Proceedings of the Edinburgh Mathematical Society (2015) **58**, 1–26
DOI:10.1017/S0013091514000169

VERTICAL SHIFT AND SIMULTANEOUS DIOPHANTINE APPROXIMATION ON POLYNOMIAL CURVES

FAUSTIN ADICEAM

Department of Mathematics, Logic House, National University of Ireland, Maynooth, Ireland (fadiceam@gmail.com)

(Received 10 January 2013)

Abstract The Hausdorff dimension of the set of simultaneously τ-well-approximable points lying on a curve defined by a polynomial $P(X)+\alpha$, where $P(X)\in\mathbb{Z}[X]$ and $\alpha\in\mathbb{R}$, is studied when τ is larger than the degree of $P(X)$. This provides the first results related to the computation of the Hausdorff dimension of the set of well-approximable points lying on a curve that is not defined by a polynomial with integer coefficients. The proofs of the results also include the study of problems in Diophantine approximation in the case where the numerators and the denominators of the rational approximations are related by some congruential constraint.

Keywords: diophantine approximation; manifolds; polynomial curves; metric theory

2010 *Mathematics subject classification:* Primary 11J83; 11K60

1. Introduction and statement of the results

For any manifold $\mathcal{M}\subset\mathbb{R}^2$ and any real number $\tau>1$, denote by $W_\tau(\mathcal{M})$ the set of simultaneously τ-well-approximable points lying on $\mathcal{M}$, i.e.

$$\hat{W}_\tau(\mathcal{M})=\left\{(x,y)\in\mathcal{M}\colon \left|x-\frac{p}{q}\right|<\frac{1}{q^\tau}\text{ and }\left|y-\frac{r}{q}\right|<\frac{1}{q^\tau}\text{ i.o.}\right\}.$$

Here, and in what follows, 'i.o.' stands for *infinitely often*, that is, for infinitely many integers p, r and q with $q\geqslant 1$.

Even in the simplest case, where $\mathcal{M}$ is prescribed to be a planar curve defined by an equation with integer coefficients, the actual Hausdorff dimension $\dim\hat{W}_\tau(\mathcal{M})$ of the set $\hat{W}_\tau(\mathcal{M})$ may exhibit very different behaviours, although the starting point of the computation of the dimension is generally the same. It is shown that, if a pair of rationals $(p/q,r/q)$ realizes an approximation of $(x,y)\in\mathcal{M}$ at order τ as in the definition of the set $\hat{W}_\tau(\mathcal{M})$, then, for τ larger than some constant depending only on the curve, the point $(p/q,r/q)$ has to belong to $\mathcal{M}$ for q large enough. Obviously, the assumption that $\mathcal{M}$ is a curve defined by some equation with *integer* coefficients is then essential. The following two examples illustrate this fact.

Consider first, for any integer $l \geqslant 2$, the Fermat curve

$$\mathcal{F}_l := \{(x, y) \in \mathbb{R}^2 \colon x^l + y^l = 1\}.$$

For $\tau > 1$, let $(x, y) \in W_\tau(\mathcal{F}_l)$ and let $(p/q, r/q)$ be a pair of rational numbers such that

$$x = \frac{p}{q} + \frac{\epsilon_x \theta_x}{q^\tau} \quad \text{and} \quad y = \frac{r}{q} + \frac{\epsilon_y \theta_y}{q^\tau},$$

with $\epsilon_x, \epsilon_y \in \{\pm 1\}$ and $\theta_x, \theta_y \in (0, 1)$. In particular, $p = O(q)$ and $r = O(q)$ as q tends to ∞. On rearranging the equation

$$q^l = \left(p + \frac{\epsilon_x \theta_x}{q^{\tau-1}}\right)^l + \left(r + \frac{\epsilon_y \theta_y}{q^{\tau-1}}\right)^l,$$

it is readily seen that

$$|q^l - p^l - r^l| \leqslant \frac{C(l, x, y)}{q^{\tau - l}},$$

where $C(l, x, y,)$ is a strictly positive constant that depends on x, y and l, but is independent of q. For $\tau > l$ and q large enough, this implies that

$$q^l = p^l + r^l, \tag{1.1}$$

i.e. $(p/q, r/q) \in \mathcal{F}_l$. By Wiles's result on Fermat's last theorem [**12**], the latter equation is not solvable in positive integers as soon as $l \geqslant 3$. Therefore, if $(x, y) \in \hat{W}_\tau(\mathcal{F}_l)$ $(l \geqslant 3)$, then $(x, y) \in \{(1, 0); (0, 1)\}$ if l is odd, and $(x, y) \in \{(\pm 1, 0); (0, \pm 1)\}$ if l is even. This means that $\hat{W}_\tau(\mathcal{F}_l)$ contains at most four points if $\tau > l \geqslant 3$.

In particular, this implies the following result.

Theorem 1.1. *For $l \geqslant 3$ and $\tau > l$,*

$$\dim \hat{W}_\tau(\mathcal{F}_l) = 0.$$

Remark 1.2. If $l = 2$, (1.1) is soluble in infinitely many Pythagorean triples (p, q, r), and the result of Theorem 1.1 is no longer true. Indeed, Dickinson and Dodson [**4**] proved that

$$\dim \hat{W}_\tau(\mathcal{F}_2) = \frac{1}{\tau}$$

for $\tau > 2$, which constituted the first reasonably complete non-trivial result for the Hausdorff dimension of the set $\hat{W}_\tau(\mathcal{M})$ for a smooth manifold $\mathcal{M}$ in $\mathbb{R}^n$ when τ is larger than the extremal value of $1 + 1/n$. From their proof, it is also clear that the result holds true for any arc contained in $\mathbb{S}^1 = \mathcal{F}_2$.

Consider now the case where the manifold is an integer polynomial curve

$$\Gamma = \{(x, P(x)) \in \mathbb{R}^2 \colon x \in \mathbb{R}\}$$

in $\mathbb{R}^2$, where $P(X) \in \mathbb{Z}[X]$ is a polynomial of degree $d \geqslant 1$. Since Hausdorff dimension is unaffected under locally bi-Lipschitz transformations [**6**], it is not difficult to see that $\hat{W}_\tau(\Gamma)$ $(\tau > 0)$ has the same Hausdorff dimension as the set

$$W_\tau(P) := \left\{x \in \mathbb{R}\colon \left|x - \frac{p}{q}\right| < \frac{1}{q^\tau} \text{ and } \left|P(x) - \frac{r}{q}\right| < \frac{1}{q^\tau} \text{ i.o.}\right\}.$$

Working with an appropriate Taylor expansion of $P(X)$, Budarina *et al.* [**2**] proved that, for $\tau > d$, the only rational points that need to be taken into account for the computation of the Hausdorff dimension of the set $W_\tau(P)$ actually lie on the polynomial curve under consideration. Their result, which gave impetus to this paper, is the following (see [**2**] for the proof).

Theorem 1.3 (Budarina *et al.* [2]). *For $\tau > \max(d, 2/d)$, the Hausdorff dimension of $W_\tau(P)$ is*

$$\dim W_\tau(P) = \frac{2}{d\tau}.$$

In particular, for any $\tau > 0$, the set $W_\tau(P)$ is always of positive Hausdorff dimension, and therefore contains uncountably many points.

The main result of this paper shows that this no longer holds true in the metric sense as soon as the curve Γ is vertically translated by a real number. More precisely, given $\alpha \in \mathbb{R}$, let $W_\tau(P_\alpha)$ denote the set of simultaneously τ-approximable points lying on the polynomial curve $\Gamma_\alpha = \{(x, P(x) + \alpha) \in \mathbb{R}^2 \colon x \in \mathbb{R}\}$ in $\mathbb{R}^2$, that is,

$$W_\tau(P_\alpha) = \left\{x \in \mathbb{R}\colon \left|x - \frac{p}{q}\right| < \frac{1}{q^\tau} \text{ and } \left|P(x) + \alpha - \frac{r}{q}\right| < \frac{1}{q^\tau} \text{ i.o.}\right\}.$$

The main result proved in this paper then reads as follows.

Theorem 1.4. *Assume that $d \geqslant 2$. If $\tau > d + 1$, then*

$$W_\tau(P_\alpha) = \emptyset$$

for almost all $\alpha \in \mathbb{R}$.

Here, as elsewhere, *almost all* and *almost everywhere* must be understood in the sense that the set of exceptions has Lebesgue measure 0.

Theorem 1.4 improves a previous result due to Dickinson in [**3**, Theorem 4], where the weaker bound $3d - 1$ was proposed. The method developed in the proof of Theorem 1.4 provides evidence that the bound $d+1$ in the above is in fact optimal. Indeed, it provides an upper bound for the Hausdorff dimension of $W_\tau(P_\alpha)$ valid for almost all $\alpha \in \mathbb{R}$ and for $\tau \in (d, d + 1]$, which vanishes when $\tau = d + 1$.

Theorem 1.5. *Assume that $d \geqslant 2$. If $\tau \in (d, d + 1]$, then*

$$\dim W_\tau(P_\alpha) \leqslant \frac{d + 1 - \tau}{\tau} \tag{1.2}$$

for almost all $\alpha \in \mathbb{R}$.

The relevance of the result of Theorem 1.5 is also clear when compared with the following one, proved by Vaughan and Velani [**11**].

Theorem 1.6 (Vaughan and Velani [11]). *Let f be a three times continuously differentiable function defined on an interval I of $\mathbb{R}$ and let $\mathcal{C}_f := \{(x, f(x)) \in \mathbb{R}^2 \colon x \in I\}$. Let $\tau \in [3/2, 2)$ be given. Assume that $\dim\{x \in I \colon f''(x) = 0\} \leqslant (3-\tau)/\tau$. Denote by $W_\tau(f)$ the set of simultaneously τ-well-approximable points in $\mathbb{R}^2$ lying on the curve $\mathcal{C}_f$. Then,*

$$\dim W_\tau(f) = \frac{3-\tau}{\tau} =: s.$$

Moreover, if $\tau \in (3/2, 2)$, then the s-Hausdorff measure of the set $W_\tau(f)$ is infinite.

Now, if the degree of the polynomial $P(X)$ equals $d = 2$, the upper bound for the Hausdorff dimension of $W_\tau(P_\alpha)$ given by (1.2) for almost all $\alpha \in \mathbb{R}$ and for τ lying in the interval $(2, 3]$ has the same expression as the exact value of $\dim W_\tau(P_\alpha)$ provided by Theorem 1.6, which is valid for all $\alpha \in \mathbb{R}$ and for $\tau \in (3/2, 2)$.

