Proceedings of the Royal Society of Edinburgh, **150**, 1265–1288, *2020*
DOI:10.1017/prm.2018.115

Explicit Salem sets, Fourier restriction, and metric Diophantine approximation in the *p*-adic numbers

Robert Fraser
Department of Mathematics, University of British Columbia,
Vancouver, BC V6T1Z2, Canada (rgf@math.ubc.ca)

Kyle Hambrook
Department of Mathematics and Statistics,
San Jose State University, San Jose, CA 95192, USA
(kyle.hambrook@sjsu.edu)

(MS received 18 August 2017; accepted 18 March 2018)

We exhibit the first explicit examples of Salem sets in $\mathbb{Q}_p$ of every dimension $0 < \alpha < 1$ by showing that certain sets of well-approximable p-adic numbers are Salem sets. We construct measures supported on these sets that satisfy essentially optimal Fourier decay and upper regularity conditions, and we observe that these conditions imply that the measures satisfy strong Fourier restriction inequalities. We also partially generalize our results to higher dimensions. Our results extend theorems of Kaufman, Papadimitropoulos, and Hambrook from the real to the p-adic setting.

Keywords: Hausdorff dimension; Fourier dimension; Salem sets; Fourier restriction; Metric Diophantine approximation; p-adic

2010 *Mathematics subject classification:* Primary 43A25
Secoundary 11J83; 11J61; 28A78; 28A80; 42B10

1. Introduction

1.1. Basic notation

For $x \in \mathbb{R}^d$ and $r > 0$, $|x| = \max_{1 \leqslant i \leqslant d} |x_i|$ and $B(x, r) = \left\{y \in \mathbb{R}^d : |x - y| \leqslant r\right\}$. Throughout, p denotes a fixed but arbitrary prime number and $\mathbb{Q}_p$ is the field of p-adic numbers. The basics of $\mathbb{Q}_p$ are reviewed in § 2.1. For $x \in \mathbb{Q}_p$, $|x|_p$ is the p-adic absolute value of x. For $x \in \mathbb{Q}_p^d$ and $r > 0$, $|x|_p = \max_{1 \leqslant i \leqslant d} |x_i|_p$ and $B(x, r) = \left\{y \in \mathbb{Q}_p^d : |x - y|_p \leqslant r\right\}$. The ring of integers of $\mathbb{Q}_p$ is $\mathbb{Z}_p = B(0, 1)$. The Fourier transform of a measure μ on $\mathbb{R}^d$ or $\mathbb{Q}_p^d$ is denoted $\widehat{\mu}$. Fourier analysis on $\mathbb{Q}_p^d$ is reviewed in § 2.2. The expression $X \lesssim Y$ means $X \leqslant CY$ for some positive constant C whose value may depend on p, but not on any other parameters. The expression $X \lesssim_\alpha Y$ has the same meaning, except the constant C is permitted to depend also on a parameter α. The expression $X \approx Y$ means both $X \lesssim Y$ and $Y \lesssim X$.

1.2. Salem sets and Fourier dimension: the real setting

It is well-known (see, e.g., [17, 27]) that the Hausdorff dimension $\dim_H(A)$ of a Borel set $A \subseteq \mathbb{R}^d$ can be expressed in terms of the average Fourier decay of measures on A:

$$\dim_H(A) = \sup\left\{\alpha \in [0,d] : \int_{\mathbb{R}^d} |\widehat{\mu}(\xi)|^2 |\xi|^{\alpha-d} \mathrm{d}\xi < \infty \text{ for some } \mu \in \mathcal{P}(A)\right\}, \quad (1.1)$$

where $\mathcal{P}(A)$ denotes the set of Borel probability measures on $\mathbb{R}^d$ with compact support contained in A.

The Fourier dimension $\dim_F(A)$ of a set $A \subseteq \mathbb{R}^d$ is defined in terms of the pointwise Fourier decay of measures on A:

$$\dim_F(A) = \sup\left\{\beta \in [0,d] : \sup_{0 \neq \xi \in \mathbb{R}^d} |\widehat{\mu}(\xi)|^2 |\xi|^{\beta} < \infty \text{ for some } \mu \in \mathcal{P}(A)\right\}.$$

The Fourier dimension of a Borel set is always less than or equal to its Hausdorff dimension. In general, they are not equal. In $\mathbb{R}^d$ with $d \geqslant 2$, subsets of hyperplanes must have Fourier dimension 0, but the Hausdorff dimension may be any number between 0 and $d-1$. For $d = 1$, the middle-thirds Cantor set in $\mathbb{R}$ has Fourier dimension 0 and Hausdorff dimension $\ln 2/\ln 3$. Some subtle properties of Fourier dimension are studied by Ekström, Persson, and Schmeling [16] and Fraser, Orponen, and Sahlsten [19].

A set whose Fourier and Hausdorff dimensions are equal is called a Salem set.

Points, spheres, and balls in $\mathbb{R}^d$ are Salem sets of dimension 0, $d-1$, and d, respectively. Salem sets are named for Raphaël Salem [37], who proved the existence of Salem sets in $\mathbb{R}$ of every dimension $0 < \alpha < 1$ via a construction of Cantor sets with random contraction ratios. Kahane [24] proved the existence of Salem sets in $\mathbb{R}^d$ of every dimension $0 < \alpha < d$ by considering trajectories of Brownian motion and more general stochastic processes. There are many other random constructions of Salem sets in $\mathbb{R}^d$ (see [7, 12, 15, 26, 38]).

The random constructions of Salem sets mentioned above are unsatisfactory in that they do not give *explicit* Salem sets. At best, they give families whose members are (with respect to some measure) almost all Salem sets.

Kaufman [25] was the first to give a construction of explicit Salem sets in $\mathbb{R}$ of every dimension $0 < \alpha < 1$. His construction comes from number theory and is (arguably) simpler than the random constructions mentioned above.

For $\tau \in \mathbb{R}$, the set of τ-well-approximable real numbers is

$$E(\tau) = \left\{x \in [-1,1] : |qx - r| \leqslant \max(|q|,|r|)^{-\tau} \text{ for infinitely many } (q,r) \in \mathbb{Z}^2\right\}.$$

A classic application of Dirichlet's pigeonhole principle is that $E(\tau) = [-1, 1]$ when $\tau \leqslant 1$. Jarník [22] and Besicovitch [6] proved that $E(\tau)$ has Hausdorff dimension $2/(1+\tau)$ when $\tau > 1$. Much further work has been done on metric properties of $E(\tau)$ and various generalizations of it. For details, we direct the reader to the recent works [2, 4, 5], and references therein.

Kaufman [25] proved

THEOREM 1.1 (Kaufman). *For every $\tau > 1$, $E(\tau)$ is a Salem set of Hausdorff and Fourier dimension $2/(1+\tau)$. Moreover, there exists a Borel probability measure μ supported on $E(\tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|^{-1/(1+\tau)} \ln(1+|\xi|) \quad \forall \xi \in \mathbb{R}, \quad \xi \neq 0.$$

All known constructions of explicit Salem sets in $\mathbb{R}^d$ of dimension $\alpha \notin \{0, d-1, d\}$ are based on Kaufman's construction. Bluhm [8] and Hambrook [20] generalized Kaufman's construction to show that some sets closely related to $E(\tau)$ are also Salem sets in $\mathbb{R}$. Bluhm [8] also observed that the radial set $\{x \in \mathbb{R}^d : |x| \in E(\tau)\}$ (here and nowhere else $|\cdot|$ is the Euclidean norm on $\mathbb{R}^d$) is a Salem set of dimension $d-1+2/(1+\tau)$ when $\tau > 1$. Hambrook [21] generalized Kaufman's construction to give explicit Salem sets in $\mathbb{R}^2$ of every dimension $0 < \alpha < 2$.

1.3. Salem sets and Fourier dimension: the p-adic setting

Hausdorff dimension in $\mathbb{Q}_p^d$ is defined exactly as it is in any metric space (see [27]). The formula (1.1) still holds (except $\mathbb{R}^d$ is replaced by $\mathbb{Q}_p^d$, and $|\xi|$ is replaced by $|\xi|_p$) because the proof is based on Frostman's lemma (which holds in any locally compact metric space, see [27]) and properties of the Riesz potential (which still hold in $\mathbb{Q}_p^d$, see [40]). Papadimitropoulos [34] gives the details in case $d = 1$; the proof for $d \geqslant 2$ is similar. The definitions of Fourier dimension and Salem set are as above (with the replacements mentioned).

Papadimitropoulos [36] (see also [34, 35]) adapted Salem's [37] random Cantor-type construction to prove the existence of Salem sets in $\mathbb{Q}_p$ of every dimension $0 < \alpha < 1$.

Our first main result, theorem 1.2 below, gives explicit Salem sets in $\mathbb{Q}_p$ of every dimension $0 < \alpha < 1$. It is a p-adic version of theorem 1.1.

For $\tau \in \mathbb{R}$, the set of τ-well-approximable p-adic numbers is

$$W(\tau) = \left\{x \in \mathbb{Z}_p : |xq - r|_p \leqslant \max(|q|, |r|)^{-\tau} \text{ for infinitely many } (q, r) \in \mathbb{Z}^2\right\}.$$

The set $W(\tau)$ is a p-adic analogue of $E(\tau)$. Note that the set $E(\tau)$ is unchanged if $\max(|q|, |r|)^{-\tau}$ is replaced by $|q|^{-\tau}$ in the definition. However, if the analogous replacement is made in the definition of $W(\tau)$, the set obtained equals $\mathbb{Z}_p$ for all τ.

For $\tau \leqslant 2$, $W(\tau) = \mathbb{Z}_p$ by Dirichlet's pigeonhole principle. For $\tau > 2$, Melničuk [29] (see also [10]) proved $W(\tau)$ has Hausdorff dimension $2/\tau$.

Our first main result is

THEOREM 1.2. *For every $\tau > 2$, $W(\tau)$ is a Salem set of Hausdorff and Fourier dimension $2/\tau$. Moreover, there exists a Borel probability measure μ supported on $W(\tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-1/\tau} \ln^2(1+|\xi|_p) \quad \forall \xi \in \mathbb{Q}_p, \quad \xi \neq 0.$$

Our two other main results, theorems 1.5 and 1.7, improve theorem 1.2 in different ways.

1.4. Upper regularity and Fourier restriction

To discuss our first improvement to theorem 1.2, we state a general Stein-Tomas restriction theorem.

THEOREM 1.3 (Mockenhaupt-Mitsis-Bak-Seeger). *Let* $0 < \alpha, \beta < d$. *Let* μ *be a Borel probability measure on* $\mathbb{R}^d$ *such that*

$$|\widehat{\mu}(\xi)| \lesssim_\beta |\xi|^{-\beta/2} \quad \forall \xi \in \mathbb{R}^d, \quad \xi \neq 0, \tag{1.2}$$

$$\mu(B(x,r)) \lesssim_\alpha r^\alpha \quad \forall x \in \mathbb{R}^d, \quad r > 0. \tag{1.3}$$

Then, whenever $1 \leqslant q \leqslant 1 + \beta/(4d - 4\alpha + \beta)$,

$$\|\widehat{f}\|_{L^2(\mu)} \lesssim_{\alpha,\beta,q} \|f\|_{L^q(\lambda)} \quad \forall f \in L^q(\lambda) \cap L^1(\lambda), \tag{1.4}$$

where λ *denotes Lebesgue measure on* $\mathbb{R}^d$.

