (2008j:12010).

Mic07 P. Michel, *Analytic number theory and families of automorphic L-functions*, in *Automorphic forms and applications*, IAS/Park City Mathematics Series, vol. 12 (American Mathematical Society, Providence, RI, 2007), 181–295; MR 2331346 (2008m:11104).

MV10 P. Michel and A. Venkatesh, *The subconvexity problem for* GL_2, Publ. Math. Inst. Hautes Études Sci. **111** (2010), 171–271; MR 2653249.

NPS14 P. D. Nelson, A. Pitale and A. Saha, *Bounds for Rankin–Selberg integrals and quantum unique ergodicity for powerful levels*, J. Amer. Math. Soc. **27** (2014), 147–191; MR 3110797.

Phi33 E. Phillips, *The zeta-function of Riemann; further developments of van der Corput's method*, Q. J. Math. **4** (1933), 209–225.

Pos55 A. G. Postnikov, *On the sum of characters with respect to a modulus equal to a power of a prime number*, Izv. Akad. Nauk SSSR. Ser. Mat. **19** (1955), 11–16; MR 0068575 (16,905f).

Ran55 R. A. Rankin, *Van der Corput's method and the theory of exponent pairs*, Q. J. Math. **6** (1955), 147–153; MR 0072170 (17,240a).

Ric06 G. Ricotta, Universality of convexity breaking exponents, in Problem Sessions: Subconvexity Bounds for L-functions (notes), 2006, http://www.aimath.org/WWN/subconvexity/subconvexity.pdf.

Rob00 A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198 (Springer, New York, 2000); MR 1760253 (2001g:11182).

Sal32 H. Salié, *Über die Kloostermanschen Summen* $S(u,v;q)$, Math. Z. **34** (1932), 91–109; MR 1545243.

Tem14 N. Templier, *Large values of modular forms*, Camb. J. Math. **2** (2014), 91–116; MR 3272013.

Tit86 E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd edition (The Clarendon Press, Oxford University Press, New York, 1986), Edited and with a preface by D. R. Heath-Brown; MR 882550 (88c:11049).

VdC22 J. G. van der Corput, *Verschärfung der Abschätzung beim Teilerproblem*, Math. Ann. **87** (1922), 39–65.

Vis13 P. Vishe, *A fast algorithm to compute* $L(1/2, f\times\chi_q)$, J. Number Theory **133** (2013), 1502–1524; MR 3007119.

Wal24 A. Walfisz, *Zur Abschätzung von* $\zeta(1/2+it)$, Nachr. Ges. Wiss. Göttingen Math.-Physik. Kl. **1924** (1924), 155–158 (in German).

Djordje Milićević dmilicevic@brynmawr.edu
Bryn Mawr College, Department of Mathematics,
101 North Merion Avenue, Bryn Mawr,
PA 19010, USA

https://doi.org/10.1112/S0010437X15007381 Published online by Cambridge University Press