Theorems 1.4 and 1.5 seem to provide the first results related to the study of the Hausdorff dimension of the set of well-approximable points lying on a curve that is not defined by a polynomial with integer coefficients. Besides this fact, the method involved in the proofs is also interesting in its own right, since it includes the study of problems of Diophantine approximation by rationals whose numerators and denominators are related by some congruential constraint.

It should also be emphasized that Theorems 1.4 and 1.5 may easily be generalized to the case of a general decreasing approximating function $\Psi \colon \mathbb{R}_+ \to \mathbb{R}_+$, which tends to 0 at ∞. To this end, denote by $W_\Psi(P_\alpha)$ the set of Ψ-well-approximable points lying on the curve defined by the polynomial $P(X) + \alpha$ in such a way that $W_\tau(P_\alpha)$ is the set $W_\Psi(P_\alpha)$ with $\Psi(q) = q^{-\tau}$. Let λ_Ψ be the *lower order* of $1/\Psi$, that is,

$$\lambda_\Psi := \liminf \frac{-\log \Psi(q)}{\log q} \quad \text{as } q \to \infty.$$

The lower order λ_Ψ indicates the growth of the function $1/\Psi$ in a neighbourhood of ∞. Note that this quantity is always positive since Ψ tends to 0 at ∞. With this notation at one's disposal, the generalization of Theorems 1.4 and 1.5 may be stated as follows.

Corollary 1.7. *Assume that $d \geqslant 2$. If $\lambda_\Psi > d + 1$, then*

$$W_\Psi(P_\alpha) = \emptyset$$

for almost all $\alpha \in \mathbb{R}$. Furthermore, if $\lambda_\Psi \in (d, d+1]$, then

$$\dim W_\Psi(P_\alpha) \leqslant \frac{d + 1 - \lambda_\Psi}{\lambda_\Psi}$$

for almost all $\alpha \in \mathbb{R}$.

Proof. From the definition of the lower order λ_Ψ, it is readily verified that, for any $\epsilon > 0$,

$$\Psi(q) \leqslant q^{-\lambda_\Psi + \epsilon} \quad \text{for all but finitely many } q \in \mathbb{N}^*.$$

Therefore, for any $\epsilon > 0$,

$$W_\Psi(P_\alpha) \subset W_{\lambda_\Psi - \epsilon}(P_\alpha).$$

The corollary then follows easily from Theorems 1.4 and 1.5. □

The paper is organized as follows. The problem of simultaneous Diophantine approximation under consideration is first reduced to a problem of Diophantine approximation concerning the quality of approximation of the real number α by rational numbers whose numerators and denominators are related by some congruential constraint in § 2. The auxiliary lemmas collected in § 3 are needed in the course of the proofs of Theorem 1.4 in § 4 and Theorem 1.5 in § 5. Some remarks on the results and the method developed conclude the paper in § 6.

For details about Hausdorff dimension and the proof of some of its basic properties, which are used throughout, we refer the reader to [**6**].

Since the set $W_\tau(P_\alpha)$ is invariant when the real number α is translated by an integer, it is assumed throughout, without loss of generality, that α lies in the unit interval $[0, 1]$. Once and for all, $P(X) \in \mathbb{Z}[X]$ is a fixed polynomial of degree $d \geqslant 2$ whose leading coefficient is denoted by $-a_d \in \mathbb{Z}^*$ for convenience.

Notation

The following notation is used throughout.

- $\lfloor x \rfloor$ (respectively, $\lceil x \rceil$), $x \in \mathbb{R}$, is the integer part of x (respectively, the smallest integer not less than x).
- $(x)_+ := \max\{0, x\}$ $(x \in \mathbb{R})$.
- $f \ll g$ (respectively, $f \gg g$) is equivalent to $f = O(g)$ (respectively, $g = O(f)$).
- $[\![x, y]\!]$ $(x, y \in \mathbb{R},\ x \leqslant y)$ is the interval of integers, i.e. $[\![x, y]\!] = \{n \in \mathbb{Z} \colon x \leqslant n \leqslant y\}$.
- λ is the Lebesgue measure on the real line (or its restriction to the unit interval).
- $\mathrm{Card}(X)$ or $|X|$ is the cardinality of a finite set X.
- $A^\times$ is the set of invertible elements of a ring A.
- $M^* = M \setminus \{0\}$ for any monoid M with identity element 0.
- $\mathbb{P}$ (respectively, π, $\nu_\pi(q)$ for $q \in \mathbb{N}^*$) is the set of prime numbers (respectively, any prime number, the π-adic valuation of q).
- $\varphi(n)$ is Euler's totient function.
- $\tau(n)$ is the number of divisors of a positive integer n.

- $\omega(n)$ is the number of distinct prime factors dividing an integer $n \geqslant 2$ ($\omega(1) = 0$).
- $\|f\|_\infty^I$ is the infinity norm of a continuous function f over a bounded interval $I \subset \mathbb{R}$, i.e. $\|f\|_\infty^I = \sup_{x \in I} |f(x)|$.
- $G_d(q)$ ($d, q \geqslant 1$ integers) is the set of dth powers modulo q.
- $aG_d(q) := \{am\colon m \in G_d(q)\}$ ($d, q \geqslant 1$ integers, $a \in \mathbb{Z}/q\mathbb{Z}$).

2. From the simultaneous case to Diophantine approximation under a constraint

In this section, simultaneous approximation properties of a real number x and of $P(x)+\alpha$ are linked to some properties of Diophantine approximation under a constraint of the real number α, and conversely. The aforementioned constraint implies the resolution of a congruence equation involving the polynomial $P(X)$. This section is the key step to the proof of Theorems 1.4 and 1.5.

2.1. Reduction of the problem

Let M be an integer and let $W_\tau^M(P_\alpha) = W_\tau(P_\alpha) \cap [M, M+1]$, i.e.

$$W_\tau^M(P_\alpha) = \left\{x \in [M, M+1]\colon \left|x - \frac{p}{q}\right| < \frac{1}{q^\tau} \text{ and } \left|P(x) + \alpha - \frac{r}{q}\right| < \frac{1}{q^\tau} \text{ i.o.}\right\}.$$

It is clear that

$$W_\tau(P_\alpha) = \bigcup_{M \in \mathbb{Z}} W_\tau^M(P_\alpha).$$

In order to compute the Hausdorff dimension of the set $W_\tau(P_\alpha)$, it is more convenient to first focus on the subsets $W_\tau^M(P_\alpha)$. To this end, the following two lemmas are needed. Recall that $d := \deg P$.

Lemma 2.1. *Let $\tau > 0$ and $x \in [M, M+1]$ such that there exist rational numbers p/q and r/q satisfying*

$$x - \frac{p}{q} = \frac{\theta_x \epsilon_x}{q^\tau} \quad \text{and} \quad P(x) + \alpha - \frac{r}{q} = \frac{\theta_y \epsilon_y}{q^\tau},$$

with $\theta_x, \theta_y \in (0,1)$ and $\epsilon_x, \epsilon_y \in \{\pm 1\}$.

Then,

$$\left|\alpha - \frac{rq^{d-1} - q^d P(p/q)}{q^d}\right| < \frac{K_M}{q^\tau},$$

where $K_M := 1 + \|P'\|_\infty^{[M,M+1]}$.

Proof. The proof is straightforward. First note that

$$\alpha + P(x) - P(x) - \frac{rq^{d-1} - q^d P(p/q)}{q^d} = \frac{\theta_y \epsilon_y}{q^\tau} - \left(P(x) - P\left(\frac{p}{q}\right)\right).$$

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

Now, by the mean-value theorem, there exists a point c in $(x, p/q)$ such that

$$P(x) - P\left(\frac{p}{q}\right) = P'(c)\frac{\theta_x \epsilon_x}{q^\tau}.$$

Therefore,

$$\alpha - \frac{rq^{d-1} - q^d P(p/q)}{q^d} = \frac{\theta_y \epsilon_y - P'(c)\theta_x \epsilon_x}{q^\tau},$$

which proves the lemma. □

The next result provides a partial converse to Lemma 2.1. Here again,

$$K_M := 1 + \|P'\|_\infty^{[M,M+1]}.$$

Lemma 2.2. *Let b and $q \geqslant 1$ be integers such that there exists an integer $p \in [\![Mq, (M+1)q]\!]$ satisfying*

$$\frac{b}{q^d} + P\left(\frac{p}{q}\right) \in \frac{\mathbb{Z}}{q} := \left\{\frac{a}{q} \colon a \in \mathbb{Z}\right\}.$$

Assume, furthermore, that

$$\alpha - \frac{b}{q^d} = \frac{\epsilon\theta K_M}{q^\tau},$$

where $\theta \in (0,1)$ and $\epsilon \in \{\pm 1\}$.

There then exists $r \in \mathbb{Z}$ such that, for any $x \in (p/q - 1/q^\tau, p/q + 1/q^\tau)$,

$$\left|P(x) + \alpha - \frac{r}{q}\right| < \frac{2K_M}{q^\tau}.$$

Proof. Let $r \in \mathbb{Z}$ be such that

$$\frac{b}{q^d} + P\left(\frac{p}{q}\right) = \frac{r}{q}.$$

By the triangle inequality and the mean-value theorem,

$$\begin{aligned}\left|P(x) + \alpha - \frac{r}{q}\right| &\leqslant \left|P(x) - P\left(\frac{p}{q}\right)\right| + \left|\alpha - \frac{b}{q^d}\right| \\ &\leqslant \frac{\|P'\|_\infty^{[M,M+1]}}{q^\tau} + \frac{\theta K_M}{q^\tau}.\end{aligned}$$

Hence, the lemma is proved. □

For any integer M and any real number $K > 0$, let

$$\begin{aligned}R_\tau^M(\alpha)[K] := \Bigg\{x \in [M, M+1] \colon \left|x - \frac{p}{q}\right| < \frac{1}{q^\tau} \text{ and } \left|\alpha - \frac{b}{q^d}\right| < \frac{K}{q^\tau} \\ \text{with } \frac{b}{q^d} + P\left(\frac{p}{q}\right) \in \frac{\mathbb{Z}}{q} \text{ i.o.}\Bigg\} \quad (2.1)\end{aligned}$$

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

and

$$W_\tau^M(P_\alpha)[K] := \left\{ x \in [M, M+1] \colon \left| x - \frac{p}{q} \right| < \frac{1}{q^\tau} \text{ and } \left| P(x) + \alpha - \frac{r}{q} \right| < \frac{K}{q^\tau} \text{ i.o.} \right\}.$$

For simplicity, omit the square brackets in the above notation if $K = 1$.