Note that (1.3) is called an upper regularity or Frostman condition, and (1.4) is called a Fourier restriction inequality (see [**28**, **39**] for further background).

Theorem 1.3 was proved by Mockenhaupt [**32**] and Mitsis [**30**] for the range $1 \leqslant q < 1 + \beta/(4d - 4\alpha + \beta)$. The endpoint was proved by Bak and Seeger [**3**].

Papadimitropoulos [**34**] extended Kaufman's [**25**] proof of theorem 1.1 to obtain

THEOREM 1.4 (Papadimitropoulos). *For every* $\tau > 1$, $E(\tau)$ *is a Salem set with Hausdorff and Fourier dimension* $2/(1+\tau)$. *Moreover, there exists a Borel probability measure* μ *supported on* $E(\tau)$ *such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|^{-1/(1+\tau)} \ln(1 + |\xi|) \quad \forall \xi \in \mathbb{R}, \quad \xi \neq 0, \tag{1.5}$$

$$\mu(B(x,r)) \lesssim r^{2/(1+\tau)} \ln(1 + r^{-1}) \quad \forall x \in \mathbb{R}, \quad r > 0, \tag{1.6}$$

and, whenever $1 \leqslant q < 1 + 1/(2(1+\tau) - 3)$,

$$\|\widehat{f}\|_{L^2(\mu)} \lesssim_{q,\tau} \|f\|_{L^q(\lambda)} \quad \forall f \in L^q(\lambda) \cap L^1(\lambda), \tag{1.7}$$

where λ *denotes Lebesgue measure on* $\mathbb{R}$.

Note that Papadimitropoulos actually proved a version of theorem 1.4 with slightly weaker versions of (1.5) and (1.6). However, by modifying the proof slightly and using the reduction technique of § 3.1 below, one may obtain theorem 1.4 as stated.

By theorem 1.3, (1.7) follows from (1.5) and (1.6). The main innovation of theorem 1.4 over theorem 1.1 is the upper regularity property (1.6).

Theorem 1.3 also holds in the p-adic setting; replace $\mathbb{R}^d$ by $\mathbb{Q}_p^d$ and $|\xi|$ by $|\xi|_p$ in the statement. The proof is translated from the real to the p-adic setting by replacing bump functions with indicator functions in a straightforward way. See Papadimitropoulos [**34**] (or [**35**]) for details in the range $1 \leqslant q < 1 + \beta/(4d - 4\alpha + \beta)$. For the endpoint, as in [**3**], one appeals to the powerful abstract interpolation theorem of Carbery, Seeger, Wainger, and Wright [**11**, § 6.2].

Our second main result (and first improvement to theorem 1.2) is a p-adic version of theorem 1.4.

THEOREM 1.5. *For every $\tau > 2$, $W(\tau)$ is a Salem set with Hausdorff and Fourier dimension $2/\tau$. Moreover, there exists a Borel probability measure μ supported on $E(\tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-1/\tau} \ln^2(1 + |\xi|_p) \quad \forall \xi \in \mathbb{Q}_p, \quad \xi \neq 0, \tag{1.8}$$

$$\mu(B(x, r)) \lesssim r^{2/\tau} \ln^2(1 + r^{-1}) \quad \forall x \in \mathbb{Q}_p, \quad r > 0, \tag{1.9}$$

and, whenever $1 \leqslant q < 1 + 1/(2\tau - 3)$,

$$\|\widehat{f}\|_{L^2(\mu)} \lesssim_{q,\tau} \|f\|_{L^q(\lambda)} \quad \forall f \in L^q(\lambda) \cap L^1(\lambda), \tag{1.10}$$

where λ denotes the Haar measure on $\mathbb{Q}_p$ with $\lambda(\mathbb{Z}_p) = 1$.

By the p-adic version of theorem 1.3, (1.10) follows from (1.8) and (1.9). The main innovation of theorem 1.5 over theorem 1.2 is the upper regularity property (1.9).

Mockenhaupt [**32**] (see also [**31**]) proved a version of theorem 1.4 for the sets and measures constructed by Salem [**37**]. Mockenhaupt and Ricker [**33**] then used this theorem to establish an optimal extension of the Hausdorff-Young inequality on the torus $\mathbb{T}$ (which may be identified with $[-1, 1]$). Papadimitropoulos [**36**] (see also [**34**, **35**]) proved a version of theorem 1.5 for the sets and measures given by his p-adic analogue of Salem's construction. Papadimitropoulos used that theorem in a manner similar to that of Mockenhaupt and Ricker to establish an optimal extension of the Hausdorff-Young inequality on $\mathbb{Z}_p$.

1.5. Multiple dimensions

Our second improvement to theorem 1.2 generalizes it to multiple dimensions.

For $m, n \in \mathbb{N}$, we identify the $m \times n$ matrix whose ij-th entry is x_{ij} with the point

$$x = (x_{11}, \ldots, x_{1n}, \ldots, x_{m1}, \ldots, x_{mn}).$$

We first consider a multi-dimensional generalization of $E(\tau)$. For $\tau \in \mathbb{R}$, we define

$$E(m, n, \tau) = \left\{ x \in [-1, 1]^{mn} : \|xq - r\|_p \leqslant \max(|q|, |r|)^{-\tau} \text{ for infinitely many } (q, r) \in \mathbb{Z}^n \times \mathbb{Z}^m \right\}.$$

By Minkowski's theorem on linear forms, $E(m, n, \tau) = \mathbb{R}^{mn}$ when $\tau \leqslant n/m$. Bovey and Dodson [**10**] showed that the Hausdorff dimension of $E(m, n, \tau)$ is $m(n-1) + (m+n)/(1+\tau)$ when $\tau > n/m$. The $n = 1$ case was done earlier by Jarník [**23**] and Eggleston [**14**].

We mentioned above that Hambrook [**20**] generalized Kaufman's construction to show that certain sets in $\mathbb{R}$ closely related to $E(\tau)$ are Salem sets. In the same paper, Hambrook also considered $E(m, n, \tau)$ and proved a version of the following theorem.

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

THEOREM 1.6 (Hambrook). *For every $\tau > n/m$, there exists a Borel probability measure μ supported on $E(m, n, \tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|^{-n/(1+\tau)} \ln^n(1 + |\xi|) \quad \forall \xi \in \mathbb{R}^{mn}, \quad \xi \neq 0.$$

Technically, theorem 1.6 as stated does not appear in [20]. However, the proof of theorem 1.2 of [20] is easily modified to obtain theorem 1.6. Theorem 1.6 is not strong enough to determine whether $E(m, n, \tau)$ is a Salem set. However, it does imply that the Fourier dimension of $E(m, n, \tau)$ is at least $2n/(1 + \tau)$.

We now consider a p-adic analogue of $E(m, n, \tau)$ that is a multi-dimensional generalization of $W(\tau)$. For $\tau \in \mathbb{R}$, we define

$$W(m,n,\tau) = \left\{x \in \mathbb{Z}_p^{mn} : \|xq - r\|_p \leqslant \max(|q|, |r|)^{-\tau} \text{ for infinitely many } (q,r) \in \mathbb{Z}^n \times \mathbb{Z}^m\right\}.$$

Dirichlet's pigeonhole principle implies $W(m, n, \tau) = \mathbb{Z}_p^{mn}$ when $\tau \leqslant (m+n)/m$. Abercrombie [1] showed that the Hausdorff dimension of $W(m, n, \tau)$ is $m(n-1) + (m+n)/\tau$ when $\tau > (m+n)/m$.

Our third main result (and second improvement to theorem 1.2) is a p-adic version of theorem 1.6.

THEOREM 1.7. *For every $\tau > (m+n)/m$, there exists a Borel probability measure μ supported on $W(m, n, \tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-n/\tau} \ln^{n+1}(1 + |\xi|_p) \quad \forall \xi \in \mathbb{Q}_p^{mn}, \quad \xi \neq 0.$$

Theorem 1.7 is not strong enough to determine whether $W(m, n, \tau)$ is a Salem set. However, it does imply that the Fourier dimension of $W(m, n, \tau)$ is at least $2n/\tau$.

By modifying the proof in a straightforward way, it is possible to generalize theorem 1.7 even further along the lines of theorem 1.2 of Hambrook [20]. However, for simplicity, we do not pursue this here.

1.6. Problems for future study

PROBLEM 1.8. For $d \geqslant 2$, construct Salem sets in $\mathbb{Q}_p^d$ of every dimension $0 < \alpha < d$. The existence of such sets is unknown. Kahane's [24] stochastic constructions and Bluhm's [7] Cantor-type construction of Salem sets in $\mathbb{R}^d$ are good candidates for adaptation to the p-adic setting.

PROBLEM 1.9. Determine the Fourier dimension of $W(m, n, \tau)$ when $\tau > (m + n)/n$ and $mn > 1$. As mentioned above, the Hausdorff dimension of $W(m, n, \tau)$ is known to be $m(n-1) + (m+n)/\tau$, and theorem 1.7 implies the Fourier dimension of $W(m, n, \tau)$ is at least $2n/\tau$. By improving on the method of the present paper, perhaps it is possible to show that $\dim_F W(m, n, \tau) \geqslant m(n-1) + (m+n)/\tau$, hence proving that $W(m, n, \tau)$ is Salem. Note that this would also resolve problem 1.8. On the other hand, it would be interesting to obtain an upper bound on $\dim_F W(m, n, \tau)$ that is strictly less than the Hausdorff dimension, as such upper bounds appear to be difficult. The analogous problem for $E(m, n, \tau)$ is also open.

PROBLEM 1.10. Prove an analogue of theorem 1.5 for $W(m, n, \tau)$. In other words, prove theorem 1.7 with an analogue of the upper regularity property (1.9) (an analogue of (1.10) would follow immediately from the p-adic version of theorem 1.3). The analogue of the upper regularity property (1.9) would take the form

$$\mu(B(x,r)) \lesssim r^{\alpha} \quad \forall x \in \mathbb{Q}_p^{mn}, \quad r > 0.$$

In the case $m > n = 1$, the best possible exponent α is $\alpha = (m+1)/\tau$. The method of proof of theorem 1.5 can be extended to obtain this, but we must assume $\tau > (m+1)/m + 1 - 1/m^2$. In full range $\tau > (m+1)/m$, we are only able to obtain $\alpha = m/\tau$. The case $n > 1$ is completely open. The analogous problem for $E(m, n, \tau)$ is also interesting to consider.

PROBLEM 1.11. Prove versions of theorems 1.2, 1.5, and theorem (1.7) in the setting of an arbitrary ultrametric local field. Note that every local field is isomorphic to either $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$ (for some prime p), a finite extension of $\mathbb{Q}_p$ (for some prime p), or the field of formal Laurent series over some finite field, and $\mathbb{R}$ and $\mathbb{C}$ are not ultrametric. Papadimitropoulos [**34**, **35**] extended Salem's [**37**] random Cantor-type construction to prove, for any ultrametric local field K, the existence of Salem sets of every dimension $0 < \alpha < 1$ in K. Moreover, Papadimitropoulos [**34**, **35**] proved a version of theorem 1.5 in K for the sets and measures produced by his construction.

1.7. Structure of the paper

In § 2, we review the definition and basics properties of the p-adic numbers as well as the necessary elements of Fourier analysis on the p-adics. In §§ 3 and 4, we prove theorems 1.5 and 1.7, respectively. Theorem 1.2 is an immediate corollary of both theorem 1.5 and 1.7.

1.8. Remarks on the proofs

The proof of theorem 1.5 is a reasonably straightforward adaptation of Papadimitropoulos 's [**34**] proof of theorem 1.4, which in turn is an extension of Kaufman's [**25**] proof of theorem 1.1, from the real to the p-adic setting. In essence, the adaptation strategy is to replace a bump function that is 1 on $[-1, 1] = B(0, 1) \subseteq \mathbb{R}$ by the indicator function of $\mathbb{Z}_p = B(0, 1) \subseteq \mathbb{Q}_p$. The details, however, are not completely straightforward. In establishing (1.8), we encounter (in the proof of lemma 3.3 below) a non-trivial exponential sum. We estimate the exponential sum by a method inspired by theorem 1 in Cilleruelo and Garaev's paper [**13**]. No such obstacle is encountered in the real setting. Establishing (1.9) is also somewhat different than in the real setting because of the unusual geometry of the p-adic numbers.

Note that the reduction technique of § 3.1 below, while simple, appears to be new. It allows us to obtain the strong Fourier decay and upper regularity inequalities (1.8) and (1.9) without the averaging technique of Kaufman [**25**]. Using Kaufman's averaging technique would make proving (1.9), even in a weaker form, significantly more complicated. Papadimitropoulos [**34**] did not use Kaufman's averaging argument to prove his version of theorem 1.4, which (as we mentioned above) has weaker forms of (1.8) and (1.9).

The proof of theorem 1.7 is a generalization of the proof of theorem 1.5 (without the upper regularity property (1.9)), following the ideas of [20].

2. The field $\mathbb{Q}_p$ of p-adic numbers

2.1. Definition and basic properties

Every non-zero $x \in \mathbb{Q}$ can be expressed uniquely in the form $x = p^M a/b$ where a, b, M are integers with a and b coprime to p and $b \geqslant 1$. The p-adic absolute value of x is defined to be $|x|_p = p^{-M}$. We define $|0|_p = 0$. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is the field of p-adic numbers $\mathbb{Q}_p$. Every non-zero $x \in \mathbb{Q}_p$ can be expressed uniquely in the form

$$x = \sum_{j=M}^{\infty} c_j p^j, \tag{2.1}$$

where $M \in \mathbb{Z}$, $c_j \in \{0, 1, \ldots, p-1\}$, and $c_M \neq 0$. We call (2.1) the p-adic expansion of x. The p-adic absolute value of x is $|x|_p = p^{-M}$. This extends the definition of the p-adic absolute value from $\mathbb{Q}$ to $\mathbb{Q}_p$. It is sometimes helpful to know that $|x|_p \geqslant |x|^{-1}$ for all non-zero $x \in \mathbb{Z}$.

The p-adic norm of $x \in \mathbb{Q}_p^d$ is $|x|_p = \max_{1 \leqslant i \leqslant d} |x_i|_p$.

The closed ball with radius $r > 0$ and centre $a \in \mathbb{Q}_p^d$ is $B(a, r) = \{x \in \mathbb{Q}_p^d : |x - a|_p \leqslant r\}$. Since the p-adic norm takes values in $\{p^k : k \in \mathbb{Z}\} \cup \{0\}$, it follows that $B(a, r) = \{x \in \mathbb{Q}_p^d : |x - a|_p \leqslant p^k\} = \{x \in \mathbb{Q}_p^d : |x - a|_p < p^{k+1}\}$ whenever $p^k < r \leqslant p^{k+1}$, and that the indicator function $\mathbf{1}_{B(a,r)}$ is continuous. Analogous statements hold for the open ball $B(a, r^-) = \{x \in \mathbb{Q}_p^d : |x - a|_p < r\}$.

The p-adic norm satisfies a strong form of the triangle inequality:

$$|x - y|_p \leqslant \max(|x|_p, |y|_p) \quad \forall x, y \in \mathbb{Q}_p, \text{ with equality whenever } |x|_p \neq |y|_p.$$

This inequality is called the ultrametric inequality. It may also be called the acute isosceles triangle inequality because it means precisely that for each x, $y \in \mathbb{Q}_p^d$ the two largest of $|x|_p$, $|y|_p$, $|x - y|_p$ are equal.

The ultrametric inequality implies two important properties of balls in $\mathbb{Q}_p^d$. First, for all a, $a' \in \mathbb{Q}_p^d$ and all $0 < r \leqslant r'$, $B(a, r) \cap B(a', r') \neq \emptyset$ if and only if $B(a, r) \subseteq B(a', r')$. In other words, two balls intersect if and only if the larger contains the smaller. The second property is that, for all integers $j < k$, every ball in $\mathbb{Q}_p^d$ of radius p^k is the union of $p^{d(k-j)}$ balls of radius p^j. Indeed, for every $x \in \mathbb{Q}_p^d$, we have $B(x, p^k) = \bigcup_y B(x + yp^{-k}, p^j)$, where the union is over all $y \in \mathbb{Q}_p^d$ such that $y_i \in \{0, 1, \ldots, p^{k-j} - 1\}$ for $i = 1, \ldots, d$. From these properties, it follows that every ball in $\mathbb{Q}_p^d$ is compact; hence, $\mathbb{Q}_p^d$ is locally compact.

The closed unit ball in $\mathbb{Q}_p$, $B(0, 1) = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$, is called the ring of p-adic integers and is denoted $\mathbb{Z}_p$. Thus $\mathbb{Z}_p^d = B(0, 1) = \{x \in \mathbb{Q}_p^d : |x|_p \leqslant 1\}$.

For nonzero $x \in \mathbb{Q}_p$ with p-adic expansion (2.1), the p-adic fractional part of x is defined to be $\{x\}_p = \sum_{j=M}^{-1} c_j p^j$. We define $\{0\}_p = 0$. For nonzero $x \in \mathbb{Q}_p$ with p-adic expansion (2.1), the p-adic integral part of x is defined to be $[x]_p = \sum_{j=0}^{\infty} c_j p^j$.

We define $[0]_p = 0$. Notice $x = \{x\}_p + [x]_p$ for all $x \in \mathbb{Q}_p$. Moreover, $x \in \mathbb{Z}_p$ if and only if $\{x\}_p = 0$, which is the case if and only if $[x]_p = x$. For all $x \in \mathbb{R}$, define

$$e(x) = e^{-2\pi i x}.$$

For all x, $y \in \mathbb{Q}_p$, $\{x\}_p + \{y\}_p$ differs from $\{x + y\}_p$ by an integer, and so

$$e(\{x\}_p + \{y\}_p) = e(\{x + y\}_p). \tag{2.2}$$

We identify $\mathbb{Q}_p/\mathbb{Z}_p$ with the set $\{x \in \mathbb{Q}_p : [x]_p = 0\} \subseteq \mathbb{Q} \cap [0, 1)$.

2.2. Fourier analysis on $\mathbb{Q}_p^d$

We review here the necessary elements of Fourier analysis on $\mathbb{Q}_p^d$. The books by Folland [**18**] and Taibleson [**40**] are excellent general references on the subject.

The additive group $(\mathbb{Q}_p^d, +)$ is a commutative locally compact Hausdorff topological group. We denote by λ the unique Haar measure on $\mathbb{Q}_p^d$ that assigns measure p^{dk} to every closed ball of radius p^k, $k \in \mathbb{Z}$. Integration with respect to λ is indicated by $\mathrm{d}x$. The Haar measure satisfies the following scaling property: $d(ax) = |a|_p^d \, \mathrm{d}x$ for all $a \in \mathbb{Q}_p$. The Haar measure on $\mathbb{Q}_p^d$ is the d-fold product of the corresponding Haar measure on $\mathbb{Q}_p$.

The characters on a commutative locally compact Hausdorff topological group are the continuous homomorphisms from the group to the unit circle in $\mathbb{C}$ (which is a group under multiplication). By (2.2), $x \mapsto e(\{x \cdot s\}_p)$ is a character on $\mathbb{Q}_p^d$ for every fixed $s \in \mathbb{Q}_p^d$. In fact, every character on $\mathbb{Q}_p^d$ is of this form.

If $f : \mathbb{Q}_p^d \to \mathbb{C}$ is integrable, the Fourier transform of f is

$$\widehat{f}(s) = \int_{\mathbb{Q}_p^d} e(\{x \cdot s\}_p) f(x) \, \mathrm{d}x \quad \forall s \in \mathbb{Q}_p^d.$$

If μ is a finite Borel measure on $\mathbb{Q}_p^d$, the Fourier transform of μ is

$$\widehat{\mu}(s) = \int_{\mathbb{Q}_p^d} e(\{x \cdot s\}_p) \, \mathrm{d}\mu(x) \quad \forall s \in \mathbb{Q}_p^d.$$

The Haar measure on $\mathbb{Z}_p^d$ is the restriction of the Haar measure on $\mathbb{Q}_p^d$. Every character on $\mathbb{Z}_p^d$ has the form $x \mapsto e(\{x \cdot s\}_p)$ for some $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^d$. If $f : \mathbb{Z}_p^d \to \mathbb{C}$ is integrable, the Fourier transform of f is

$$\widehat{f}(s) = \int_{\mathbb{Z}_p^d} e(\{x \cdot s\}_p) f(x) \, \mathrm{d}x \quad \forall s \in (\mathbb{Q}_p/\mathbb{Z}_p)^d.$$

If μ is a finite Borel measure on $\mathbb{Z}_p^d$, the Fourier transform of μ is

$$\widehat{\mu}(s) = \int_{\mathbb{Z}_p^d} e(\{x \cdot s\}_p) \, \mathrm{d}\mu(x) \quad \forall s \in (\mathbb{Q}_p/\mathbb{Z}_p)^d.$$

We now present two lemmas that we will need. The first is a simple calculation.

Lemma 2.1. *For every $k \in \mathbb{Z}$, $a \in \mathbb{Q}_p^d$, and $s \in \mathbb{Q}_p^d$, we have*

$$\int_{B(a,p^{-k})} e(\{s \cdot x\}_p)\, \mathrm{d}x = \begin{cases} p^{-dk} e(\{s \cdot a\}_p) & \text{if } |s|_p \leqslant p^k \\ 0 & \text{if } |s|_p > p^k. \end{cases} \tag{2.3}$$

Proof. By a change of variable,

$$\int_{B(a,p^{-k})} e(\{s \cdot x\}_p)\, \mathrm{d}x = p^{-dk} e(\{s \cdot a\}_p) \int_{B(0,1)} e(\{p^k s \cdot x\}_p)\, \mathrm{d}x,$$

so it will suffice to prove (2.3) when $a = 0$ and $k = 0$. As the $d > 1$ case follows from the $d = 1$ case, we will also assume $d = 1$. If $|s|_p \leqslant 1$, then $\{sx\}_p = 0$ for all $x \in B(0, 1)$, and so $\int_{B(0,1)} e(\{sx\}_p)\, \mathrm{d}x = 1$. Now suppose $|s|_p > 1$. By first making a change of variable and then using that $B(-1, 1) = B(0, 1)$, we get

$$\int_{B(0,1)} e(\{sx\}_p)\, \mathrm{d}x = e(\{s\}_p) \int_{B(-1,1)} e(\{sx\}_p)\, \mathrm{d}x = e(\{s\}_p) \int_{B(0,1)} e(\{sx\}_p)\, \mathrm{d}x.$$

Therefore, since $e(\{s\}_p) \neq 1$, we must have $\int_{B(0,1)} e(\{sx\}_p)\, \mathrm{d}x = 0$. □

The second lemma says that the Fourier transform of a finite Borel measure on $\mathbb{Q}_p^d$ with support contained in $\mathbb{Z}_p^d$ is completely determined by its values at points $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^d$.