With these definitions, Lemmas 2.1 and 2.2 amount to claiming that, for any integer M,

$$W_\tau^M(P_\alpha) \subset R_\tau^M(\alpha)[K_M] \subset W_\tau^M(P_\alpha)[2K_M].$$

It is now readily seen that, for any $\epsilon > 0$, the above inclusions imply that

$$W_\tau^M(P_\alpha) \subset R_{\tau-\epsilon}^M(\alpha) \subset W_{\tau-2\epsilon}^M(P_\alpha).$$

Defining

$$R_\tau(\alpha) := \bigcup_{M \in \mathbb{Z}} R_\tau^M(\alpha), \tag{2.2}$$

it follows that, for any $\epsilon > 0$,

$$W_\tau(P_\alpha) \subset R_{\tau-\epsilon}(\alpha) \subset W_{\tau-2\epsilon}(P_\alpha).$$

Thus, the following proposition has been proved.

Proposition 2.3. *For any $\tau > 0$, $\dim W_\tau(P_\alpha) \leqslant \lim_{\epsilon \to 0^+} \dim R_{\tau-\epsilon}(\alpha)$.*

Furthermore, the equality $\dim W_\tau(P_\alpha) = \dim R_\tau(\alpha)$ holds at any point of continuity of the function $\tau \mapsto \dim W_\tau(P_\alpha)$.

Since the function $\tau \mapsto \dim W_\tau(P_\alpha)$ is obviously decreasing, it defines a regulated function (that is, it admits at every point both left and right limit). Now, it is well known that the set of discontinuities of a regulated function is at most countable, from which it follows that, for almost all $\tau > 0$, $\dim W_\tau(P_\alpha) = \dim R_\tau(\alpha)$.

In fact, much more may be expected. Defining the set $W_\tau(f)$ for any function f in the same way as $W_\tau(P)$, one may indeed state this conjecture.

Conjecture 2.4. *For any smooth function f defined over $\mathbb{R}$, the map $\tau \mapsto \dim W_\tau(f)$ is continuous.*

Obviously, the statement may be extended both to higher dimensions and by weakening the assumption on the regularity of the function f. Note that, in the case of simultaneous approximation of independent quantities, the dimension function is known to be continuous in any case (see [**9**] for the specifics of this assertion). However, one cannot assume that the function $\tau \mapsto \dim W_\tau(f)$ is differentiable for any positive value of τ in the general case, as shown by the example of the circle $\mathbb{S}^1$. Indeed, combining the multi-dimensional extension of Dirichlet's theorem in Diophantine approximation, Remark 1.2 and Theorem 1.2, it is possible to compute the value of $\dim W_\tau(\mathbb{S}^1)$ for any $\tau > 0$:

$$\dim W_\tau(\mathbb{S}^1) = \begin{cases} 1 & \text{if } 0 \leqslant \tau \leqslant \frac{3}{2}, \\ (3-\tau)/\tau & \text{if } \frac{3}{2} < \tau \leqslant 2, \\ 1/\tau & \text{if } \tau > 2. \end{cases}$$

From Remark 1.2, this also holds true for any arc contained in $\mathbb{S}^1$. Thus, the function $\tau \mapsto \dim W_\tau(\mathbb{S}^1)$ is piecewise differentiable as a continuous piecewise rational function. It may be expected, as a generalization of Conjecture 2.4, that this behaviour holds true for any function $\tau \mapsto \dim W_\tau(f)$ provided that f is *regular enough*.

In what follows, Theorems 1.4 and 1.5 are proven for the set $R_\tau(\alpha)$. Since the bounds provided by these theorems are continuous in τ, it suffices to study $\dim R_\tau(\alpha)$ rather than dealing with $\dim R_{\tau-\epsilon}(\alpha)$ before letting ϵ tend to 0.

2.2. The congruential constraint

The condition

$$\frac{b}{q^d} + P\left(\frac{p}{q}\right) \in \frac{\mathbb{Z}}{q},$$

with b and p integers and q a positive integer, appears in the definition of the set $R_\tau(\alpha)$. Plainly, it amounts to the congruence equation

$$b \equiv -q^d P\left(\frac{p}{q}\right) \pmod{q^{d-1}} \tag{2.3}$$

having a solution. Since the reduction modulo q of (2.3) is

$$b \equiv a_d p^d \pmod{q}$$

(recall that the leading coefficient of $P(X)$ is $-a_d$), it should be obvious that

$$\tilde{R}_\tau(\alpha) \subset R_\tau(\alpha) \subset R^*_\tau(\alpha) \tag{2.4}$$

for any $\tau > 0$, where

$$R^*_\tau(\alpha) := \left\{ x \in \mathbb{R} \colon \left| x - \frac{p}{q} \right| < \frac{1}{q^\tau} \text{ and } \left| \alpha - \frac{b}{q^d} \right| < \frac{1}{q^\tau} \text{ with } b \equiv a_d p^d \ (\mathrm{mod}\, q) \text{ i.o.} \right\} \tag{2.5}$$

and where the set $\tilde{R}_\tau(\alpha)$ is defined in the same way as $R_\tau(\alpha)$ in (2.1) and (2.2) with the additional constraint $\gcd(q, pda_d) = 1$ on the denominators of the rational approximants.

In fact, the upper bound in Theorem 1.5 is established in § 5 for the set $R^*_\tau(\alpha)$, whereas Theorem 1.4 follows in an obvious way from the proof in § 4.1 that the set

$$I^*_\tau(P) := \left\{ \alpha \in (0,1) \colon \left| \alpha - \frac{b}{q^d} \right| < \frac{1}{q^\tau} \text{ with } b \in a_d G_d(q) \text{ i.o.} \right\} \tag{2.6}$$

has zero Lebesgue measure when $\tau > d+1$ (recall that $G_d(q)$ denotes the set of dth powers modulo q). Furthermore, the bound $d+1$ given by Theorem 1.4 cannot be trivially improved if it is shown that $I^*_\tau(P)$ contains a subset that is not of Lebesgue measure 0 when $\tau \leqslant d+1$.

To this end, it is proven in § 4.2 that the subset $\tilde{I}_\tau(P) \subset I^*_\tau(P)$ has full measure whenever $\tau \leqslant d+1$, where

$$\tilde{I}_\tau(P) := \left\{ \alpha \in (0,1) \colon \left| \alpha - \frac{b}{q^d} \right| < \frac{1}{q^\tau} \text{ with } b \in a_d G^\times_d(q) \text{ and } \gcd(q, da_d) = 1 \text{ i.o.} \right\} \tag{2.7}$$

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

and where $G_d^\times(q)$ denotes (with an abuse of notation) the set of *primitive* dth powers modulo q.

It should be noted that $\tilde{I}_\tau(P)$ is to the set $\tilde{R}_\tau(\alpha)$ as $I^*_\tau(P)$ is to the set $R^*_\tau(\alpha)$ in the following sense. Assume that $b \equiv a_d\tilde{p}^d \pmod q$ for some $\tilde{p} \in \mathbb{Z}$ satisfying $\gcd(q, \tilde{p}da_d) = 1$ as in the definition (2.7) of the set $\tilde{I}_\tau(P)$. From the Chinese remainder theorem, solving this congruence equation modulo q amounts to solving the same equation modulo $\pi^{\nu_\pi(q)}$ for any prime divisor π of q. Now, under the assumption that $\gcd(q, \tilde{p}da_d) = 1$, any solution $\tilde{p}$ of $b \equiv a_d\tilde{p}^d \pmod{\pi^{\nu_\pi(q)}}$ may be lifted, thanks to Hensel's lemma, to a unique solution p of the congruence equation (2.3) taken modulo $\pi^{\nu_\pi(q)(d-1)}$ ($d \geqslant 2$) such that π does not divide the product pda_d. Therefore, using once again the Chinese remainder theorem, a solution in $\tilde{p}$ to $b \equiv a_d\tilde{p}^d \pmod q$ satisfying $\gcd(q, \tilde{p}da_d) = 1$ may be lifted in a unique way to a solution p of (2.3) such that $\gcd(q, pda_d) = 1$ as in the definition of the set $\tilde{R}_\tau(\alpha)$.

3. Some auxiliary lemmas

In this section we collect various results that will be needed later.

3.1. Comparative growths of some arithmetical functions

For $n \geqslant 2$ an integer, let $\tau(n)$ be the number of divisors of n and let $\omega(n)$ be the number of *distinct* prime factors dividing n. If $n = \prod_{i=1}^r \pi_i^{\nu_i}$ is the prime factor decomposition of this integer, recall that

$$\omega(n) = r \quad \text{and} \quad \tau(n) = \prod_{i=1}^r (\nu_i + 1).$$

We now recall some results about comparative growth properties of these two arithmetical functions.

Lemma 3.1. *For any $\epsilon > 0$, $\tau(n) = o(n^\epsilon)$ and the average value of $\tau(n)$ is $\log n$, i.e.*

$$\frac{1}{n}\sum_{k=1}^{n} \tau(k) \underset{n\to+\infty}{\sim} \log n.$$

Proof. See [**7**, Theorems 315 and 320]. □

As is well known, the average value of $\omega(n)$ is asymptotic to $\log\log n$ when n tends to ∞ (see [**7**, § 22.11]). However, a stronger statement similar to Lemma 3.1 is needed in the proofs to come. To this end, the definition of the maximal order of an arithmetical function is introduced.

Definition 3.2. An arithmetical function f has *maximal* (respectively, *minimal*) *order* g if g is a positive non-decreasing arithmetical function such that

$$\limsup_{n\to+\infty} \frac{f(n)}{g(n)} = 1 \quad \left(\text{respectively, } \liminf_{n\to+\infty} \frac{f(n)}{g(n)} = 0\right).$$

For instance, it is not difficult to see that the identity function is both a minimal and a maximal order for Euler's totient function.

Lemma 3.3. *A maximal order for* $\omega(n)$ *is* $\log n/\log\log n$.
In particular, for any $\epsilon > 0$ *and any positive integer* m,

$$\omega(n) = o(\log n) \quad \text{and} \quad m^{\omega(n)} = o(n^{\epsilon}).$$

Proof. The first result is implicit in [**7**, p. 355]. The others then follow easily. □

3.2. Counting the number of power residues in a reduced system of residues

The congruence equations appearing in § 2.2 in the definition of the sets $\tilde{I}_\tau(P)$ and $I^*_\tau(P)$ on the one hand, and $\tilde{R}_\tau(\alpha)$ and $R^*_\tau(\alpha)$ on the other, involve power residues modulo an integer $q \geqslant 1$. The cardinality of such a set is now computed.