Lemma 2.2. *Let μ be a finite Borel measure on $\mathbb{Q}_p^d$ with support contained in $\mathbb{Z}_p^d$. Then*

$$\widehat{\mu}(s) = \widehat{\mu}((\{s_1\}_p, \ldots, \{s_d\}_p)) \quad \forall s \in \mathbb{Q}_p^d,$$

and (consequently) $\widehat{\mu}$ is constant on balls of radius 1.

Proof. We assume $d = 1$. The proof when $d > 1$ is similar. Let $s \in \mathbb{Q}_p$. If $x \in \mathbb{Z}_p$, then $x[s]_p \in \mathbb{Z}_p$, and hence $e(\{x[s]_p\}_p) = 1$. Combining this observation with (2.2) gives

$$\widehat{\mu}(s) = \widehat{\mu}(\{s\}_p + [s]_p) = \int_{\mathbb{Z}_p} e(\{x\{s\}_p\}_p) e(\{x[s]_p\}_p)\, \mathrm{d}\mu(x) = \widehat{\mu}(\{s\}_p).$$

□

3. Proof of theorem 1.5

3.1. Reduction

We show here that to prove theorem 1.5 it suffices to prove the following seemingly weaker theorem.

THEOREM 3.1. *Let g be a non-negative non-decreasing function defined on $(0, \infty)$ such that $\lim_{x\to\infty} g(x) = \infty$. For every $\tau > 2$, there exists a Borel probability measure μ supported on $W(\tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-1/\tau} \ln^2(1 + |\xi|_p) g(|\xi|_p) \quad \forall \xi \in \mathbb{Q}_p, \quad \xi \neq 0. \tag{3.1}$$

$$\mu(B(x, r)) \lesssim r^{2/\tau} \ln(1 + r^{-1}) g(r^{-1}) \quad \forall x \in \mathbb{Q}_p, \quad r > 0. \tag{3.2}$$

We emphasize that the constant implied by $\lesssim$ does not depend on g.

We prove theorem 3.1 in § 3.2.

Proof that theorem 3.1 implies theorem 1.5. Let $\tau > 2$. For each $k \in \mathbb{N}$, theorem 3.1 gives a probability measure μ_k supported on $W(\tau)$ that satisfies (3.1) and (3.2) with μ and $g(t)$ replaced by μ_k and $\ln^{1/k}(1 + t)$, respectively. By Prohorov's theorem (see [**9**, vol.2, p.202]), the sequence $(\mu_k)_{k=1}^{\infty}$ has a subsequence $(\mu_{k_j})_{j=1}^{\infty}$ which converges weakly (that is, in distribution) to a probability measure μ. Therefore $\widehat{\mu}(\xi) = \lim_{j\to\infty} \widehat{\mu_{k_j}}(\xi)$ for all $\xi \in \mathbb{Q}_p$, and $\mu(B(x, r)) = \lim_{j\to\infty} \mu_{k_j}(B(x, r))$ for all $x \in \mathbb{Q}_p$, $r > 0$ (because $B(x, r)$ is both open and closed). It follows that μ satisfies (1.8) and (1.9) because $\lim_{k\to\infty} \ln^{1/k}(1 + t) = 1$ for any fixed $t > 0$. This proves theorem 1.5. □

3.2. Proof of theorem 3.1

Let $\tau > 2$. Let g be any non-negative non-decreasing function defined on $(0, \infty)$ such that $\lim_{x\to\infty} g(x) = \infty$. For each $M \in \mathbb{N}$, define

$$Q_M = \left\{ q \in \mathbb{Z} : \frac{1}{2} p^M \leqslant q < p^M,\ |q|_p = 1,\ q \text{ prime} \right\},$$
$$R_M = \left\{ r \in \mathbb{Z} : 0 \leqslant r < p^M \right\}.$$

Note that Q_M is non-empty unless $p = 2$ and $M = 1$. For everything that follows, we make the standing assumption that $M \geqslant 2$ if $p = 2$. For each $q \in Q_M$ and $r \in R_M$, define the function $\phi_{q,r}$ on $\mathbb{Z}_p$ by

$$\phi_{q,r}(x) = p^{\lceil \tau M \rceil} \mathbf{1}_{B(0,1)}(p^{-\lceil \tau M \rceil}(xq - r)) \quad \forall x \in \mathbb{Z}_p.$$

For each $M \in \mathbb{N}$, define the function F_M on $\mathbb{Z}_p$ by

$$F_M(x) = |Q_M|^{-1} |R_M|^{-1} \sum_{q \in Q_M} \sum_{r \in R_M} \phi_{q,r}(x) \quad \forall x \in \mathbb{Z}_p.$$

Choose a strictly increasing sequence of non-negative integers $(M_k)_{k=0}^{\infty}$ such that for all $k \in \mathbb{N}$

$$\lceil \tau M_{k-1} \rceil < M_k, \tag{3.3}$$

$$p^{\lceil \tau M_{k-1} \rceil} < g(p^{M_k}), \tag{3.4}$$

$$\prod_{i=1}^{k-1} \frac{p^{\lceil \tau M_i \rceil}}{|Q_{M_i}||R_{M_i}|} < g(p^{M_k}). \tag{3.5}$$

Let ψ_0 be any non-negative function on $\mathbb{Z}_p$ such that

$$\widehat{\psi_0}(0) = 1, \tag{3.6}$$

$$\widehat{\psi_0}(s) = 0 \quad \text{for all } s \in \mathbb{Q}_p/\mathbb{Z}_p \text{ with } |s|_p > p^{\lceil \tau M_0 \rceil}, \tag{3.7}$$

$$\psi_0(x) = 0 \quad \text{for all } x \in \mathbb{Z}_p \text{ with } |x|_p \leqslant p^{-\lceil \tau M_1 \rceil} \text{ or } |x|_p = 1, \tag{3.8}$$

$$\|\psi_0\|_\infty < \infty. \tag{3.9}$$

In light of lemma 2.1, we may choose, for example,

$$\psi_0 = (p^{-1} - p^{-2})^{-1}(\mathbf{1}_{B(0,p^{-1})} - \mathbf{1}_{B(0,p^{-2})}).$$

For each $k \in \mathbb{N}$, define the measure μ_k on $\mathbb{Z}_p$ by

$$\mathrm{d}\mu_k(x) = \psi_0(x) F_{M_1}(x) \cdots F_{M_k}(x)\, \mathrm{d}x.$$

For convenience in lemma 3.4 below, we define $\mathrm{d}\mu_{-1}(x) = \mathrm{d}\mu_0(x) = \psi_0(x)\, \mathrm{d}x$.

To construct the measure μ and prove that it satisfies (3.1), we need the following sequence of lemmas.

LEMMA 3.2. *For all $M \in \mathbb{N}$, $q \in Q_M$, $r \in R_M$, and $s \in \mathbb{Q}_p/\mathbb{Z}_p$,*

$$\widehat{\phi_{q,r}}(s) = \begin{cases} e(\{rs/q\}_p) & \text{if } |s|_p \leqslant p^{\lceil \tau M \rceil} \\ 0 & \text{if } |s|_p > p^{\lceil \tau M \rceil} \end{cases}$$

LEMMA 3.3. *For all $M \in \mathbb{N}$ and $s \in \mathbb{Q}_p/\mathbb{Z}_p$,*

$$\widehat{F_M}(s) = 1 \qquad \text{if } s = 0 \tag{3.10}$$

$$\widehat{F_M}(s) = 0 \qquad \text{if } 0 < |s|_p \leqslant p^M \tag{3.11}$$

$$|\widehat{F_M}(s)| \lesssim |s|^{-1/\tau} \ln^2(|s|_p) \qquad \text{if } p^M < |s|_p \leqslant p^{\lceil \tau M \rceil} \tag{3.12}$$

$$\widehat{F_M}(s) = 0 \qquad \text{if } |s|_p > p^{\lceil \tau M \rceil} \tag{3.13}$$

LEMMA 3.4. *For all integers $k \geqslant 0$ and all $s \in \mathbb{Q}_p/\mathbb{Z}_p$,*

$$\widehat{\mu_k}(s) = 1 \qquad \text{if } s = 0 \tag{3.14}$$

$$\widehat{\mu_k}(s) = \widehat{\mu_{k-1}}(s) \qquad \text{if } 0 < |s|_p \leqslant p^{M_k} \tag{3.15}$$

$$|\widehat{\mu_k}(s)| \lesssim |s|^{-1/\tau} \ln^2(|s|_p) g(|s|_p) \qquad \text{if } p^{M_k} < |s|_p \leqslant p^{\lceil \tau M_k \rceil} \tag{3.16}$$

$$\widehat{\mu_k}(s) = 0 \qquad \text{if } |s|_p > p^{\lceil \tau M_k \rceil} \tag{3.17}$$

Lemma 3.2 is an immediate corollary of lemma 2.1. The proofs of lemmas 3.3 and 3.4 are given in §§ 3.3 and 3.4, respectively.

Note that (3.14) implies that each μ_k is a probability measure. By Prohorov's theorem (see [**9**, vol. 2, p. 202]), the sequence $(\mu_k)_{k=1}^{\infty}$ has a subsequence that converges weakly (that is, in distribution) to a probability measure μ. Though μ is technically a measure on $\mathbb{Z}_p$, it extends to a measure on $\mathbb{Q}_p$ by defining $\mu(A) = \mu(A \cap \mathbb{Z}_p)$ for $A \subseteq \mathbb{Q}_p$.

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

Since

$$\operatorname{supp}(F_{M_k}) = \left\{x \in \mathbb{Z}_p : |xq - r|_p \leqslant p^{-\lceil \tau M_k \rceil} \text{ for some } (q, r) \in Q_{M_k} \times R_{M_k}\right\}$$

for any $k \in \mathbb{N}$, and since (3.3) implies that $Q_{M_k} \times R_{M_k}$ and $Q_{M_{k'}} \times R_{M_{k'}}$ are disjoint for any two k, $k' \in \mathbb{N}$, we have

$$\operatorname{supp}(\mu) \subseteq \bigcap_{k=1}^{\infty} \operatorname{supp}(F_{M_k}) \subseteq W(\tau).$$

By (3.7) and (3.15)–(3.17),

$$|\widehat{\mu}(s)| \leqslant \sup_{k\in\mathbb{N}} |\widehat{\mu_k}(s)| \lesssim |s|_p^{-1/\tau} \ln^2(|s|_p) g(|s|_p) \quad \forall s \in \mathbb{Q}_p/\mathbb{Z}_p, \quad s \neq 0.$$

An application of lemma 2.2 shows that μ satisfies (3.1).

Now we move on to proving (3.2).

Since μ is a probability measure supported on $\mathbb{Z}_p$, and since every closed ball in $\mathbb{Z}_p$ can be written in the form $B(x, p^{-\ell})$ with $x \in \mathbb{Z}_p$ and $\ell \in \mathbb{Z}$, $\ell \geqslant 0$, it suffices to prove

$$\mu(B(x, p^{-\ell})) \lesssim p^{-2\ell/\tau} \ln(1 + p^{\ell}) g(p^{\ell}) \quad \forall x \in \mathbb{Z}_p, \quad \ell \in \mathbb{Z}, \quad \ell \geqslant 0.$$

We can reduce things further. If $x \in \mathbb{Z}_p$ and $0 \leqslant \ell \leqslant \lceil \tau M_0 \rceil$, then

$$\mu(B(x, p^{-\ell})) \leqslant 1 \leqslant p^{2\lceil \tau M_0 \rceil/\tau} p^{-2\ell/\tau} \lesssim p^{-2\ell/\tau} \ln(1 + p^{\ell}) g(p^{\ell}),$$

and we are done. Thus we can assume $\lceil \tau M_{j-1} \rceil < \ell \leqslant \lceil \tau M_j \rceil$ for some integer $j \geqslant 1$. Moreover, since μ is the weak limit of a subsequence of $(\mu_k)_{k=1}^{\infty}$ and $B(x, p^{-\ell})$ is both open and closed, we know $\mu(B(x, p^{-\ell}))$ is the limit of a subsequence of $(\mu_k(B(x, p^{-\ell})))_{k=1}^{\infty}$. Therefore, to prove (3.2), it suffices to prove

Lemma 3.5. *For all $x \in \mathbb{Z}_p$ and j, $\ell \in \mathbb{N}$ with $\lceil \tau M_{j-1} \rceil < \ell \leqslant \lceil \tau M_j \rceil$ there is a $k_0(x, j, \ell) > 0$ such that*

$$\mu_k(B(x, p^{-\ell})) \lesssim p^{-2\ell/\tau} \ln(p^{\ell}) g(p^{\ell}) \tag{3.18}$$

for all integers $k \geqslant k_0(x, j, \ell)$.

We will prove lemma 3.5 with $k_0(x, j, \ell) = j$.

We introduce the following definitions. For $k \in \mathbb{N}$, $P_k = F_{M_1} \cdots F_{M_k}$ and any ball of the form $B(r/q, p^{-\lceil \tau M_k \rceil})$ with $(q, r) \in Q_{M_k} \times R_{M_k}$ will be called a k-ball.

We will need the following four lemmas.

Lemma 3.6. *If (q, r), $(q', r') \in Q_M \times R_M$ with $r/q \neq r'/q'$, then*

$$\left|\frac{r}{q} - \frac{r'}{q'}\right|_p > p^{-2M}.$$

Proof. Since $|q|_p = |q'|_p = 1$, $rq' \neq r'q$, and $0 \leqslant r, q, r', q' < p^M$, we have

$$\left|\frac{r}{q} - \frac{r'}{q'}\right|_p = |rq' - r'q|_p \geqslant |rq' - r'q|^{-1} > p^{-2M}.$$

□

LEMMA 3.7. *For every $M \in \mathbb{N}$,*

$$F_M(x) \leqslant \frac{p^{\lceil \tau M \rceil}}{|Q_M||R_M|} \quad \forall x \in \mathbb{Z}_p, \quad p^{-\lceil \tau M \rceil} < |x|_p < 1. \tag{3.19}$$

Proof. Fix $x \in \mathbb{Z}_p$ with $p^{-\lceil \tau M \rceil} < |x|_p < 1$. Since

$$F_M(x) = \frac{1}{|Q_M||R_M|} \sum_{(q,r) \in Q_M \times R_M} p^{\lceil \tau M \rceil} \mathbf{1}_{B(r/q, p^{-\lceil \tau M \rceil})}(x),$$

it suffices to prove that the sum can have most one non-zero term. Thus, seeking a contradiction, suppose there are two pairs $(q, r) \neq (q', r')$ in $Q_M \times R_M$ such that $x \in B(r/q, p^{-\lceil \tau M \rceil}) \cap B(r'/q', p^{-\lceil \tau M \rceil})$. This implies $|r/q - r'/q'|_p \leqslant p^{-\lceil \tau M \rceil}$. Then lemma 3.6 gives $r/q = r'/q'$. Since $(q, r) \neq (q', r')$, we must have $q \neq q'$. Then, because q and q' are primes, the number $r/q = r'/q'$ must be an integer. Furthermore, since $0 \leqslant r, r' < p^M$ and $1/2p^M \leqslant q, q'$, we have either $r/q = r'/q' = 0$ or $r/q = r'/q' = 1$. Thus $x \in B(0, p^{-\lceil \tau M \rceil})$ or $x \in B(1, p^{-\lceil \tau M \rceil})$. Both possibilities contradict that $p^{-\lceil \tau M \rceil} < |x|_p < 1$. □

LEMMA 3.8. *Let $x \in \mathbb{Z}_p$ and $j, \ell \in \mathbb{N}$ with $\ell \leqslant \lceil \tau M_j \rceil$. Let J be the number of j-balls that intersect $B(x, p^{-\ell})$. Then:*

(a) $J \leqslant \max\left\{1, p^{2M_j - \ell}\right\}$

(b) $J \leqslant \max\left\{1, p^{M_j - \ell}\right\} |Q_M|$

Proof. We prove (a) by considering two cases.

Case: $\ell \geqslant 2M_j$. If two distinct j-balls $B(r/q, p^{-\lceil \tau M_j \rceil})$ and $B(r'/q', p^{-\lceil \tau M_j \rceil})$ intersect $B(x, p^{-\ell})$, then $|r/q - r'/q'|_p \leqslant p^{-\ell}$, which contradicts lemma 3.6. Thus $J \leqslant 1$.

Case: $\ell < 2M_j$. Then $B(x, p^{-\ell})$ is a union of $p^{2M_j - \ell}$ balls of radius p^{-2M_j}. By lemma 3.6, any ball of radius p^{-2M_j} intersects (hence contains) at most one j-ball. Thus $J \leqslant p^{2M_j - \ell}$.

Now we turn to the proof of (b). Suppose $(q, r) \in Q_{M_j} \times R_{M_j}$. Note that $B(x, p^{-\ell})$ intersects the j-ball $B(r/q, p^{-\lceil \tau M_j \rceil})$ if and only if $|r/q - x|_p \leqslant p^{-\ell}$, which (because $|q|_p = 1$) is the case if and only if $r \equiv qx \pmod{p^\ell}$. Therefore J is less than or equal to the number of $(q, r) \in Q_{M_j} \times R_{M_j}$ such that $r \equiv qx \pmod{p^\ell}$. The proof is completed by noting that, for any $q \in Q_{M_j}$ (in fact, for any $q \in \mathbb{Z}$), the number of integers r with $r \equiv qx \pmod{p^\ell}$ and $0 \leqslant r < p^{M_j}$ is $\leqslant p^{M_j - \ell}$ if $M_j \geqslant \ell$ and is $\leqslant 1$ if $M_j \leqslant \ell$. □

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

LEMMA 3.9. *Let j, $k \in \mathbb{N}$ with $j \leqslant k$. If B is a j-ball such that $B \cap supp(P_k) \neq \emptyset$, then $B \cap supp(P_k)$ is a union of at most*

$$\prod_{i=j+1}^{k} |Q_{M_i}| p^{M_i - \lceil \tau M_{i-1} \rceil}$$

k-balls.

Proof. Let B be a j-ball such that $B \cap \text{supp}(P_k) \neq \emptyset$. The proof is by induction on k.

Base Step: $k = j$. Since $\text{supp}(F_{M_j})$ is a union of j-balls, the same is true of $\text{supp}(P_j)$. Since intersecting j-balls are equal, $B \cap \text{supp}(P_j) = B$.

Inductive Step: $k > j$. Note $B \cap \text{supp}(P_k)$ is the union of all k-balls contained in $B \cap \text{supp}(P_{k-1})$. Since $\text{supp}(P_k) \subseteq \text{supp}(P_{k-1})$, we have $B \cap \text{supp}(P_{k-1}) \neq \emptyset$. By the inductive hypothesis, $B \cap \text{supp}(P_{k-1})$ is a union of at most

$$\prod_{i=j+1}^{k-1} |Q_{M_i}| p^{(M_i - \lceil \tau M_{i-1} \rceil)}$$

$(k-1)$-balls. Let $B(r'/q', p^{-\lceil \tau M_{k-1} \rceil})$ be any such $(k-1)$-ball. It suffices to show that $B(r'/q', p^{-\lceil \tau M_{k-1} \rceil})$ contains $\leqslant |Q_{M_k}| p^{(M_k - \lceil \tau M_{k-1} \rceil)}$ k-balls. This follows from lemma 3.8(b) by taking $\ell = \lceil \tau M_{k-1} \rceil$. □

Now we are ready to prove lemma 3.5, which (as we noted above) implies (3.2).

Proof of lemma 3.5. Let $x \in \mathbb{Z}_p$ and let j, k, $l \in \mathbb{N}$ with $\lceil \tau M_{j-1} \rceil < \ell \leqslant \lceil \tau M_j \rceil$ and $k \geqslant j$. Let $B_1, \ldots, B_J$ be the collection of all j-balls that intersect $B(x, p^{-\ell})$. These balls are disjoint and contained in $B(x, p^{-\ell})$. Since $\text{supp}(P_k) \subseteq \text{supp}(P_j)$, and since $\text{supp}(P_j)$ is a union of j-balls, we have

$$\mu_k(B(x, p^{-\ell})) = \sum_{i=1}^{J} \mu_k(B_i) = \sum_{i=1}^{J} \int_{B_i \cap \text{supp}(P_k)} \psi_0(x) F_{M_1}(x) \cdots F_{M_k}(x) \, \mathrm{d}x.$$

First using (3.8), (3.9) and lemma 3.7, and then using lemma 3.9, $|R_M| = p^M$, and the fact that k-balls have Haar measure $p^{-\lceil \tau M_k \rceil}$, we obtain

$$\begin{aligned} \mu_k(B(x, p^{-\ell})) &\leqslant \|\psi_0\|_\infty \prod_{i=1}^{k} \frac{p^{\lceil \tau M_i \rceil}}{|Q_{M_i}||R_{M_i}|} \sum_{i=1}^{J} \int_{B_i \cap \text{supp}(P_k)} \mathrm{d}x \\ &\leqslant \|\psi_0\|_\infty \frac{J}{|Q_{M_j}||R_{M_j}|} \prod_{i=1}^{j-1} \frac{p^{\lceil \tau M_i \rceil}}{|Q_{M_i}||R_{M_i}|}. \end{aligned}$$

Now we consider three cases and use (3.5), lemma 3.8, $|Q_M| \approx p^M / \ln(p^M)$, and $|R_M| = p^M$.

Case: $2M_j < \ell \leqslant \lceil \tau M_j \rceil$. We get

$$\mu_k(B(x,p^{-\ell})) \leqslant \|\psi_0\|_\infty \frac{1}{|Q_{M_j}||R_{M_j}|} g(p^{M_j}) \approx p^{-2M_j} \ln(p^{M_j}) g(p^{M_j})$$

Since $\ell \leqslant \lceil \tau M_j \rceil \leqslant 1 + \tau M_j$, we have $p^{-2M_j} \leqslant p^{2/\tau} p^{-2\ell/\tau} \lesssim p^{-2\ell/\tau}$. Thus (3.18) follows immediately.

Case: $M_j < \ell \leqslant 2M_j$. We get

$$\mu_k(B(x,p^{-\ell})) \leqslant \|\psi_0\|_\infty \frac{p^{2M_j-\ell}}{|Q_{M_j}||R_{M_j}|} g(p^{M_j}) \approx p^{-\ell} \ln(p^{M_j}) g(p^{M_j})$$

Since $\tau > 2$, we have $p^{-\ell} < p^{-2\ell/\tau}$. Thus (3.18) follows immediately.