Let $n \geqslant 2$ and $d \geqslant 2$ be integers. Denote by $r_d(n)$ (respectively, $e_d(n)$) the number of distinct dth powers in the system of residues modulo n (respectively, in the *reduced* system of residues modulo n) and by $u_d(n)$ the number of dth roots of unity modulo n, that is,

$$\begin{aligned} r_d(n) &= \operatorname{Card}\{m^d \pmod n \colon m \in \mathbb{Z}/n\mathbb{Z}\},\\ e_d(n) &= \operatorname{Card}\{m^d \pmod n \colon m \in (\mathbb{Z}/n\mathbb{Z})^{\times}\},\\ u_d(n) &= \operatorname{Card}\{m \in \mathbb{Z}/n\mathbb{Z} \colon m^d \equiv 1 \pmod n\}. \end{aligned}$$

Furthermore, set $r_d(1) = e_d(1) = u_d(1) = 1$.

Remark 3.4. If $u(f, n)$ denotes the number of solutions in x of the congruence

$$f(x) := \sum_{k=0}^{d} a_k x^k \equiv 0 \pmod n$$

for a given polynomial $f \in \mathbb{Z}[X]$ of degree $d \geqslant 1$, it is well known that, as a consequence of the Chinese remainder theorem, $u(f, n)$ is a multiplicative function of n. It follows that $u_d(n)$ is multiplicative with respect to n for any fixed d.

In fact, the same holds true for $r_d(n)$ and $e_d(n)$.

Lemma 3.5. *For any fixed* d, *the functions* $r_d(n)$, $e_d(n)$ *and* $u_d(n)$ *are multiplicative with respect to* n.

Proof. See [**8**, Lemma 1] for the case of the functions $r_d(n)$ and $e_d(n)$. □

Explicit formulae may be given for $r_d(n)$, $e_d(n)$ and $u_d(n)$. Since these arithmetical functions are multiplicative when d is fixed, it suffices to give such formulae in the case where n is a power of a prime.

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

Proposition 3.6. *Let $n = \pi^k$ be a power of a prime number ($\pi \in \mathbb{P}$, $k \geqslant 1$ integer). The following equations then hold:*

$$e_d(n) = \frac{\varphi(\pi^k)}{u_d(\pi^k)} \quad \text{and} \quad r_d(n) = \frac{\varphi(\pi^k)}{u_d(\pi^k)} + \frac{\varphi(\pi^{k-d})}{u_d(\pi^{k-d})} + \cdots + \frac{\varphi(\pi^{k-md})}{u_d(\pi^{k-md})} + 1,$$

where m stands for the largest integer such that $k - md \geqslant 1$.

Furthermore,

$$u_d(n) = \begin{cases} \gcd(2d, \varphi(n)) & \text{if } 2 \mid d,\ \pi = 2 \text{ and } k \geqslant 3, \\ \gcd(d, \varphi(n)) & \text{otherwise.} \end{cases}$$

Proof. See [**8**, Lemmas 2 and 3]. □

Remark 3.7. Consider a partition of all numbers in the complete system of residues modulo π^k ($\pi \in \mathbb{P}$, $k \geqslant 1$ integer) into classes with regard to their divisibility by π^s and not π^{s+1}, that is, the numbers of the form $x\pi^s$ with $\gcd(x, \pi) = 1$ belong to the class numbered s, $0 \leqslant s \leqslant k$. As is clear from the proof of Proposition 3.6 in [**8**], the quantity $\varphi(\pi^{k-sd})/u_d(\pi^{k-sd})$ with $k - sd \geqslant 1$ counts the number of distinct elements modulo π^k obtained when taking the dth power of the numbers in the sth class. If $sd \geqslant k$, then the dth power of any element in the sth class is equal to 0 modulo π^k.

Furthermore, the proof of Proposition 3.6 also implies that, if $k - sd \geqslant 1$ and if $b \pmod{\pi^k}$ is the dth power of an element in the sth class, the number of solutions in x to the congruence equation $b \equiv x^d \pmod{\pi^k}$ is precisely $u_d(\pi^{k-sd})$.

4. The set $W_\tau(P_\alpha)$ when $\tau > d + 1$

Theorem 1.4 is now proved and the optimality of the lower bound $d+1$ appearing in this theorem is also studied.

4.1. Emptiness of the set for almost all $\alpha \in \mathbb{R}$

In order to establish the result of Theorem 1.4, recall that, from the discussion held in § 2.1 and from the inclusions (2.4), it suffices to prove that the set $R^*_\tau(\alpha)$ as defined in (2.5) is empty in the metric sense when $\tau > d + 1$. This in turn follows from the fact that, as a consequence of the convergent part of the Borel–Cantelli lemma, the set $I^*_\tau(P)$ as defined in (2.6) satisfies the same property.

To see this, first note that, for any $N \geqslant 1$, a cover of $I^*_\tau(P)$ is given by $\bigcup_{q \geqslant N} J^*_\tau(q)$, where

$$J^*_\tau(q) := \bigcup_{\substack{0 \leqslant b \leqslant q^d - 1 \\ b \in a_d G_d(q)}} \left(\frac{b}{q^d} - \frac{1}{q^\tau}, \frac{b}{q^d} + \frac{1}{q^\tau} \right). \tag{4.1}$$

If $\tau > d$ and $q \geqslant 1$ is large enough, $J^*_\tau(q)$ is a union of $|a_d G_d(q)| q^{d-1}$ non-overlapping intervals, each of length $2/q^\tau$, that is,

$$\lambda(J^*_\tau(q)) = \frac{2|a_d G_d(q)| q^{d-1}}{q^\tau}, \tag{4.2}$$

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

where λ denotes the Lebesgue measure on the real line. On the other hand, since the ring $a_d\mathbb{Z}/q\mathbb{Z}$ is isomorphic to $\mathbb{Z}/\tilde{q}\mathbb{Z}$, where $\tilde{q} = q/\gcd(q, a_d)$, the following relationships hold true:

$$r_d(\tilde{q}) := |G_d(\tilde{q})| = |a_d G_d(q)| \leqslant |G_d(q)| =: r_d(q). \tag{4.3}$$

In order to study the convergence of the series $\sum_{q\geqslant 1} \lambda(J^*_\tau(q))$, an upper bound (respectively, a lower bound) for $r_d(q)$ (respectively, for $r_d(\tilde{q})$) is established. Regarding the upper bound for $r_d(q)$, Lemma 3.5 and Proposition 3.6 imply that

$$r_d(q) = \prod_{\substack{\pi \mid q \\ \pi\in\mathbb{P}}} \left(1 + \sum_{s=0}^{m_q(\pi,d)} \frac{\varphi(\pi^{\nu_\pi(q)-sd})}{u_d(\pi^{\nu_\pi(q)-sd})}\right),$$

where $m_q(\pi, d) := \lfloor(\nu_\pi(q) - 1)/d\rfloor$. It is now easily checked that, for all $s \in [\![0, m_q(\pi, d)]\!]$,

$$\frac{\varphi(\pi^{\nu_\pi(q)-sd})}{u_d(\pi^{\nu_\pi(q)-sd})} \leqslant \frac{\varphi(\pi^{\nu_\pi(q)})}{u_d(\pi^{\nu_\pi(q)})},$$

and hence

$$\begin{aligned} r_d(q) &\leqslant \prod_{\substack{\pi \mid q \\ \pi\in\mathbb{P}}} \left[1 + \left(1 + \frac{\nu_\pi(q) - 1}{d}\right) \frac{\varphi(\pi^{\nu_\pi(q)})}{u_d(\pi^{\nu_\pi(q)})}\right] \\ &\leqslant 2^{\omega(q)} \frac{\varphi(q)}{u_d(q)} \prod_{\substack{\pi \mid q \\ \pi\in\mathbb{P}}} (1 + \nu_\pi(q)) \\ &= 2^{\omega(q)} \frac{\varphi(q)}{u_d(q)} \tau(q) \\ &\leqslant 2^{\omega(q)} \tau(q) q. \end{aligned} \tag{4.4}$$

As for the lower bound for $r_d(\tilde{q})$, first note that Lemma 3.5 and Proposition 3.6 lead to the estimate

$$1 \leqslant u_d(q) \leqslant (2d)^{\omega(q)}, \tag{4.5}$$

valid for all $q \geqslant 1$. One may then deduce that

$$\begin{aligned} r_d(\tilde{q}) \geqslant e_d(\tilde{q}) = \frac{\varphi(\tilde{q})}{u_d(\tilde{q})} &= \frac{\tilde{q}}{u_d(\tilde{q})} \prod_{\substack{\pi \mid \tilde{q} \\ \pi\in\mathbb{P}}} \left(1 - \frac{1}{\pi}\right) \\ &\geqslant \frac{\tilde{q}}{(4d)^{\omega(\tilde{q})}} \\ &\geqslant \frac{q}{|a_d|(4d)^{\omega(q)}}, \end{aligned} \tag{4.6}$$

the last inequality following from the definition of $\tilde{q}$.

Finally, the combination of the relationships (4.2), (4.3), (4.4) and (4.6) leads to the inequalities

$$\sum_{q\geqslant 1} \frac{1}{(4d)^{\omega(q)} q^{\tau-d}} \ll \sum_{q\geqslant 1} \lambda(J^*_\tau(q)) \ll \sum_{q\geqslant 1} \frac{2^{\omega(q)}\tau(q)}{q^{\tau-d}}. \tag{4.7}$$

From Lemmas 3.1 and 3.3, the right-hand side converges for any $\tau > d+1$, and hence $\lambda(I_\tau^*(P)) = 0$ for $\tau > d+1$. This bound is the best possible according to the convergent part of the Borel–Cantelli lemma, since the series $\sum_{q\geqslant 1} \lambda(J_\tau^*(q))$ diverges for $\tau \leqslant d+1$. This is indeed implied by (4.7) and the following general lemma.

Lemma 4.1. *Let n be a positive integer and let z be a positive real number. Define for any positive real number s the series*

$$L_z(s) := \sum_{\substack{q\geqslant 1\\ \gcd(q,n)=1}} \frac{z^{\omega(q)}}{q^s}.$$

The series $L_z(s)$ then converges if and only if $s > 1$.