Case: $\lceil \tau M_{j-1} \rceil < \ell \leqslant M_j$. We get

$$\begin{aligned}\mu_k(B(x,p^{-\ell})) &\leqslant \|\psi_0\|_\infty \frac{|Q_{M_j}|p^{M_j-\ell}}{|Q_{M_j}||R_{M_j}|} \cdot \frac{p^{\lceil \tau M_{j-1} \rceil}}{|Q_{M_{j-1}}||R_{M_{j-1}}|} g(p^{M_{j-1}}) \\ &\approx p^{\lceil \tau M_{j-1} \rceil - 2M_{j-1} - \ell} \ln(p^{M_{j-1}}) g(p^{M_{j-1}}).\end{aligned}$$

Since $\tau > 2$ and $\tau M_{j-1} < \ell$, we have

$$\lceil \tau M_{j-1} \rceil - 2M_{j-1} \leqslant 1 + \tau M_{j-1}\left(1 - \frac{2}{\tau}\right) \leqslant 1 + \ell - \frac{2\ell}{\tau}.$$

Thus (3.18) follows immediately. □

3.3. Proof of lemma 3.3

Proof. Let $M \in \mathbb{N}$ and $s \in \mathbb{Q}_p/\mathbb{Z}_p$. For $|s|_p > p^{\lceil \tau M \rceil}$, lemma 3.2 implies (3.13). For $|s|_p \leqslant p^{\lceil \tau M \rceil}$, lemma 3.2 gives

$$\widehat{F_M}(s) = |Q_M|^{-1} |R_M|^{-1} \sum_{q \in Q_M} \sum_{0 \leqslant r < p^M} e(\{rs/q\}_p). \tag{3.20}$$

Setting $s = 0$ yields (3.10). From now on, assume $0 < |s|_p \leqslant p^{\lceil \tau M \rceil}$. So $|s|_p = p^\ell$ for some $\ell \in \{1, \ldots, \lceil \tau M \rceil\}$. We will study the sum over r in (3.20). Fix $q \in Q_M$. Since $|q|_p = 1$, we have $|s/q|_p = |s|_p = p^\ell$. Thus the p-adic expansion of s/q has the form

$$\frac{s}{q} = \sum_{i=-\ell}^{\infty} c_i p^i, \quad c_i \in \{0, 1, \ldots, p-1\}, \quad c_{-\ell} \neq 0. \tag{3.21}$$

Evidently $0 < \{s/q\}_p < 1$, and so $e(\{s/q\}_p) \neq 1$. Because of (2.2), we have the geometric summation formula

$$\sum_{0 \leqslant r < p^M} e(\{rs/q\}_p) = \frac{1 - e(\{sp^M/q\}_p)}{1 - e(\{s/q\}_p)}. \tag{3.22}$$

If $|s|_p \leqslant p^M$, we have $\{sp^M/q\}_p = 0$, hence the sum in (3.22) is zero. Applying this observation to (3.20) proves (3.11).

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

Now only (3.12) remains to be proved. Assume $p^M < |s|_p = p^\ell \leqslant p^{\lceil \tau M \rceil}$. For all $z \in \mathbb{R}$, $|1 - e(z)| = 2|\sin(\pi z)| = 2\sin(\pi\|z\|) \geqslant \pi\|z\|$, where $\|z\| = \min_{k\in\mathbb{Z}} |z-k|$ is the distance from z to the nearest integer. Hence the sum in (3.22) satisfies

$$\left| \sum_{0\leqslant r<p^M} e(\{rs/q\}_p) \right| \leqslant \min\left\{ \frac{1}{\|\{s/q\}_p\|}, p^M \right\}. \tag{3.23}$$

In light of (3.21),

$$\|\{s/q\}_p\| = \begin{cases} \{s/q\}_p = \sum_{i=-\ell}^{-1} c_i p^i & \text{if } \{s/q\}_p \leqslant 1/2 \\ 1 - \{s/q\}_p = 1 - \sum_{i=-\ell}^{-1} c_i p^i & \text{if } \{s/q\}_p > 1/2. \end{cases}$$

Combining (3.20), (3.23), and the fact that $p^{-\ell} \leqslant \|\{s/q\}_p\| < 1$ leads to

$$|\widehat{F_M}(s)| \leqslant |Q_M|^{-1}|R_M|^{-1} \sum_{k=1}^{\ell} \sum_{\substack{1/2p^M \leqslant q < p^M \\ |q|_p=1, \quad q \text{ prime} \\ p^{-k} \leqslant \|\{s/q\}_p\| < p^{-k+1}}} \min\left\{p^k, p^M\right\}. \tag{3.24}$$

For fixed $1 \leqslant k \leqslant \ell$, we now estimate the number of terms in the sum over q in (3.24). This estimate is similar to the proof of theorem 1 in Cilleruelo and Garaev's paper [**13**]. Consider any prime q with $1/2p^M \leqslant q < p^M$, $|q|_p = 1$, and $p^{-k} \leqslant \|\{s/q\}_p\| < p^{-k+1}$. Define $N = \|\{s/q\}_p\| p^\ell q$. Note that N is a positive integer $\leqslant p^{M+\ell-k+1}$. If $\{s/q\}_p \leqslant 1/2$, then $N = \left(s/q - [s/q]_p\right) p^\ell q \equiv sp^\ell \pmod{p^\ell}$. Similarly, if $\{s/q\}_p > 1/2$, then $N = \left(1 - s/q + [s/q]_p\right) p^\ell q \equiv -sp^\ell \pmod{p^\ell}$. Therefore q is a prime $\geqslant 1/2p^M$ that divides a positive integer N with $N \leqslant p^{M+\ell-k+1}$ and $N \equiv \pm sp^\ell \pmod{p^\ell}$. The number of positive integers N with $N \leqslant p^{M+\ell-k+1}$ and $N \equiv \pm sp^\ell \pmod{p^\ell}$ is $\lesssim \max\left\{p^{M-k+1}, 1\right\}$. And the number of primes $q \geqslant 1/2p^M$ that divide a given positive integer N is $\lesssim \ln N / \ln p^M$. Therefore the number of terms in the sum over q in (3.24) is

$$\lesssim \max\left\{p^{M-k+1}, 1\right\} \frac{\ln p^{M+\ell-k+1}}{\ln p^M}.$$

Thus (3.24) implies

$$|\widehat{F_M}(s)| \lesssim |Q_M|^{-1}|R_M|^{-1} \sum_{k=1}^{\ell} \min\left\{p^k, p^M\right\} \max\left\{p^{M-k+1}, 1\right\} \frac{\ln p^{M+\ell-k+1}}{\ln p^M}.$$

Since $p^M < |s|_p = p^\ell \leqslant p^{\lceil \tau M \rceil}$, $|Q_M| \gtrsim p^M / \ln p^M$, and $|R_M| = p^M$, we obtain (3.12). $\square$

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

3.4. Proof of lemma 3.4

Proof. Let $s \in \mathbb{Q}_p/\mathbb{Z}_p$. The proof is by induction on k. The case $k=0$ follows immediately from (3.6) and the definition $\mathrm{d}\mu_0 = \mathrm{d}\mu_{-1} = \psi_0\, \mathrm{d}x$. Assume $k \geqslant 1$. The inductive hypothesis is that (3.14)–(3.17) hold with k replaced by $k-1$. By the usual argument with the Fourier inversion theorem (see [**18**, p.102] or [**40**, p. 120]) and Fubini's theorem, we have

$$\widehat{\mu_k}(s) = \widehat{F_{M_k}\mu_{k-1}}(s) = \sum_{t \in \mathbb{Q}_p/\mathbb{Z}_p} \widehat{F_{M_k}}(s-t)\widehat{\mu_{k-1}}(t). \tag{3.25}$$

If the summand $\widehat{F_{M_k}}(s-t)\widehat{\mu_{k-1}}(t)$ is non-zero, then we must have $|t|_p \leqslant p^{\lceil \tau M_{k-1} \rceil}$ by the inductive hypothesis, and either

$$t = s \qquad \text{or} \qquad p^{M_k} < |s|_p = |s-t|_p \leqslant p^{\lceil \tau M_k \rceil}$$

by (3.3) and lemma 3.3. Therefore, if $|s|_p > p^{\lceil \tau M_k \rceil}$, every term of the sum in (3.25) is zero, and $\widehat{\mu_k}(s) = 0$. This proves (3.17). On the other hand, if $|s|_p \leqslant p^{M_k}$, then only the $t = s$ term contributes to the sum, and $\widehat{\mu_k}(s) = \widehat{F_{M_k}}(0)\widehat{\mu_{k-1}}(s) = \widehat{\mu_{k-1}}(s)$. This proves (3.15) and, using the inductive hypothesis, (3.14). Only (3.16) remains to be proved. Suppose $p^{M_k} < |s|_p \leqslant p^{\lceil \tau M_k \rceil}$. For all $t \in \mathbb{Q}_p/\mathbb{Z}_p$ with $\widehat{F_{M_k}}(s-t)\widehat{\mu_{k-1}}(t) \neq 0$ we must have $|s|_p = |s-t|_p$, and so (3.12) gives $|\widehat{F_{M_k}}(s-t)| \lesssim |s|^{-1/\tau} \ln^2(|s|_p)$. By the inductive hypothesis, $|\widehat{\mu_{k-1}}(t)| \leqslant \widehat{\mu_{k-1}}(0) = 1$ for all $t \in \mathbb{Q}_p/\mathbb{Z}_p$. By counting digits, the number of $t \in \mathbb{Q}_p/\mathbb{Z}_p$ with $|t|_p \leqslant p^{\lceil \tau M_{k-1} \rceil}$ is exactly $p^{\lceil \tau M_{k-1} \rceil}$; hence, the sum in (3.25) has at most $p^{\lceil \tau M_{k-1} \rceil}$ non-zero terms. Putting it all together, we get

$$|\widehat{\mu_k}(s)| \lesssim p^{\lceil \tau M_{k-1} \rceil} |s|_p^{-1/\tau} \ln^2(|s|_p).$$

Finally, applying (3.4) gives (3.16). □

4. Proof of theorem 1.7

4.1. Reduction

To prove theorem 1.7, it suffices to prove the following seemingly weaker theorem.

THEOREM 4.1. *Let g be a non-negative non-decreasing function defined on $(0, \infty)$ such that $\lim_{x\to\infty} g(x) = \infty$. For every $\tau > (m+n)/m$, there exists a Borel probability measure μ supported on $W(m, n, \tau)$ such that*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-n/\tau} \ln^{n+1}(1 + |\xi|_p) g(|\xi|_p) \quad \forall \xi \in \mathbb{Q}_p^{mn}, \quad \xi \neq 0.$$

We emphasize that the constant implied by $\lesssim$ does not depend on g.

The proof that theorem 4.1 implies theorem 1.7 is analogous to the proof in § 3.1 that theorem 3.1 implies theorem 1.5.

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

4.2. Proof of theorem 4.1

Let $\tau > (m+n)/m$. Let g be any non-negative non-decreasing function defined on $(0,\infty)$ such that $\lim_{x\to\infty} g(x) = \infty$. For each $M \in \mathbb{N}$, define Q_M and R_M as in § 3.2. Then

$$Q_M^n = \left\{ q \in \mathbb{Z}^n : \frac{1}{2}p^M \leqslant q_j < p^M, \quad |q_j|_p = 1, \quad q_j \text{ prime } \forall 1 \leqslant j \leqslant n \right\},$$
$$R_M^m = \left\{ r \in \mathbb{Z}^m : 0 \leqslant r_i < p^M \ \ \forall 1 \leqslant i \leqslant m \right\}.$$

Note that Q_M is non-empty unless $p=2$ and $M=1$. For everything that follows, we make the standing assumption that $M \geqslant 2$ if $p=2$. For each $q \in Q_M^n$ and $r \in R_M^m$, define the function $\phi_{q,r}$ on $\mathbb{Z}_p^{mn}$ by

$$\phi_{q,r}(x) = p^{m\lceil \tau M \rceil} \mathbf{1}_{B(0,1)}(p^{-\lceil \tau M \rceil}(xq - r)) \quad \forall x \in \mathbb{Z}_p^{mn}.$$

For each $M \in \mathbb{N}$, define the function F_M on $\mathbb{Z}_p^{mn}$ by

$$F_M(x) = |Q_M^n|^{-1} |R_M^m|^{-1} \sum_{q \in Q_M^n} \sum_{r \in R_M^m} \phi_{q,r}(x) \quad \forall x \in \mathbb{Z}_p^{mn}.$$

Choose a strictly increasing sequence of non-negative integers $(M_k)_{k=0}^{\infty}$ such that for all $k \in \mathbb{N}$

$$\lceil \tau M_{k-1} \rceil < M_k, \tag{4.1}$$
$$p^{mn\lceil \tau M_{k-1} \rceil} < g(p^{M_k}). \tag{4.2}$$

Let ψ_0 be any non-negative function on $\mathbb{Z}_p^{mn}$ such that

$$\widehat{\psi_0}(0) = 1, \tag{4.3}$$
$$\widehat{\psi_0}(s) = 0 \quad \text{for all } s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn} \text{ with } |s|_p > p^{\lceil \tau M_0 \rceil}. \tag{4.4}$$

In light of lemma 2.1, we may choose, for example, $\psi_0 = \mathbf{1}_{B(0,1)}$. For each $k \in \mathbb{N}$, define the measure μ_k on $\mathbb{Z}_p^{mn}$ by

$$\mathrm{d}\mu_k(x) = \psi_0(x) F_{M_1}(x) \cdots F_{M_k}(x)\, \mathrm{d}x.$$

For notational convenience in lemma 3.4 below, we define $\mathrm{d}\mu_{-1}(x) = \mathrm{d}\mu_0(x) = \psi_0(x)\,\mathrm{d}x$. For each $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$, define

$$D(s) = \left\{ q \in \mathbb{Z}^n : \{s_{ij}/q_j\}_p = \{s_{ij'}/q_{j'}\}_p \ \forall 1 \leqslant i \leqslant m,\ 1 \leqslant j,\ j' \leqslant n \right\}.$$

The proof proceeds by the following sequence of lemmas.

LEMMA 4.2. *For all $M \in \mathbb{N}$, $q \in Q_M^n$, $r \in R_M^m$, and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

$$\widehat{\phi_{q,r}}(s) = \begin{cases} e\left(\sum_{i=1}^{m} \{r_i s_{i1}/q_1\}_p \right) & \text{if } |s|_p \leqslant p^{\lceil \tau M \rceil} \text{ and } q \in D(s) \\ 0 & \text{otherwise} \end{cases}$$

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

LEMMA 4.3. *For all $M \in \mathbb{N}$ and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

$$\widehat{F_M}(s) = 1 \qquad \text{if } s = 0 \tag{4.5}$$
$$\widehat{F_M}(s) = 0 \qquad \text{if } 0 < |s|_p \leqslant p^M \tag{4.6}$$
$$|\widehat{F_M}(s)| \lesssim |s|^{-n/\tau} \ln^{n+1}(|s|_p) \qquad \text{if } p^M < |s|_p \leqslant p^{\lceil \tau M \rceil} \tag{4.7}$$
$$\widehat{F_M}(s) = 0 \qquad \text{if } |s|_p > p^{\lceil \tau M \rceil} \tag{4.8}$$

LEMMA 4.4. *For all integers $k \geqslant 0$ and all $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

$$\widehat{\mu_k}(s) = 1 \qquad \text{if } s = 0 \tag{4.9}$$
$$\widehat{\mu_k}(s) = \widehat{\mu_{k-1}}(s) \qquad \text{if } 0 < |s|_p \leqslant p^{M_k} \tag{4.10}$$
$$|\widehat{\mu_k}(s)| \lesssim |s|^{-n/\tau} \ln^{n+1}(|s|_p) g(|s|_p) \qquad \text{if } p^{M_k} < |s|_p \leqslant p^{\lceil \tau M_k \rceil} \tag{4.11}$$
$$\widehat{\mu_k}(s) = 0 \qquad \text{if } |s|_p > p^{\lceil \tau M_k \rceil} \tag{4.12}$$

Unlike lemma 3.2, lemma 4.2 is not quite an immediate corollary of lemma 2.1. The proof of lemma 4.3 is a generalization of the proof of lemma 3.3. The proofs of lemmas 4.2 and 4.3 are given in §§ 4.3 and 4.4, respectively. We omit the proof of lemma 4.4 because it is virtually identical to the proof of lemma 3.4 in § 3.4.

The rest of the proof of theorem 4.1 proceeds as in § 3.2, so we omit it.

4.3. Proof of lemma 4.2

Proof. Let $M \in \mathbb{N}$, $q \in Q_M^n$, $r \in R_M^m$, and $s \in \mathbb{Q}_p/\mathbb{Z}_p$ be given. Define the function ϕ_r on $\mathbb{Z}_p^m$ by

$$\phi_r(x) = p^{m\lceil \tau M \rceil} \mathbf{1}_{B(0,1)}(p^{-\lceil \tau M \rceil}(x - r)) \quad \forall x \in \mathbb{Z}_p^m.$$

By lemma 2.1, for all $k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m$,

$$\widehat{\phi_r}(k) = \begin{cases} e(\{r \cdot k\}_p) & \text{if } |k|_p \leqslant p^{\lceil \tau M \rceil} \\ 0 & \text{if } |k|_p > p^{\lceil \tau M \rceil} \end{cases} \tag{4.13}$$

By Fourier inversion (see [**18**, p. 102] or [**40**, p. 120]),

$$\phi_r(x) = \sum_{k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi_r}(k) e(-\{k \cdot x\}_p) \quad \forall x \in \mathbb{Z}_p^m.$$

Therefore, since $|q_j|_p = 1$ for all $1 \leqslant j \leqslant n$,

$$\phi_{q,r}(x) = \phi_r(xq) = \sum_{k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi_r}(k) e(-\{k \cdot xq\}_p) \quad \forall x \in \mathbb{Z}_p^{mn}.$$

By Fubini's theorem,

$$\widehat{\phi_{q,r}}(s) = \sum_{k\in(\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi_r}(k) \int_{\mathbb{Z}_p^{mn}} e(\{s\cdot x\}_p) e(-\{k\cdot xq\}_p)\, \mathrm{d}x \tag{4.14}$$

$$= \sum_{k\in(\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi_r}(k) \prod_{i=1}^{m}\prod_{j=1}^{n} \int_{\mathbb{Z}_p} e(\{x_{ij}(s_{ij}-k_i q_j)\}_p)\, \mathrm{d}x_{ij}.$$

Fix $k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m$. By lemma 2.1,

$$\int_{\mathbb{Z}_p} e(\{x_{ij}(s_{ij}-k_i q_j)\}_p)\, \mathrm{d}x_{ij} = \begin{cases} 1 & \text{if } |s_{ij}-k_iq_j|_p \leqslant 1 \\ 0 & \text{otherwise} \end{cases}$$

Note that, since $k_i \in \mathbb{Q}_p/\mathbb{Z}_p$ and $|q_j|_p = 1$, $|s_{ij}-k_iq_j|_p \leqslant 1$ is equivalent to $k_i = \{s_{ij}/q_j\}_p$. Thus (4.14) gives

$$\widehat{\phi_{q,r}}(s) = \begin{cases} \widehat{\phi_r}(\{s_{11}/q_1\}_p, \ldots, \{s_{m1}/q_1\}_p) & \text{if } q \in D(s) \\ 0 & \text{otherwise} \end{cases}$$

To complete the proof, use (2.2), (4.13), and the fact that for all $\ell \geqslant 0$ and $y \in \mathbb{Q}_p$, we have $|y|_p \leqslant p^\ell$ if and only if $|\{y\}_p|_p \leqslant p^\ell$. □

4.4. Proof of lemma 4.3

Proof. Let $M \in \mathbb{N}$ and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$. Choose $1 \leqslant i_0 \leqslant m$ and $1 \leqslant j_0 \leqslant n$ such that $|s_{i_0j_0}|_p = |s|_p$. For $|s|_p > p^{\lceil \tau M\rceil}$, lemma 4.2 implies (4.8). For $|s|_p \leqslant p^{\lceil \tau M\rceil}$, (2.2), lemma 4.2, and the definition of $D(s)$ give

$$\widehat{F_M}(s) = |Q_M^n|^{-1}|R_M^m|^{-1} \sum_{q\in Q_M^n\cap D(s)} \prod_{i=1}^{m} \sum_{0\leqslant r_i<p^M} e(\{r_i s_{ij_0}/q_{j_0}\}_p) \tag{4.15}$$

Setting $s = 0$ yields (4.5).

From now on, assume $0 < |s|_p \leqslant p^{\lceil \tau M\rceil}$. So $|s|_p = p^\ell$ for some $\ell \in \{1, \ldots, \lceil \tau M\rceil\}$. We will study the sum over r_{i_0} in (4.15). Fix $q \in Q_M^n \cap D(s)$. Since $|q_{j_0}|_p = 1$, we have $|s_{i_0j_0}/q_{j_0}|_p = |s_{i_0j_0}|_p = |s|_p = p^\ell$. Thus the p-adic expansion of $s_{i_0j_0}/q_{j_0}$ has the form

$$\frac{s_{i_0j_0}}{q_{j_0}} = \sum_{i=-\ell}^{\infty} c_i p^i, \quad c_i \in \{0, 1, \ldots, p-1\}, \quad c_{-\ell} \neq 0. \tag{4.16}$$

Evidently $0 < \{s_{i_0j_0}/q_{j_0}\}_p < 1$, and so $e(\{s_{i_0j_0}/q_{j_0}\}_p) \neq 1$. Because of (2.2), we have the geometric summation formula

$$\sum_{0\leqslant r_{i_0}<p^M} e(\{r_{i_0}s_{i_0j_0}/q_{j_0}\}_p) = \frac{1-e(\{p^M s_{i_0j_0}/q_{j_0}\}_p)}{1-e(\{s_{i_0j_0}/q_{j_0}\}_p)}. \tag{4.17}$$

If $|s|_p \leqslant p^M$, we have $\{p^M s_{i_0j_0}/q_{j_0}\}_p = 0$; hence, the sum in (4.17) is zero. Applying this observation to (4.15) proves (4.6).

https://doi.org/10.1017/prm.2018.115 Published online by Cambridge University Press

Now only (4.7) remains to be proved. Assume $p^M < |s|_p = p^\ell \leqslant p^{\lceil \tau M \rceil}$. For all $z \in \mathbb{R}$, $|1 - e(z)| = 2|\sin(\pi z)| = 2\sin(\pi\|z\|) \geqslant \pi\|z\|$, where $\|z\| = \min_{k\in\mathbb{Z}} |z-k|$ is the distance from z to the nearest integer. Hence the sum in (4.17) satisfies

$$\left| \sum_{0 \leqslant r_{i_0} < p^M} e(\{r_{i_0} s_{i_0 j_0}/q_{j_0}\}_p) \right| \leqslant \min\left\{ \frac{1}{\| \{s_{i_0 j_0}/q_{j_0}\}_p \|}, p^M \right\}. \tag{4.18}$$