Proof. Let χ_n be the Dirichlet principal character modulo n, i.e., for an integer $q \geqslant 1$,

$$\chi_n(q) = \begin{cases} 1 & \text{if } \gcd(n,q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then,

$$L_z(s) = \sum_{q\geqslant 1} \frac{\chi_n(q) z^{\omega(q)}}{q^s}.$$

Since $\chi_n(q) z^{\omega(q)}$ is a multiplicative arithmetical function, $L_z(s)$ admits an Euler product expansion given by

$$L_z(s) = \prod_{\pi\in\mathbb{P}} \left(1 + \sum_{k=1}^{+\infty} \frac{\chi_n(\pi) z^{\omega(\pi)}}{\pi^{ks}}\right) = \prod_{\substack{\pi\in\mathbb{P}\\ \gcd(\pi,n)=1}} \left(1 + \frac{z}{\pi^s - 1}\right). \tag{4.8}$$

Since only positive quantities are considered, $L_z(s)$ converges if and only if the right-hand side of (4.8) converges. Taking the logarithm of these equations, $L_z(s)$ is seen to converge if and only if

$$\sum_{l\in(\mathbb{Z}/n\mathbb{Z})^\times} \sum_{\substack{\pi\in\mathbb{P}\\ \pi\equiv l \ (\mathrm{mod}\ n)}} \frac{1}{\pi^s}$$

converges, which is the case if and only if, for all $l \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{\substack{\pi\in\mathbb{P}\\ \pi\equiv l \ (\mathrm{mod}\ n)}} \frac{1}{\pi^s}$$

converges. By Dirichlet's theorem on arithmetic progressions, for all $l \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{\substack{\pi\in\mathbb{P}\\ \pi\equiv l \ (\mathrm{mod}\ n)}} \frac{1}{\pi^s} \underset{s\to 1^+}{\sim} \frac{1}{\varphi(n)} \log\left(\frac{1}{s-1}\right).$$

This completes the proof. □

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

4.2. Optimality of the lower bound $d+1$

The divergence of the series $\sum_{q\geqslant 1}\lambda(J_\tau^*(q))$ for $\tau\leqslant d+1$ does not guarantee that the set $I_\tau^*(P)$ is not of Lebesgue measure 0, in which case the bound $d+1$ appearing in the statement of Theorem 1.4 could be trivially improved. This problem is now tackled by showing, as mentioned in the discussion in § 2.2, that the subset $\tilde{I}_\tau(P)$ of $I_\tau^*(P)$ as defined by (2.7) has full measure whenever $\tau\leqslant d+1$.

To this end, the author considered in [**1**] the theorem of Duffin and Schaeffer in Diophantine approximation [**5**], which generalizes the classical theorem of Khintchine to the case of any error function under the assumption that all the rational approximants are irreducible. He extended it to the case where the numerators and the denominators of the rational approximants were related by a congruential constraint stronger than coprimality (see [**1**, Theorem 1.2]). As a corollary of this extension, setting

$$s_d(q) := \frac{e_d(q)}{q} \tag{4.9}$$

for all integers $q\geqslant 1$ (see Lemma 3.5 and Proposition 3.6 for an expression of $e_d(q)$), the following result was also obtained.

Theorem 4.2 (Adiceam [1, Theorem 1.2]). *Let $(q_k)_{k\geqslant 1}$ be a strictly increasing sequence of positive integers and let $(\alpha_k)_{k\geqslant 1}$ be a sequence of positive real numbers. Assume that*

(a) $\sum_{k=1}^{+\infty}\alpha_k = +\infty$,

(b) $\sum_{k=1}^{n}\alpha_k s_d(q_k^d) > c\sum_{k=1}^{n}\alpha_k$ *for infinitely many positive integers n and a real number $c>0$,*

(c) $\gcd(q_k, a_d)=1$ *for all $k\geqslant 1$.*

Then, for almost all $\alpha\in\mathbb{R}$, there exist arbitrarily many relatively prime integers b_k and q_k such that

$$\left|\alpha-\frac{b_k}{q_k^d}\right| < \frac{\alpha_k}{q_k^d} \quad \text{and} \quad b_k\in a_d G_d^\times(q_k),$$

where $G_d^\times(q_k)$ was defined at the same time as the set $\tilde{I}_\tau(P)$ by (2.7).

One can deduce from Theorem 4.2 a stronger result than the one required to prove that the set $\tilde{I}_\tau(P)$ has full Lebesgue measure when $\tau\leqslant d+1$.

Corollary 4.3. *Let $s\in(0,1]$ and let m be a positive integer.*

Then, for almost all $\alpha\in\mathbb{R}$, there exist infinitely many integers q and b, $q\geqslant 1$, satisfying that

(i) $|\alpha - b/q^d| < 1/q^{d+s}$,

(ii) $b\in a_d G_d^\times(q)$,

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

(iii) $\gcd(q, da_d) = 1$,

(iv) $\omega(q) \leqslant m$.

In particular, $\lambda(\tilde{I}_\tau(P)) = \lambda(I^*_\tau(P)) = 1$ *when* $\tau \leqslant d+1$.

Proof. Maintaining the notation of Theorem 4.2, choose for the sequence $(q_k)_{k\geqslant 1}$ the successive elements of the set $\{n \in \mathbb{N}^* \colon \gcd(n, da_d) = 1 \text{ and } \omega(n) \leqslant m\}$ ordered increasingly, and for $(\alpha_k)_{k\geqslant 1}$ the sequence $(1/q_k^s)_{k\geqslant 1}$.

Then,

$$\sum_{k\geqslant 1} \alpha_k \geqslant \sum_{\substack{\pi\in\mathbb{P}\\ \pi\nmid da_d}} \frac{1}{\pi^s},$$

and the right-hand side is a divergent series for $s \in (0, 1]$. Furthermore, from (4.4) and (4.9) on the one hand and from the choice of the sequence $(q_k)_{k\geqslant 1}$ on the other, for any positive integer k,

$$s_d(q_k^d) = \frac{\varphi(q_k^d)}{q_k^d u_d(q_k^d)} \geqslant \frac{1}{(4d)^m} > 0.$$

Theorem 4.2 completes the proof. □

Remark 4.4. It is not difficult to see that, for almost all $\alpha \in \mathbb{R}$, the sequence of denominators $(q_k)_{k\geqslant 1}$ in Corollary 4.3 may be chosen in such a way that (i), (ii) and (iii) hold and such that the sequence $(\omega(q_k))_{k\geqslant 1}$ is unbounded. Indeed, first define, for any positive integer m, the sequence $(n_{m,k})_{k\geqslant 1}$ as being the sequence of the successive elements of the set

$$\{n \in \mathbb{N}^* \colon \gcd(n, da_d) = 1 \text{ and } \omega(n) = m\}$$

ordered increasingly. Let $(\alpha_{m,k})_{k\geqslant 1}$ be the sequence $(1/n_{m,k}^s)_{k\geqslant 1}$, where $s \in (0, 1]$, and let

$$D_m := \{\alpha \in (0, 1] \colon \text{(i), (ii) and (iii) hold true with } \omega(q) = m \text{ i.o.}\}.$$

Denote by $(\pi_i)_{i\geqslant 1}$ the increasing sequence of primes. Since, for all $k \geqslant 1$,

$$s_d(n_{m,k}^d) \geqslant \frac{1}{(4d)^m} > 0 \quad \text{and} \quad \sum_{k\geqslant 1} \alpha_{m,k} \geqslant \sum_{\substack{1\leqslant i_1<\cdots<i_m\\ \pi_{i_j}\nmid 2da_d}} \frac{1}{(\pi_{i_1}\cdots\pi_{i_m})^s},$$

which is a divergent series, similar reasoning to that in the proof of Corollary 4.3 shows that $\lambda(D_m) = 1$ for any $m \in \mathbb{N}^*$. Then, $\lambda(\cap_{m\geqslant 1} D_m) = 1$, and the result follows.

5. Upper bound for the Hausdorff dimension of $W_\tau(P_\alpha)$ when τ lies in the interval $(d, d+1]$

Theorem 1.5 is proven in this section after the study of the asymptotic behaviour of the number of solutions of Diophantine inequalities.

5.1. Asymptotic behaviour of the number of solutions of Diophantine inequalities

Given a sequence of intervals $(I_q)_{q\geqslant 1}$ inside the unit interval and a real number α, let $\mathcal{N}(Q,\alpha)$ denote the number of integers $q \leqslant Q$ such that $q\alpha \in I_q \pmod 1$, that is,

$$\mathcal{N}(Q,\alpha) := \operatorname{Card}\{q \in [\![1,Q]\!] : q\alpha \in I_q \pmod 1\}. \tag{5.1}$$

The asymptotic behaviour of $\mathcal{N}(Q,\alpha)$ as Q tends to ∞ has been studied by Sprindžuk, who exploited ideas from the works of Schmidt and Rademacher on the theory of orthogonal series (see [**10**] for further details).

Theorem 5.1 (Sprindžuk and Silverman [10, Theorem 18]). *Let $(I_q)_{q\geqslant 1}$ be a sequence of intervals inside the unit interval $[0,1]$ such that*

$$\sum_{q=1}^{+\infty} \lambda(I_q) = +\infty.$$

For any real number α, define $\mathcal{N}(Q,\alpha)$ as in (5.1).

Then, for almost all $\alpha \in \mathbb{R}$,

$$\mathcal{N}(Q,\alpha) = \Phi(Q) + O(\sqrt{\Psi(Q)}(\log \Psi(Q))^{3/2+\kappa}),$$

where

$$\Phi(Q) := \sum_{q=1}^{Q} \lambda(I_q), \qquad \Psi(Q) := \sum_{q=1}^{Q} \lambda(I_q)\tau(q)$$

and $\kappa > 0$ is arbitrary.

The notation of Theorem 5.1 is maintained in the next corollary.

Corollary 5.2. *Under the assumptions of Theorem 5.1, suppose that one of the following conditions holds.*

(i) $\Phi(Q) \gg Q^{\delta}$ *for all $Q > 0$, for some $\delta > 0$.*

(ii) $\lambda(I_q)$ *decreases monotonically and $\Phi(Q) \gg (\log Q)^{1+\delta}$ for all $Q > 0$, for some $\delta > 0$.*

Then,

$$\mathcal{N}(Q,\alpha) \sim \sum_{q=1}^{Q} \lambda(I_q) \quad \text{as } Q \to +\infty.$$

Proof. If condition (i) holds, then the result is a simple consequence of Theorem 5.1 and the fact that $\tau(q) \ll q^{\epsilon}$ for any $\epsilon > 0$ (see Lemma 3.1).