We will also need that

$$\left| \sum_{0 \leqslant r_i < p^M} e(\{r_i s_{i j_0}/q_{j_0}\}_p) \right| \leqslant p^M \quad \forall 1 \leqslant i \leqslant m. \tag{4.19}$$

In light of (4.16),

$$\| \{s_{i_0 j_0}/q_{j_0}\}_p \| = \begin{cases} \{s_{i_0 j_0}/q_{j_0}\}_p = \sum_{i=-\ell}^{-1} c_i p^i & \text{if } \{s_{i_0 j_0}/q_{j_0}\}_p \leqslant 1/2 \\ 1 - \{s_{i_0 j_0}/q_{j_0}\}_p = 1 - \sum_{i=-\ell}^{-1} c_i p^i & \text{if } \{s_{i_0 j_0}/q_{j_0}\}_p > 1/2. \end{cases}$$

Combining (4.15), (4.18) (4.19), and the fact that $p^{-\ell} \leqslant \| \{s_{i_0 j_0}/q_{j_0}\}_p \| < 1$ leads to

$$|\widehat{F_M}(s)| \leqslant |Q_M^n|^{-1} |R_M^m|^{-1} \sum_{k=1}^{\ell} \sum_{q} p^{(m-1)M} \min\left\{p^k, p^M\right\}, \tag{4.20}$$

where the inner sum runs over all $q \in Q_M^n \cap D(s)$ such that $p^{-k} \leqslant \| \{s_{i_0 j_0}/q_{j_0}\}_p \| < p^{-k+1}$. We claim $(q_1, \ldots, q_n) \mapsto q_{j_0}$ is an injection from $Q_M^n \cap D(s)$ to the set

$$\left\{ q_{j_0} \in \mathbb{Z} : \frac{1}{2} p^M \leqslant q_{j_0} < p^M, \quad |q_{j_0}|_p = 1, \quad q_{j_0} \text{ prime} \right\}.$$

This claim follows from the following two observations. First, for each $q \in Q_M^n$ and $1 \leqslant j \leqslant n$, we have $\{s_{i_0 j_0}/q_{j_0}\}_p = \{s_{i_0 j}/q_j\}_p$ if and only if $|s_{i_0 j_0}/q_{j_0} - s_{i_0 j}/q_j|_p \leqslant 1$ if and only if $|q_j - q_{j_0} s_{i_0 j} s_{i_0 j_0}^{-1}|_p \leqslant |s_{i_0 j_0}^{-1}|_p = p^{-\ell}$ if and only if $q_j \equiv q_{j_0} s_{i_0 j} s_{i_0 j_0}^{-1} \pmod{p^\ell}$. Second, for any given $b \in \mathbb{Q}_p$, there can be at most one integer a satisfying $a \equiv b \pmod{p^\ell}$ and $1/2p^M \leqslant a < p^M \leqslant p^\ell$. Applying the claim to (4.20) yields

$$|\widehat{F_M}(s)| \leqslant |Q_M^n|^{-1} |R_M^m|^{-1} \sum_{k=1}^{\ell} \sum_{q_{j_0}} p^{(m-1)M} \min\left\{p^k, p^M\right\}, \tag{4.21}$$

where the inner sum runs over all $q_{j_0} \in Q_M$ such that $p^{-k} \leqslant \| \{s_{i_0 j_0}/q_{j_0}\}_p \| < p^{-k+1}$. Arguing as in the proof of lemma 3.3 in § 3.3, we see that for each fixed

$1 \leqslant k \leqslant \ell$ the number of terms in the sum over q_{j_0} in (4.21) is

$$\lesssim \max\left\{p^{M-k+1}, 1\right\} \frac{\ln p^{M+\ell-k+1}}{\ln p^M}.$$

Thus (4.21) implies

$$|\widehat{F_M}(s)| \lesssim |Q_M^n|^{-1}|R_M^m|^{-1} \sum_{k=1}^{\ell} p^{(m-1)M} \min\left\{p^k, p^M\right\} \max\left\{p^{M-k+1}, 1\right\} \frac{\ln p^{M+\ell-k+1}}{\ln p^M}.$$

Since $p^M < |s|_p = p^\ell \leqslant p^{\lceil \tau M \rceil}$, $|Q_M^n| \approx p^{nM}/(\ln p^M)^n$, and $|R_M^m| = p^{mM}$, we obtain (4.7). □

Acknowledgements

This work was supported by NSERC.

References

1 A. G. Abercrombie. The Hausdorff dimension of some exceptional sets of p-adic integer matrices. *J. Number Theory*, **53** (1995), 311–341.

2 D. Allen and S. Troscheit. The Mass Transference Principle: Ten Years On. https://arxiv.org/abs/1704.06628v2.

3 J.-G. Bak and A. Seeger. Extensions of the Stein-Tomas theorem. *Math. Res. Lett.*, **18** (2011), 767–781.

4 V. Beresnevich, D. Dickinson and S. Velani. Measure theoretic laws for lim sup sets. *Mem. Amer. Math. Soc.*, **179** (2006)

5 V. Beresnevich, V. Bernik, M. Dodson and S. Velani. Classical metric Diophantine approximation revisited. In *Analytic number theory*, pages 38–61 (Cambridge: Univ Cambridge Press 2009).

6 A. S. Besicovitch. Sets of Fractional Dimensions (IV): On Rational Approximation to Real Numbers. *J. London Math. Soc.*, S1–9 126, 1934.

7 C. Bluhm. Random recursive construction of Salem sets. *Ark. Mat.*, **34** (1996), 51–63.

8 C. Bluhm. On a theorem of Kaufman: Cantor-type construction of linear fractal Salem sets. *Ark. Mat.*, **36** (1998), 307–316.

9 V. I. Bogachev. *Measure theory. Vol. I, II* (Berlin: Springer-Verlag, 2007).

10 J. D. Bovey and M. M. Dodson. The Hausdorff dimension of systems of linear forms. *Acta Arith.*, **45** (1986), 337–358.

11 A. Carbery, A. Seeger, S. Wainger and J. Wright. Classes of singular integral operators along variable lines. *J. Geom. Anal.*, **9** (1999), 583–605.

12 X. Chen and A. Seeger. Convolution powers of Salem measures with applications. *Canad. J. Math.*, **69** (2017), 284–320.

13 J. Cilleruelo and M. Z. Garaev. Concentration of points on two and three dimensional modular hyperbolas and applications. *Geom. Funct. Anal.*, **21** (2011), 892–904.

14 H. G. Eggleston. Sets of fractional dimensions which occur in some problems of number theory. *Proc. London Math. Soc. (2)* **54** (1952), 42–93.

15 F. Ekström. Fourier dimension of random images. *Ark. Mat.*, **54** (2016), 455–471.

16 F. Ekström, T. Persson and J. Schmeling. On the Fourier dimension and a modification. *J. Fractal Geom.*, **2** (2015), 309–337.

17 K. J. Falconer. *The geometry of fractal sets, volume 85 Cambridge Tracts in Mathematics* (Cambridge: Cambridge University Press, 1986).

18 G. B. Folland. *A course in abstract harmonic analysis*. Studies in Advanced Mathematics. (Boca Raton FL: CRC Press, 1995).

19 J. M. Fraser, T. Orponen and T. Sahlsten. On Fourier analytic properties of graphs. *Int. Math. Res. Not. IMRN* (2014), 2730–2745.

20 K. Hambrook. Explicit Salem sets and applications to metrical Diophantine approximation. https://arxiv.org/abs/1604.00411v1.

21 K. Hambrook. Explicit Salem sets in $\mathbb{R}^2$. *Adv. Math.* **311** (2017), 634–648.

22 V. Jarník. Diophantischen Approximationen und Hausdorffsches Mass. *Mat. Sborjnik* **36** (1929), 371–382.

23 V. Jarník. über die simultanen diophantischen Approximationen. *Math. Z.*, **33** (1931), 505–543.

24 J.-P. Kahane. *Some random series of functions*, 2nd edn, volume. 5, of *Cambridge Studies in Advanced Mathematics* (Cambridge: Cambridge University Press, 1985)

25 R. Kaufman. On the theorem of Jarník and Besicovitch. *Acta Arith.*, **39** (1981), 265–267.

26 I. Łaba and M. Pramanik. Arithmetic progressions in sets of fractional dimension. *Geom. Funct. Anal.*, **19** (2009), 429–456.

27 P. Mattila. *Geometry of sets and measures in Euclidean spaces, volume 44 of Cambridge Studies in Advanced Mathematics* (Cambridge: Cambridge University Press, 1995). Fractals and rectifiability.

28 P. Mattila. *Fourier analysis and Hausdorff dimension, volume 150 of Cambridge Studies in Advanced Mathematics* (Cambridge: Cambridge University Press, 2015).

29 J. V. Melničuk. Hausdorff dimension in Diophantine approximations of p-adic numbers, *Ukrain. Mat. Zh.*, **32** (1980), 118–124.

30 T. Mitsis. A Stein-Tomas restriction theorem for general measures. *Publ. Math. Debrecen* **60** (2002), 89–99.

31 G. Mockenhaupt. *Bounds in Lebesgue spaces of oscillatory integral operators* (Siegen: Habilitationsschrift, Gesamthochschule, 1996).

32 G. Mockenhaupt. Salem sets and restriction properties of Fourier transforms. *Geom. Funct. Anal.* **10** (2000), 1579–1587.

33 G. Mockenhaupt and W. J. Ricker. Optimal extension of the Hausdorff-Young inequality. *J. Reine Angew. Math.* **620** (2008), 195–211.

34 C. Papadimitropoulos. *The Fourier restriction phenomenon in thin sets.* PhD thesis, University of Edinburgh, (2010a).

35 C. Papadimitropoulos. Salem sets in local fields, the Fourier restriction phenomenon and the Hausdorff-Young inequality. *J. Funct. Anal.* **259** (2010b), 1–27.

36 C. Papadimitropoulos. Salem sets in the p-adics, the Fourier restriction phenomenon and optimal extension of the Hausdorff-Young inequality. In (Guillermo P. Curbera, Gerd Mockenhaupt and Werner J. Ricker, eds) *Vector measures, integration and related topics, volume 201 of Oper Theory Adv. Appl.* pages 327–338 (Basel: Birkhäuser Verlag 2010c).

37 R. Salem. On singular monotonic functions whose spectrum has a given Hausdorff dimension. *Ark. Mat.* **1** (1951), 353–365.

38 P. Shmerkin and V. Suomala. Spatially independent martingales, intersections, and applications. To appear in Memoirs of the Amer. Math. Soc. https://arxiv.org/abs/1409.6707v4.

39 E. M. Stein. *Harmonic analysis: real-variable methods, orthogonality, and oscillatory integrals, volume 43 of Princeton Mathematical Series* (Princeton, NJ: Princeton University Press 1993.) With the assistance of Timothy S. Murphy, Monographs in Harmonic Analysis, III.

40 M. H. Taibleson. *Fourier analysis on local fields* (Princeton, NJ, Tokyo: Princeton University Press, University of Tokyo Press, 1975).