If condition (ii) holds, since $\sum_{1\leqslant k\leqslant q} \tau(k) \ll q \log q$ by Lemma 3.1, making an Abel transformation in the expression for $\Psi(Q)$ shows that $\Psi(Q) \ll \Phi(Q) \log Q$. The conclusion also follows in this case. □

Remark 5.3. In the statement of Theorem 5.1, no restrictions whatsoever are imposed on the way the intervals I_q vary with q. Therefore, the condition $q\alpha \in I_q \pmod 1$ appearing in the definition (5.1) of $\mathcal{N}(Q,\alpha)$ may be regarded as holding for the numbers q_k of an arbitrarily increasing sequence. Corollary 5.2 is then still valid for such a sequence $(q_k)_{k\geqslant 1}$.

5.2. The proof of Theorem 1.5

In order to prove Theorem 1.5, recall that it suffices to establish the upper bound for the Hausdorff dimension of $W_\tau(P_\alpha)$ in the case of the set $R^*_\tau(\alpha)$ as defined in (2.5). Without loss of generality, it may be assumed that $\tau \in (d, d+1)$, the result in the case $\tau = d+1$ following from an obvious passage to the limit. Furthermore, since the set $R^*_\tau(\alpha)$ is invariant when translated by an integer, it suffices to prove Theorem 1.5 for the subset $R^*_\tau(\alpha) \cap [0,1]$, which, for the sake of simplicity, is still denoted by $R^*_\tau(\alpha)$ in what follows.

The fact that the fractions p/q are not necessarily irreducible in the definition of the set $R^*_\tau(\alpha)$ induces considerable difficulties, as one needs to take into account the order of magnitude of the highest common factor between p and q to compute $\dim R^*_\tau(\alpha)$. In fact, it is more convenient to work with $\gcd(b,q)$. To this end, define for $\epsilon \in [0,1]$ and $\delta > 0$ the set $R^*_\tau(\alpha,\epsilon,\delta)$ as

$$\Big\{x \in [0,1]\colon \left|x - \frac{p}{q}\right| < \frac{1}{q^\tau} \text{ and } \left|\alpha - \frac{b}{q^d}\right| < \frac{1}{q^\tau} \\ \text{with } b \equiv a_d p^d \pmod q \text{ i.o. with } q^\epsilon \leqslant \gcd(b,q) < q^{\epsilon+\delta}\Big\}. \quad (5.2)$$

It should be obvious that

$$R^*_\tau(\alpha) = \bigcup_{0\leqslant\epsilon<\epsilon+\delta\leqslant 1} R^*_\tau(\alpha,\epsilon,\delta).$$

Furthermore, let $I^*_\tau(\alpha,\epsilon,\delta)$ be the set

$$I^*_\tau(\alpha,\epsilon,\delta) := \Big\{\alpha \in (0,1)\colon \left|\alpha - \frac{b}{q^d}\right| < \frac{1}{q^\tau} \text{ i.o.} \\ \text{with } b \in a_d G_d(q) \text{ and } q^\epsilon \leqslant \gcd(b,q) < q^{\epsilon+\delta}\Big\}. \quad (5.3)$$

Notation. Given $\epsilon \in [0,1]$ and $\delta > 0$, $\mathcal{N}(Q,\alpha,\epsilon,\delta)$ denotes the counting function of the set $I^*_\tau(\alpha,\epsilon,\delta)$, and can be defined more conveniently in this case as

$$\mathcal{N}(Q,\alpha,\epsilon,\delta) := \operatorname{Card}\{q^d \in [\![1,Q]\!]\colon |q^d\alpha - b| < q^{d-\tau} \text{ i.o.} \\ \text{with } b \in a_d G_d(q) \text{ and } q^\epsilon \leqslant \gcd(b,q) < q^{\epsilon+\delta}\}. \quad (5.4)$$

With these definitions and this notation at one's disposal, one may now state the following lemma.

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

Lemma 5.4. *Assume that $\tau \in (d, d+1)$. The set $R^*_\tau(\alpha, \epsilon, \delta)$ is then empty for almost all $\alpha \in [0,1]$ if $\epsilon > d+1-\tau$.*

Furthermore, if $0 \leqslant \epsilon < \epsilon + \delta < d+1-\tau$, then, for almost all $\alpha \in [0,1]$,

$$Q^{d+1-\tau-\epsilon-\delta-\mu} \ll \mathcal{N}(Q, \alpha, \epsilon, \delta) \ll Q^{d+1-\tau-\epsilon+\nu},$$

where $\mu, \nu > 0$ are arbitrarily small.

Proof. To demonstrate the first part of the statement, it suffices to prove that the set $I^*_\tau(\alpha, \epsilon, \delta)$ is empty in the metric sense as soon as $\epsilon > d+1-\tau$. With this goal in mind, define

$$B_P(q, \epsilon, \delta) := \{b \pmod q \colon b \in a_d G_d(q) \text{ and } q^\epsilon \leqslant \gcd(b, q) < q^{\epsilon+\delta}\}$$

and

$$J^*_\tau(q, \epsilon, \delta) := \bigcup_{\substack{0 \leqslant b \leqslant q^d - 1 \\ b \in B_P(q,\epsilon,\delta)}} \left(\frac{b}{q^d} - \frac{1}{q^\tau}, \frac{b}{q^d} + \frac{1}{q^\tau} \right) \tag{5.5}$$

in such a way that $\bigcup_{q \geqslant N} J^*_\tau(q, \epsilon, \delta)$ is a cover of $I^*_\tau(\alpha, \epsilon, \delta)$ for any $N \geqslant 1$.

Since

$$|B_P(q, \epsilon, \delta)| = \sum_{\substack{a \mid q \\ q^\epsilon \leqslant a < q^{\epsilon+\delta}}} \mathrm{Card}\{b \pmod q \colon b \in a_d G_d(q) \text{ and } \gcd(b, q) = a\},$$

it should be clear that

$$|B_P(q, \epsilon, \delta)| = \sum_{\substack{a \mid q \\ q^\epsilon \leqslant a < q^{\epsilon+\delta}}} \mathrm{Card}\{b \pmod q \colon b \in G_d(q) \text{ and } \gcd(b, q) = a\}$$

if $\gcd(a_d, q) = 1$, and that

$$|B_P(q, \epsilon, \delta)| \leqslant \sum_{\substack{a \mid q \\ q^\epsilon \leqslant a < q^{\epsilon+\delta}}} \mathrm{Card}\{b \pmod q \colon b \in G_d(q) \text{ and } \gcd(b, q) = a\}$$

if $\gcd(a_d, q) > 1$.

Now, if a divides q, the ring $a\mathbb{Z}/q\mathbb{Z}$ is isomorphic to $\mathbb{Z}/\tilde{q}\mathbb{Z}$, where $\tilde{q} = q/a$. Therefore, for such an integer a,

$$\begin{aligned} \mathrm{Card}\{b \pmod q \colon b \in G_d(q) \text{ and } \gcd(b, q) = a\} &= \mathrm{Card}\left\{b \left(\mathrm{mod}\, \frac{q}{a}\right) \colon b \in G_d\left(\frac{q}{a}\right)\right\} \\ &:= r_d\left(\frac{q}{a}\right) \end{aligned}$$

from the definition of $r_d(n)$ in § 3.2. Therefore,

$$|B_P(q, \epsilon, \delta)| = \sum_{\substack{a \mid q \\ q^\epsilon \leqslant a < q^{\epsilon+\delta}}} r_d\left(\frac{q}{a}\right) = \sum_{\substack{l \mid q \\ q^{1-\epsilon-\delta} < l \leqslant q^{1-\epsilon}}} r_d(l) \tag{5.6}$$

if $\gcd(a_d, q) = 1$, and

$$|B_P(q,\epsilon,\delta)| \leqslant \sum_{\substack{a|q \\ q^{\epsilon} \leqslant a < q^{\epsilon+\delta}}} r_d\left(\frac{q}{a}\right) = \sum_{\substack{l|q \\ q^{1-\epsilon-\delta} < l \leqslant q^{1-\epsilon}}} r_d(l)$$

if $\gcd(a_d, q) > 1$.

From (4.4) and (4.6), it is readily checked that

$$\frac{q^{1-\epsilon-\delta}}{(4d)^{\omega(q)}} \leqslant \sum_{\substack{l|q \\ q^{1-\epsilon-\delta} < l \leqslant q^{1-\epsilon}}} r_d(l) \leqslant 2^{\omega(q)}\tau(q)^2 q^{1-\epsilon}. \tag{5.7}$$

Thus, combining (5.5), (5.6) and (5.7), it follows that, if $\gcd(a_d, q) = 1$,

$$\frac{2q^{d-\epsilon-\delta}}{(4d)^{\omega(q)}q^{\tau}} \leqslant \lambda(J_\tau^*(q,\epsilon,\delta)) = \frac{2|B_P(q,\epsilon,\delta)|q^{d-1}}{q^{\tau}} \leqslant \frac{2\cdot 2^{\omega(q)}\tau(q)^2 q^{d-\epsilon}}{q^{\tau}}. \tag{5.8}$$

On the one hand, Lemmas 3.1 and 3.3 imply that the right-hand side of (5.8) is the general term of a series that converges whenever $\epsilon > 1 + d - \tau$; hence, from the convergent part of the Borel–Cantelli lemma, $\lambda(I_\tau^*(q,\epsilon,\delta)) = 0$ as soon as $\epsilon > 1 + d - \tau$.

On the other hand, Lemmas 3.1 and 3.3 and (5.8) also imply that, for any $\mu, \nu > 0$,

$$\begin{aligned} Q^{1+d-\tau-\epsilon-\delta-\mu} &\ll \sum_{\substack{1\leqslant q\leqslant Q \\ \gcd(a_d,q)=1}} \frac{1}{q^{\tau-d+\epsilon+\delta+\mu}} \\ &\ll \sum_{1\leqslant q\leqslant Q} \lambda(J_\tau^*(q,\epsilon,\delta)) \\ &\ll \sum_{1\leqslant q\leqslant Q} \frac{1}{q^{\tau-d+\epsilon-\nu}} \\ &\ll Q^{1+d-\tau-\epsilon+\nu}. \end{aligned}$$

To conclude the proof, it suffices to note that if μ is chosen so small that $1 + d - \tau - \epsilon - \delta - \mu > 0$, then, from Corollary 5.2,

$$\mathcal{N}(Q,\alpha,\epsilon,\delta) \sim \sum_{1\leqslant q\leqslant Q} \lambda(J_\tau^*(q,\epsilon,\delta)) \quad \text{as } Q \to +\infty$$

almost everywhere. □

Corollary 5.5. *Let $\tau \in (d, d+1)$. Assume that ϵ and δ are such that $0 \leqslant \epsilon < \epsilon + \delta < 1 + d - \tau$. Then, for almost all $\alpha \in [0,1]$,*

$$\dim R_\tau^*(\alpha,\epsilon,\delta) \leqslant \frac{1+d-\tau+\delta}{\tau}.$$

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

Proof. By the definition of the set $R_\tau^*(\alpha,\epsilon,\delta)$ in (5.2), its s-dimensional Hausdorff measure $\mathcal{H}^s(R_\tau^*(\alpha,\epsilon,\delta))$ satisfies the inequality

$$\mathcal{H}^s(R_\tau^*(\alpha,\epsilon,\delta)) \leqslant \sum_{q\geqslant 1}\sum_{b}\sum_{\substack{0\leqslant p\leqslant q-1\\ b\equiv a_d p^d \ (\mathrm{mod}\ q)}} \frac{2}{q^{\tau s}}, \tag{5.9}$$

where the second sum runs over all the possible integers b such that

$$\left|\alpha - \frac{b}{q^d}\right| < \frac{1}{q^\tau} \quad \text{and} \quad q^\epsilon \leqslant \gcd(b,q) < q^{\epsilon+\delta}. \tag{5.10}$$

Note that, provided that $q \geqslant 1$ is large enough and that $\tau > d$, there exists at most one integer b that is a solution to (5.10). So, let $(q_n)_{n\geqslant 1}$ denote the strictly increasing sequence of denominators q_n such that (5.10) is satisfied for some integer b_n. From the definition of this sequence, (5.9) may be rewritten as

$$\mathcal{H}^s(R_\tau^*(\alpha,\epsilon,\delta)) \ll \sum_{n\geqslant 1}\frac{c_n}{q_n^{\tau s}}, \tag{5.11}$$

where $c_n := \mathrm{Card}\{p \pmod{q_n}\colon b_n \equiv a_d p^d \pmod{q_n}\}$.

In order to compute the value of c_n, first note that, from the reasoning developed in Remark 3.4, c_n is multiplicative in q_n (i.e. $c_{nm} = c_n c_m$ whenever $\gcd(q_n,q_m) = 1$). Consider now the equation $b_n \equiv a_d p^d \pmod{\pi^{\nu_\pi(q_n)}}$, where π is any prime divisor of q_n.

- If $b_n \equiv 0 \pmod{\pi^{\nu_\pi(q_n)}}$, then the equation $a_d p^d \equiv 0 \pmod{\pi^{\nu_\pi(q_n)}}$ amounts to $d\nu_\pi(p) + \nu_\pi(a_d) \geqslant \nu_\pi(q_n)$. It is readily checked that the number of solutions in $p \pmod{q_n}$ to this equation is

$$\pi^{\nu_\pi(q_n)} - \pi^{k_d(n,\pi)}, \quad \text{where } k_d(n,\pi) := \left\lceil \frac{(\nu_\pi(q_n)-\nu_\pi(a_d))_+}{d}\right\rceil.$$

- If $b_n \not\equiv 0 \pmod{\pi^{\nu_\pi(q_n)}}$, then the equation $b_n \equiv a_d p^d \pmod{\pi^{\nu_\pi(q_n)}}$ amounts to

$$p^d \equiv \frac{b_n}{\pi^{\nu_\pi(a_d)}}\left(\frac{a_d}{\pi^{\nu_\pi(a_d)}}\right)^{-1} \pmod{\pi^{\nu_\pi(q_n)-\nu_\pi(a_d)}},$$

  where the division by $\pi^{\nu_\pi(a_d)}$ denotes ordinary integer division, while multiplicative inversion is performed in $\mathbb{Z}/(\pi^{\nu_\pi(q_n)-\nu_\pi(a_d)})\mathbb{Z}$. Using the terminology introduced in Remark 3.7, the class of any solution $p \pmod{\pi^{\nu_\pi(q_n)-\nu_\pi(a_d)}}$ to this equation has to be $(\nu_\pi(b_n)-\nu_\pi(a_d))/d$. Therefore, from Remark 3.7, the number of solutions in $p \pmod{\pi^{\nu_\pi(q_n)-\nu_\pi(a_d)}}$ to this equation is

$$u_d(\pi^{\nu_\pi(q_n)-\nu_\pi(a_d)-d(\nu_\pi(b_n)-\nu_\pi(a_d))/d}) = u_d(\pi^{\nu_\pi(q_n)-\nu_\pi(b_n)}) \leqslant u_d(\pi^{\nu_\pi(q_n)})$$

  (see Proposition 3.6 for this last inequality).

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

All things considered,

$$c_n \leqslant \prod_{\substack{\pi | q_n \\ b_n \equiv 0 \ (\mathrm{mod}\ \pi^{\nu_\pi(q_n)})}} \pi^{\nu_\pi(q_n)} \prod_{\substack{\pi | q_n \\ b_n \not\equiv 0 \ (\mathrm{mod}\ \pi^{\nu_\pi(q_n)})}} u_d(\pi^{\nu_\pi(q_n)}) \leqslant \gcd(b_n, q_n) u_d(q_n).$$

Now, from the definition of the set $R^*_\tau(\alpha, \epsilon, \delta)$, it may be assumed that $\gcd(b_n, q_n) \leqslant q_n^{\epsilon+\delta}$. Therefore, using (4.5) and Lemma 3.3, it is readily seen that (5.11) implies that

$$\mathcal{H}^s(R^*_\tau(\alpha, \epsilon, \delta)) \ll \sum_{n \geqslant 1} \frac{1}{q_n^{\tau s - \epsilon - \delta - \gamma}} \tag{5.12}$$

for arbitrarily small $\gamma > 0$. Since $\mathcal{N}(q_n, \alpha, \epsilon, \delta) = n$ by the definition of the sequence $(q_n)_{n \geqslant 1}$, Lemma 5.4 leads to the estimate

$$n^{1/(d+1-\tau-\epsilon+\gamma)} \ll q_n,$$

valid for almost all $\alpha \in [0, 1]$ and for arbitrarily small $\gamma > 0$. Thus,

$$\mathcal{H}^s(R^*_\tau(\alpha, \epsilon, \delta)) \ll \sum_{n \geqslant 1} \frac{1}{n^{(\tau s - \epsilon - \delta - \gamma)/(d+1-\tau-\epsilon+\gamma)}},$$

which is a convergent series for $s \geqslant (d + 1 - \tau + \delta + 2\gamma)/\tau$, that is,

$$\dim R^*_\tau(\alpha, \epsilon, \delta) \leqslant \frac{d + 1 - \tau + \delta + 2\gamma}{\tau}.$$

The result follows on letting γ tend to 0. □

The proofs of Lemma 5.4 and Corollary 5.5 rely strongly on the fact that, when $\epsilon < 1 + d - \tau$, it is always possible to choose $\delta > 0$ and $\mu > 0$ so small that $1 + d - \tau - \epsilon - \delta - \mu > 0$. While Lemma 5.4 also implies that the set $R^*_\tau(\alpha, \epsilon, \delta)$ is empty in the metric sense whenever $\epsilon > 1 + d - \tau$, this leaves a gap corresponding to the case where $\epsilon = 1 + d - \tau$. This limit case is now studied.

Since $R^*_\tau(\alpha, \epsilon, \delta) = \emptyset$ for almost all $\alpha \in [0, 1]$ when $\epsilon > 1 + d - \tau$, it should be clear that $R^*_\tau(\alpha, 1 + d - \tau, \delta) = R^*_\tau(\alpha, 1 + d - \tau, \mu)$ for any $\delta, \mu > 0$, the equality holding true in the metric sense. Denote by $R^*_\tau(\alpha, 1 + d - \tau)$ the common set determined by these different values of $\delta > 0$ and $\mu > 0$, i.e.

$$R^*_\tau(\alpha, 1 + d - \tau) := \bigcap_{\delta > 0} R^*_\tau(\alpha, 1 + d - \tau, \delta).$$

In other words, $R^*_\tau(\alpha, 1 + d - \tau) = R^*_\tau(\alpha, 1 + d - \tau, \delta)$ for any $\delta > 0$ and for almost all $\alpha \in [0, 1]$. In a similar way, let

$$I^*_\tau(\alpha, 1 + d - \tau) := \bigcap_{\delta > 0} I^*_\tau(\alpha, 1 + d - \tau, \delta).$$

Thus, $I^*_\tau(\alpha, 1 + d - \tau)$ is to $R^*_\tau(\alpha, 1 + d - \tau)$ as $I^*_\tau(\alpha, \epsilon, \delta)$ is to $R^*_\tau(\alpha, \epsilon, \delta)$ when $0 \leqslant \epsilon < \epsilon + \delta < 1 + d - \tau$, these last two sets having been defined by (5.2) and (5.3).

Notation. The quantity $\mathcal{N}(Q,\alpha,1+d-\tau)$ denotes the counting function of the set $I^*_\tau(\alpha,1+d-\tau)$ defined in a similar way as in (5.4).

As might be expected, the asymptotic behaviour of the function $\mathcal{N}(Q,\alpha,1+d-\tau)$ is different from that of $\mathcal{N}(Q,\alpha,\epsilon,\delta)$ when $0\leqslant\epsilon<\epsilon+\delta<1+d-\tau$.

Lemma 5.6. *Assume that $\tau\in(d,d+1)$. Then, for almost all $\alpha\in\mathbb{R}$,*

$$\mathcal{N}(Q,\alpha,1+d-\tau)\ll Q^\mu,$$

where $\mu>0$ is arbitrarily small.

Proof. Let $\delta>0$. Define $J^*_\tau(q,1+d-\tau,\delta)$ as in (5.5). The upper bound for $\lambda(J^*_\tau(q,1+d-\tau,\delta))$ provided by (5.8) then still holds, namely,

$$\lambda(J^*_\tau(q,1+d-\tau,\delta))\leqslant\frac{2\cdot 2^{\omega(q)}\tau(q)^2}{q}.$$

Therefore, since $2^{\omega(q)}=o(q^\mu)$ and $\tau(q)=o(q^\mu)$ for any $\mu>0$ from Lemmas 3.1 and 3.3, for all $Q\geqslant 1$,

$$\Phi(Q):=\sum_{q=1}^{Q}\lambda(J^*_\tau(q,1+d-\tau,\delta))\ll\sum_{q=1}^{Q}\frac{1}{q^{1-3\mu}}\ll Q^{3\mu}$$

and, in a similar way,

$$\Psi(Q):=\sum_{q=1}^{Q}\lambda(J^*_\tau(q,1+d-\tau,\delta))\tau(q)\ll Q^{4\mu}.$$

Now, $\bigcup_{q\geqslant N}J^*_\tau(q,1+d-\tau,\delta)$ is a cover of $I^*_\tau(\alpha,1+d-\tau,\delta)$ for any $N\geqslant 1$. Since the latter set is equal to $I^*_\tau(\alpha,1+d-\tau)$ for almost all $\alpha\in[0,1]$, it follows from Theorem 5.1 that, for almost all $\alpha\in[0,1]$,

$$\mathcal{N}(Q,\alpha,1+d-\tau)=\Phi(Q)+O(\sqrt{\Psi(Q)}(\log\Psi(Q))^{3/2+\kappa})\ll Q^{3\mu},$$

where $\kappa>0$ has been chosen arbitrarily. □

Corollary 5.7. *Assume that $\tau\in(d,d+1)$. Then, for almost all $\alpha\in[0,1]$,*

$$\dim R^*_\tau(\alpha,1+d-\tau)\leqslant\frac{1+d-\tau}{\tau}.$$

Proof. Let $\delta>0$. Denote by $(q_n)_{n\geqslant1}$ the strictly increasing sequence of denominators q_n such that (5.10) with $\epsilon=1+d-\tau$ is satisfied for some integer b_n. The inequality (5.12) then still holds for the set $R^*_\tau(\alpha,1+d-\tau,\delta)$, namely,

$$\mathcal{H}^s(R^*_\tau(\alpha,1+d-\tau,\delta))\ll\sum_{n\geqslant1}\frac{1}{q_n^{\tau s-1-d+\tau-\delta-\gamma}}$$

for arbitrarily small $\gamma>0$.

https://doi.org/10.1017/S0013091514000169 Published online by Cambridge University Press

Since $I^*_\tau(\alpha, 1+d-\tau, \delta) = I^*_\tau(\alpha, 1+d-\tau)$ for almost all $\alpha \in [0,1]$, the counting functions of these two sets have the same asymptotic behaviour, and hence, from Lemma 5.6,

$$n = \mathcal{N}(q_n, \alpha, 1+d-\tau) \ll q_n^\mu$$

almost everywhere, with $\mu > 0$ arbitrary. Therefore, for almost all $\alpha \in [0,1]$,

$$\mathcal{H}^s(R^*_\tau(\alpha, 1+d-\tau)) \ll \sum_{n \geqslant 1} \frac{1}{n^{(\tau s - 1 - d + \tau - \delta - \gamma)/\mu}},$$

which is a convergent series for $s \geqslant (1+d-\tau+\delta+\gamma+\mu)/\tau$, that is,

$$\dim R^*_\tau(\alpha, 1+d-\tau) \leqslant \frac{d+1-\tau+\delta+\gamma+\mu}{\tau}.$$

The result follows on letting γ, δ and μ tend to 0. □

Completion of the proof of Theorem 1.5. In order to prove that $\dim R^*_\tau(\alpha) \leqslant (d+1-\tau)/\tau$ for almost all $\alpha \in [0,1]$ when $\tau \in (d, d+1)$, first recall that, from Lemma 5.4, the equality

$$R^*_\tau(\alpha) = \left(\bigcup_{0 \leqslant \epsilon < \epsilon+\delta < 1+d-\tau} R^*_\tau(\alpha, \epsilon, \delta) \right) \cup R^*_\tau(\alpha, 1+d-\tau)$$

holds almost everywhere. Corollary 5.7 also implies that it suffices to prove that

$$\dim \left(\bigcup_{0 \leqslant \epsilon < \epsilon+\delta < 1+d-\tau} R^*_\tau(\alpha, \epsilon, \delta) \right) \leqslant \frac{1+d-\tau}{\tau}$$

for almost all $\alpha \in [0,1]$ when τ lies in the interval $(d, d+1)$.

To this end, consider a strictly increasing sequence $(\beta_p)_{p \geqslant 0}$ of real numbers from the interval $(0, 1+d-\tau)$ tending to $1+d-\tau$ as p tends to ∞. It should then be obvious that

$$\bigcup_{0 \leqslant \epsilon < \epsilon+\delta < 1+d-\tau} R^*_\tau(\alpha, \epsilon, \delta) = \bigcup_{p \geqslant 0} R^*_\tau(\alpha)[p], \quad \text{where } R^*_\tau(\alpha)[p] := \bigcup_{0 \leqslant \epsilon < \epsilon+\delta \leqslant \beta_p} R^*_\tau(\alpha, \epsilon, \delta).$$

Given $p \in \mathbb{N}$, let $(\epsilon_p(k))_{0 \leqslant k \leqslant n}$ be the finite sequence subdividing the interval $[0, \beta_p]$ into $n \geqslant 1$ intervals of equal length $\delta_p(n)$ and satisfying

$$\epsilon_p(0) = 0 \quad \text{and} \quad \epsilon_p(n) = \beta_p = \epsilon_p(n-1) + \delta_p(n).$$

Then,

$$R^*_\tau(\alpha)[p] = \bigcup_{k=0}^{n-1} R^*_\tau(\alpha, \epsilon_p(k), \delta_p(n))$$

for any regular subdivision $(\epsilon_p(k))_{0 \leqslant k \leqslant n}$ of $[0, \beta_p]$ into $n \geqslant 1$ intervals. Thus, from Corollary 5.5,

$$\dim R^*_\tau(\alpha)[p] = \sup_{0 \leqslant k \leqslant n-1} \dim R^*_\tau(\alpha, \epsilon_p(k), \delta_p(n)) \leqslant \frac{d+1-\tau+\delta_p(n)}{\tau},$$

which holds true for almost all $\alpha \in [0,1]$ and for any $n \geqslant 1$. On letting n tend to ∞, $\delta_p(n)$ tends to 0 and it follows that, outside a zero Lebesgue measure set,

$$\dim R^*_\tau(\alpha)[p] \leqslant \frac{1+d-\tau}{\tau}$$

when $\tau \in (d, d+1)$. Since the set $R^*_\tau(\alpha)$ is the countable union of $R^*_\tau(\alpha, 1+d-\tau)$ and of $R^*_\tau(\alpha)[p]$ ($p \in \mathbb{N}$) for almost all $\alpha \in [0,1]$, this completes the proof. □

6. Concluding remarks

We conclude the paper by stating some remarks on the method developed in this paper and the relevance of the results obtained.

(1) The upper bound for the Hausdorff dimension of the set $W_\tau(P_\alpha)$ stated in Theorem 1.5 is easily seen to be non-optimal as soon as $\tau < d-1$, as it is superseded by the Hausdorff dimension of the set of τ-well-approximable numbers given by the theorem of Jarník and Besicovitch: if W_τ denotes the latter set, then $W_\tau(P_\alpha) \subset W_\tau$ for any $\tau > 0$, and $\dim W_\tau = 2/\tau$ whenever $\tau > 2$.

Now, if $\tau \in [d-1, d]$, the study of the case $d = 3$ also tends to provide evidence that the upper bound $(1+d-\tau)/\tau$ is still not relevant in the general case. Indeed, when $d = 3$, on letting τ tend to 2 from above (respectively, from below) in Theorem 1.5 (respectively, in Theorem 1.6), the upper bound thus found for $\lim_{\tau \to 2^+} \dim W_\tau(P_\alpha)$ is clearly seen to be non-optimal.

More generally, the actual Hausdorff dimension of the set of τ-well-approximable points lying on a polynomial curve when τ is larger than 2 and less than the degree of the polynomial remains an open problem for which no solution is known (see also [**2**] for another mention of this problem).

(2) As mentioned in § 1, the upper bound for $\dim W_\tau(P_\alpha)$ given by Theorem 1.5 is more than likely the actual value for the Hausdorff dimension of $W_\tau(P_\alpha)$ for almost all $\alpha \in [0,1]$ when τ lies in the interval $(d, d+1]$. To also obtain $(d+1-\tau)/\tau$ as a lower bound for $\dim W_\tau(P_\alpha)$, it would be sufficient to prove such a result for the set $\tilde{R}_\tau(\alpha)$ as defined in (2.4). However, this would require the study of the distribution of solutions to congruence equations and a quantitative result on the uniformity of such a distribution. For arbitrary polynomials, this appears to be out of reach at the moment.

(3) The set of exceptions (with respect to α) left by Theorem 1.4 actually contains uncountably many points. Indeed, let $\tau > d+1$ be given and let (x, y) be a pair of real numbers simultaneously τ-well-approximable; this set is uncountable as its Hausdorff dimension is $3/\tau$ from the multidimensional generalization of the theorem of Jarník and Besicovitch. Then, setting $\alpha = y - P(x)$, it is readily seen that x lies in $W_\tau(P_\alpha)$, since x and $P(x) + \alpha$ are simultaneously τ-well-approximable.

Acknowledgements. The author thanks his PhD supervisor Detta Dickinson for suggesting the problem and for discussions that helped to develop the ideas put forward. The last concluding remark is entirely due to her. The author was supported by the Science Foundation Ireland (Grant RFP11/MTH3084).

References

1. F. Adiceam, An extension of a theorem of Duffin and Schaeffer in Diophantine approximation, *Acta Arith.* **162**(3) (2014), 243–254.
2. N. Budarina, D. Dickinson and J. Levesley, Simultaneous Diophantine approximation on polynomial curves, *Mathematika* **56**(1) (2010), 77–85.
3. D. Dickinson, Ideas and results from the theory of Diophantine approximation, in *Diophantine phenomena in differential equations and dynamical systems* (Research Institute for Mathematical Sciences, Kyoto, 2004).
4. H. Dickinson and M. M. Dodson, Simultaneous Diophantine approximation on the circle and Hausdorff dimension, *Math. Proc. Camb. Phil. Soc.* **130**(3) (2001), 515–522.
5. R. J. Duffin and A. C. Schaeffer, Khintchine's problem in metric Diophantine approximation, *Duke Math. J.* **8** (1941), 243–255.
6. K. J. Falconer, *The geometry of fractal sets*, Cambridge Tracts in Mathematics, Volume 85, p. 14 (Cambridge University Press, 1985).
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th edn (Clarendon, Oxford, 1960).
8. M. A. Korolev, On the average number of power residues modulo a composite number, *Izv. Math.* **74**(6) (2010), 1225–1254.
9. B. P. Rynne, Hausdorff dimension and generalized simultaneous Diophantine approximation, *Bull. Lond. Math. Soc.* **30**(4) (1998), 365–376.
10. V. G. Sprindžuk, *Metric theory of Diophantine approximations* (transl. R. A. Silverman), Scripta Series in Mathematics (V. H. Winston, Washington D.C., 1979).
11. R. C. Vaughan and S. Velani, Diophantine approximation on planar curves: the convergence theory, *Invent. Math.* **160**(1) (2006), 103–124.
12. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Annals Math. (2)* **142** (1995), 443–551.